S. HRG. 109–577

VETERANS AFFAIRS DATA PRIVACY BREACH: TWENTY-SIX MILLION PEOPLE DESERVE ANSWERS

JOINT HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS AND THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 25, 2006

Printed for the use of the Committee on Veterans' Affairs

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

28-754 PDF WASHINGTON : 2007

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

COMMITTEE ON VETERANS' AFFAIRS

LARRY CRAIG, Idaho, *Chairman*

ARLEN SPECTER, Pennsylvania
KAY BAILEY HUTCHISON, Texas
LINDSEY O. GRAHAM, South Carolina
RICHARD BURR, North Carolina
JOHN ENSIGN, Nevada
JOHN THUNE, South Dakota
JOHNNY ISAKSON, Georgia

DANIEL K. AKAKA, Hawaii, *Ranking Member*
JOHN D. ROCKEFELLER IV, West Virginia
JAMES M. JEFFORDS, (I) Vermont
PATTY MURRAY, Washington
BARACK OBAMA, Illinois
KEN SALAZAR, Colorado

LUPE WISSEL, *Majority Staff Director*
D. NOELANI KALIPI, *Minority Staff Director*

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
LINCOLN D. CHAFEE, Rhode Island
ROBERT F. BENNETT, Utah
PETE V. DOMENICI, New Mexico
JOHN W. WARNER, Virginia

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
THOMAS R. ELDRIDGE, *Senior Counsel*
MICHAEL L. ALEXANDER, *Minority Staff Director*
LAWRENCE B. NOVEY, *Minority Senior Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

C O N T E N T S

MAY 25, 2006

SENATORS

WITNESSES

APPENDIX

VETERANS AFFAIRS DATA PRIVACY BREACH: TWENTY-SIX MILLION PEOPLE DESERVE ANSWERS

THURSDAY, MAY 25, 2006

U.S. SENATE,
COMMITTEE ON VETERANS AFFAIRS,
AND COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committees met, pursuant to notice, at 10:09 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Larry E. Craig, Chairman of the Committee, presiding.

Present: Senators Craig, Burr, Thune, Isakson, Collins, Chafee, Warner, Akaka, Murray, Obama, Salazar, Lieberman, Carper, Lautenberg, Pryor and Jeffords.

OPENING STATEMENT OF HON. LARRY E. CRAIG, CHAIRMAN, COMMITTEE ON VETERANS' AFFAIRS, U.S. SENATOR FROM IDAHO

Chairman CRAIG. The Committee will be in order.

I will ask the Secretary to sit down, take a deep breath and collect his thoughts. He has just come from a hearing in the House. Then we would appreciate photographers and media keeping it down as much as you can in the front. Thank you.

We have an announced vote at or around 20 after, so we will attempt to get opening statements as much as we can prior.

Good morning, ladies and gentlemen. On behalf of Chairman Collins, as well as the Ranking Members of the two Committees, Senator Akaka of Veterans' Affairs and Senator Joe Lieberman of Homeland Security and Governmental Affairs, I want to welcome all of you to this joint hearing this morning.

First, I want to thank all of the Members of our two Committees for their willingness to participate jointly in this important hearing. I think the American public should understand that while this hearing is about the Department of Veterans Affairs and the compromising of sensitive personal information about our veterans, the issue of data security is a concern all across Government.

As I said on the Senate floor just 2 days ago, nearly every agency of the Federal Government maintains sensitive information on millions of American citizens. Most of this data is not of the classified nature. Rather, it is information compiled simply to carry out the mission and programs of various agencies.

For example, the Federal student financial aid form requires that you provide your name, address, Social Security number, date of birth, information of your parents, and their addresses, along with many other things. Clearly, the release of that data would be as devastating to the privacy of millions of students and their families as VA's breach was to millions of America's veterans and their families.

Still, we are here today to talk about what the Secretary of Veterans Affairs announced to the Nation this past Monday. He told my Committee and other Members that an employee of the Department downloaded data of nearly 26 million veterans and then walked right out the front door with it. Subsequently, the data was stolen from this employee's home.

Mr. Secretary, I must tell you, that is pretty unbelievable. How is it that VA's computer system permits one person to download the records of 26 million individuals and do so without any alert going off to anyone else who has the responsibility of the integrity of that system.

Candidly to me, that is not even the most absurd part of the story as I now know it. What is even more important and mind-boggling is after he revealed the facts of the theft to his supervisor, it took 13 more days for anyone else to discover the lost data was on 26 million veterans and their families. Then it took 2 more days for the FBI to be notified. So somebody lost the names, the birthdates and the Social Security numbers of 26 million veterans and their families and the FBI knew nothing for nearly 2 weeks.

Mr. Secretary, I read your statement yesterday in the press about the anger you felt at having discovered the lapse in security nearly 13 days after it happened. I am glad you are angry. You should be. You can only imagine how I and millions of veterans felt and now feel.

I just came from doing C–SPAN. I did call-ins. America's veterans across this country are frustrated. The word scared was used. The words are we at risk were used. And what do we do to protect ourselves?

Mr. Secretary, I understand the need to spend some time with your staff assessing problems and reviewing options, but I find it increasingly frustrating that decisions are made without the knowledge and the input of a few of us. I think we can be trusted. I think you know that.

Now, before I turn to Chairman Collins for her comments, I want to say a word about the employee who took the data home, as I now know it. While there is still an ongoing investigation as to the situation by the FBI, and I know that will limit some statements this morning, as best as I can tell from the information I have thus far, this person is a dedicated Federal employee who took work home with the hopes of improving VA's operations. Yes, his actions were inexcusable. He knew better than to take information home, or I hope he did. I hope policy suggested he should not or insisted he should not. He knew better than to take information home. And yet, a terrible lapse in judgment, and now he is faced with the serious consequences. But at least he told his supervisors and the law enforcement right away, which is more than we have been accorded.

I am not going to lose sight of the actions of everyone else in this situation. There were many lapses in judgment from many people. I hope this hearing today will shed some light on the shortcomings in VA's data security programs and on what needs to happen to ensure such a major breach never occurs again.

Also, I think our discussion will heighten the awareness of many other agencies across our Government to the vigilance about data protection and information security. As I said earlier, students, farmers, and others who seek Government assistance deserve our best efforts to protect their critical, vital, private information.

Most importantly, I hope today's hearings will provide millions of veterans and their families the assurance they deserve to have, that you are doing everything possible, Mr. Secretary, and we will do the same.

Thank you for being with us.

Chairman Collins.

OPENING STATEMENT OF HON. SUSAN M. COLLINS, CHAIRMAN, HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE, U.S. SENATOR FROM MAINE

Chairman COLLINS. Thank you, Mr. Chairman.

First, let me begin by commending you for your leadership for seizing the initiative for suggesting this joint hearing. I and the Members of the Homeland Security Committee are very pleased to join you in this effort to quickly address a very serious matter that is of great concern to our Nation's veterans, including some 141,000 veterans in my home State of Maine.

We are here today not merely to examine one incident, one moment of carelessness—make that recklessness—by one Federal employee. The specific incident compels us to confront the persistent and pervasive laxity with which the VA safeguards the personal information of the veterans it serves.

For 5 straight years, the VA's Inspector General has criticized the Department for inadequate information security. On the annual Federal Computer Security Report Card issued by the House Government Reform Committee, the VA has received a grade of F for 4 of the last 5 years, including each of the last 2 years.

This ongoing failure during a time when identity theft has been such a high-profile problem is simply appalling. The immediate result of this failure is what appears to be the largest theft of Social Security numbers ever. The fact that the information also included veterans' names and dates of birth means that the stolen data can easily be used to commit identity theft and financial fraud.

The lingering result will be increased doubts among the American people about the Federal Government's commitment to safeguarding their personal, sensitive information.

When we think of cyber security, we focus on protecting vital information systems against intrusion by criminals or terrorists. We now see that all the high-tech fixes in the world cannot protect these systems against one employee who disregards an established policy, and one agency that does not take sufficient measures to ensure compliance with the policy.

I am also troubled by the VA's response. The burglary that led to this potentially massive intrusion occurred on May 3. Yet, as the

Chairman indicated, it apparently was not reported to the FBI for 2 weeks. The American people, and most important our veterans, were not informed for nearly 3 weeks.

Now, some delay prior to disclosure could well be reasonable, to allow law enforcement time to hunt for the stolen information or to put in place a system to respond to the many inquiries from our veterans. However, much of the delay in this case appears to be because the VA did not promptly investigate the nature and the scope of the data breach. It simply appears that the VA did not handle this matter with the clear sense of urgency that it required.

I am also concerned about the initiatives the VA has taken to address the immediate crisis. Is it sufficient simply to establish a toll-free number for veterans to call? We have already heard, in my office and others, that veterans have called this number, but have been unable to learn much of anything.

Is it sufficient to just accelerate a schedule of computer security training for VA employees? Or should more be done? We must ensure that the remedies the VA puts in place, both short-term and long-term, are real, will make a difference and are not merely cosmetic.

We must also view this incident as a wake-up call to the rest of the Federal Government. It is likely that the VA is not alone in the potential to suffer a data breach of this magnitude. Federal managers must recognize that they are stewards of a large amount of personal data on law abiding citizens, and they must guard this information wisely or lose the people's trust.

It is tragically ironic that this profound betrayal of trust occurs just as the American people are preparing to honor our veterans. On this Memorial Day, the pride our veterans should feel in their service to our Nation will be dampened by anxiety and justifiable anger.

These are the people who have served our Nation yesterday and who serve today. They are brave, patriotic, and devoted to duty. They deserve our gratitude and much more. They certainly deserve better than this. We owe them our best efforts so that the deep problems that this incident has exposed are fixed and so that the trust they should be able to have, not only in the VA but across our Government can be restored.

Thank you, Mr. Chairman.

Chairman CRAIG. Thank you, Madame Chairman.

We do have a vote on and it started at 10:16. I suspect we can go. So Senator Akaka, if you would wish to go ahead with your opening statement, we will get a few more. I would ask that we keep these as limited as possible so we can get to the Secretary. But please proceed.

STATEMENT OF HON. DANIEL K. AKAKA, RANKING MEMBER, U.S. SENATOR FROM HAWAII

Senator AKAKA. Thank you very much, Mr. Chairman, and Chairman Collins, for working together for calling this very important and timely joint hearing.

As the Ranking Member on the Veterans' Affairs Committee and a senior Member on the Homeland Security and Governmental Affairs Committee, I am privileged to sit on two committees that

have oversight on this issue. Having both Committees investigating this matter will allow us to address the specifics of the incident involving VA data and work to craft safeguards for the entire Government.

I would like to say, Mr. Chairman, that I want to associate myself with the eloquent statement that you made.

Let me be clear, the specific incident that brings us here today happens to involve VA and VA data. It could just as easily have involved other departments and agencies. It may be wise to have other departments and agencies examine their policies on classified and confidential data and the proper use and security for such data.

Shortly after the news that the incident broke, I spoke with VA Inspector General George Opfer. He told me his office launched a full investigation into the matter which would examine all of the facts. I eagerly await his findings as the investigation will provide independent information for Congress to assess the situation.

I also wrote to Secretary Nicholson with a number of questions and I look forward to his responses today.

I have a longer statement, Mr. Chairman, but I will not read it so we have more time to hear from and question the witnesses. I ask that my full statement appear in the record as if read. Thank you very much, Mr. Chairman.

[The prepared statement of Senator Akaka follows:]

PREPARED STATEMENT OF HON. DANIEL K. AKAKA, RANKING MEMBER, U.S. SENATOR FROM HAWAII

Thank you Chairman Craig and Chairman Collins for working together to call this very important and timely joint hearing. As the Ranking Member on the Veterans' Affairs Committee and a senior member on the Homeland Security and Governmental Affairs Committee, I am privileged to sit on the two committees that have oversight on this issue. Having both Committees investigating this matter will allow us to address the specifics of the incident involving VA data and work to craft safeguards for the entire government.

Let me be clear—the specific incident that brings us here today happens to involve VA and VA data. It could just as easily have involved other departments and agencies. Shortly after the news of this incident broke, I spoke with VA Inspector General George Opfer. He told me his office launched a full investigation into the matter that will examine all the facts. I eagerly await his findings as the investigation will provide independent information for Congress to assess this situation. I also wrote to Secretary Nicholson with a number of questions that need to be answered. I look forward to his response today.

I am especially concerned with the manner in which VA handled this investigation. Although the breach occurred more than 3 weeks ago, Congress and the public were only notified of the incident this week.

Regardless of whether identity theft actually occurs as a result of this incident, anytime the government loses a database of personal information, privacy is compromised. We must do all we can do to prevent this from ever happening again. The security mechanisms at VA are not working if a mid-level VA employee was able to walk out of the building with a massive amount of personal information. It seems to me that data of this magnitude and importance should be in the hands of very few VA employees and should be guarded with the utmost security. Thus far, VA has said the employee was not authorized to take the information home.

I am troubled as to how an employee who is not authorized to take home the private information of more than twenty-six million veterans was still able to do just that. The VA failed to take several steps to safeguard this information. For example, VA could have scrambled Social Security numbers based upon an encryption formula, whereby access to files that translate scrambled Social Security numbers is only possible with special authorization. This procedure was not followed in this instance, and we need to know why. It is important to note how we came to learn about the loss of the data. The VA employee whose computer equipment was stolen

disclosed this to VA. If the employee had chosen not to report the theft immediately, VA and the public could possibly still be in the dark about the incident.

As I said earlier, while today's hearing is focusing on the information security practices at VA, I believe the data breach is indicative of broader information security and privacy problems throughout the government. I understand the problems that agencies face, as I have been working on Federal data collection and privacy for a number of years. At my request, the Government Accountability Office (GAO) conducted several investigations on Federal data mining activities and found that Federal agencies are not following all key privacy and information security practices. Last week, I introduced legislation to strengthen the investigative authority and independence of the Chief Privacy Officer at the Department of Homeland Security.

I believe we need to make sure that all agencies have a strong privacy official to ensure that what happened at VA will not happen again. Last year, the Office of Management and Budget directed each agency to designate a senior privacy official. However, issues remain as to whether these individuals are focused on matters other than privacy, which may cause a conflict of interest; the training received by and the expertise of these individuals; and the enforcement authority of the privacy officers in each agency. Having policies and safeguards in place will not work if agencies are not following the law.

The incident at VA demonstrates the need to review the Privacy Act. I believe it is appropriate at this time, Chairman Collins, for your Committee to undertake this review as soon as possible. The applicability of the Act in this increasingly electronic age, combined with limited remedial action, necessitates that we take a closer look, and make sure that the personal information that the government collects is properly maintained.

It is unfortunate that, as the Nation prepares to celebrate those that paid the ultimate sacrifice in defense of our freedom, our government has breached the trust of its heroes. Our veterans deserve much better. I intend to work with all appropriate parties to provide real solutions to these glaring problems, not just in VA but across all government agencies and departments. Thank you.

STATEMENT OF HON. JOSEPH I. LIEBERMAN, U.S SENATOR FROM CONNECTICUT

Senator LIEBERMAN. Thanks, Senator Akaka. We are going to continue going around and hope that Chairman Craig and Chairman Collins come back in time.

I want to thank them and Senator Akaka for holding this hearing as quickly as they have, so that we can get some answers about this enormous security breach, how it occurred in the first place and how we can quickly assist those veterans to whom we all owe so much and who have been put at risk by the loss of their confidential information.

The security of Government computer systems and the vast databases contained within them is a subject we on the Homeland Security and Governmental Affairs Committee have been working on for some time.

As information technology continues to advance by leaps and bounds, we must take equivalent leaps and bounds to protect against the theft, misuse and abuse of information brought together as never before by that technology.

At various times in our lives we, the American people, are required to provide the Government with all sorts of personal information. We do so out of necessity and sometimes out of choice. But we also, of course, provide it on the basis of trust. We, the American people, will not feel comfortable sharing that information that the Federal Government needs if the Federal Government cannot guarantee that it is kept private and secure.

This latest incident at the VA is just the most recent reminder that the Federal Government generally, I have concluded, is not

doing enough to guarantee that security. Three years ago, I asked the Government Accountability Office to assess and evaluate Federal privacy protections. GAO looked into the privacy practices of 25 Federal agencies and reported back that compliance was very uneven and that in nearly one-third of cases when agencies disclosed personal information to non-Federal organizations, the agencies did not have procedures in place to ensure that the personal information disclosed was complete, accurate, relevant, and timely as required by the Privacy Act.

Last year, Senator Collins and I took the Transportation Security Administration to task for violating the privacy of thousands of commercial airline passengers when it collected and stored personal information about those passengers. Not only did TSA violate its own privacy policy, it also failed to meet the basic requirements of the Privacy Act, which is law.

The VA security lapse is particularly troubling to all of us. Infuriating, in fact, because of the population of veterans that may have been placed at risk. So we are here today to get answers to questions and they have really been framed by my colleagues who have spoken before.

So, I will simply conclude by saying, Secretary Nicholson, I have great respect for you. I think you know that it is now up to you and your Department to restore the American public's trust in the VA, which is a good and efficient Department, and in the ability of Government as a whole to carry out its duties without jeopardizing personal and sensitive information the people of this country have and give to their Government.

As part of that, I hope you will not hesitate to hold accountable anyone who was responsible for this failure to protect the confidential information of millions of American veterans.

Thank you very much.

Senator Warner.

STATEMENT OF HON. JOHN W. WARNER, U.S. SENATOR FROM VIRGINIA

Senator WARNER. Thank you, Mr. Chairman.

I want to first say a few words about the Secretary of Veterans Affairs. I have known him for a very long time. In times like this, when we have literally a very serious problem at hand, it is fortunate Jim Nicholson has stepped up for continued public service. He has about as distinguished a career in the United States military as one can have in contemporary times.

I thank you, my good friend, for calling me very promptly on the early morning when this news first became public and reassuring me, as I am sure you are going to reassure veterans all over America, that you are going to have a total hand on the situation to hold accountable those who have perpetrated any wrongs or breach of law, and to reassure veterans that we are going to protect them to the extent we can.

If I may say with some modesty, I am a veteran myself of World War II and Korea, and I have had a lifetime association, as you have Mr. Secretary, with the men and women of the Armed Forces who have served. And we must recognize, as my colleagues alluded, that technology has gone forward so rapidly. Ten years ago, if you

were trying to plan a theft like this, you would have to have a six-wheeler van to haul the information out. Now a simple disk can slide into the pocket. Consequently, we have to take measures which keep apace with technology to give the security that is required in this situation.

But I would like to once again say, as this hearing is commencing and as people are following it all across the United States, you will do a good job, Mr. Secretary. You will get to the bottom of this and solve it, because of your deep love, respect and affection for America's veterans.

Thank you.

I think we should stand in recess until the return of the Chair. Do you wish to—good, thank you very much.

STATEMENT OF HON. JAMES M. JEFFORDS, U.S. SENATOR VERMONT

Senator JEFFORDS. Mr. Chairman, I appreciate your holding this hearing on such short notice to examine the frightful breach of security at the VA that has led to the loss of significant data of millions of veterans. I understand that the Government, and in particular agencies such as the VA, who deal in direct health of individuals need to have sensitive personal information. But the Government therefore has a sacred obligation to make sure that this information is secure. This is an inexcusable breach of the basic compact of trust between the veteran and the VA. I am a veteran myself.

The FBI must get to the bottom of how this happened and take immediate measure to ensure that it never happens again. We owe our veterans nothing less.

I look forward to your testimony, Mr. Secretary, and hope you will give us reason to be reassured that the VA is taking immediate action to address this horrendous problem.

Thank you, Mr. Chairman.

The Committee will now stand in recess until the Chairman returns.

[Recess.]

Chairman CRAIG. The Committee will be back in order.

Mr. Secretary, thank you for standing down for a few moments while we went to vote.

Now let me turn to Senator Murray.

STATEMENT OF HON. PATTY MURRAY, U.S. SENATOR FROM WASHINGTON

Senator MURRAY. Let me thank Chairman Craig and Collins, as well as our Ranking Members Akaka and Lieberman, for calling this very important hearing today.

Simply put, this is really a disaster. Our phones are ringing off the hook with veterans from all across the country who feel that their privacy has been violated and they are really losing faith in the VA. We have 85-year-old veterans who do not know the first thing about credit checks, and they are being told that their identity has been compromised and they really do not know what to do. We need to find a way to provide assistance for all of our veterans and give them the peace of mind that they deserve.

Now, I know that some say that this is just an isolated incident, that this is an accident caused by one employee at the Department of Veterans Affairs, but Mr. Secretary, I have to tell you, from where I sit, this seems like just another demonstration of the agency's incompetence.

As Chairman Collins said, the VA was told time and again by the IG that it had weaknesses in its information security systems. The VA was warned about the lack of protection for veterans' sensitive health care and benefits information, and these warnings seem to have gone unnoticed by leadership within the VA.

I hope we hear this morning from you, Mr. Secretary, about how this happened, why it took so long to tell our veterans that their information was compromised, what we are going to do to rectify this situation and what steps you are taking to ensure that it never happens again.

Again, as we have discussed before, these Committees and this Congress have instilled in you the responsibility to fight and defend our veterans. I know that all of our veterans need you to be their greatest advocate.

I am very disappointed by what has transpired and I hope that this agency really now rises to the occasion under your leadership and show all of us here and the millions of veterans that are at risk that you are here to protect them even from your own agency's mistakes.

Thank you, Mr. Chairman.

Chairman CRAIG. Thank you, Senator.

I note that statement was made in under 3 minutes. I appreciate that very much and would hope that our colleagues would attempt to adhere to that so that we can get to the Secretary.

Let me turn to Senator Isakson.

Johnny.

STATEMENT OF HON. JOHNNY ISAKSON, U.S. SENATOR FROM GEORGIA

Senator ISAKSON. Thank you, Mr. Chairman, and I will be brief.

I thank you and Chairman Collins for calling this hearing.

Mr. Secretary, I can empathically identify with the 760,000 veterans in Georgia who are probably on this list, because a year ago I was notified that my information had been lost or stolen by an American corporation and I know how I felt. I also know how they responded. And I hope we will and the Administration will respond swiftly to ensure the veterans are protected and they get the information they need.

To that end, Mr. Chairman, I would like to ask unanimous consent to submit a letter for the record.

Chairman CRAIG. Without objection.

[The letter referred to follows:]

EQUIFAX INC.,
Peachtree Street, Georgia, May 24, 2006.

Hon. JOHNNY ISAKSON,
U.S. Senate,
Washington, DC.

DEAR SENATOR ISAKSON: At Equifax, we honor the enormity of our veteran's contribution to the success and security of our great country, and are pleased to assist them in any way possible. Upon learning of the data breach at the Veterans Admin-

istration Office, Equifax immediately developed a special assistance page on our Equifax.com website. This page is designed to educate and assist our veterans on identity theft, and the ways in which they can safeguard their personal, information. This special assistance page includes the following:

1. How to place an initial fraud alert on their credit file. This will alert creditors of possible fraudulent activity and request they contact the veteran prior to establishing credit in their name.

2. How to request a free copy of their credit file atannualcreditreport.com, or by phone or mail.

3. A special offer for Equifax's Credit Watch products available to veterans at a 50 percent discount until June 30, 2006. Credit Watch, will monitor the veteran's credit file and alert them to changes that could be early warning signs of identity theft.

We look forward to continuing to work with the Veterans Administration Office to assist our veterans.

Sincerely,

RICHARD F. SMITH,
Chairman and Chief Executive Officer, Equifax, Inc.

Senator ISAKSON. The Equifax Corporation out of Atlanta, on the day of the announcement, notified the VA and all veterans of a hotline, affording them immediate access to a free credit report, and offered them a 50 percent discount on 1 year's credit card service to monitor their credit. Mr. Richard Smith, who is the CEO of that company, was in Washington yesterday. I had the chance to talk to him and I thanked him personally for their voluntary effort. But I think it is important that the agency come together with a seamless policy to protect all veterans.

Lastly, Mr. Chairman, I want to commend you on your statement with regard to this being a wake-up call. As terrible as this loss of information is, just think if the Social Security Administration or the IRS and all their computer data information did not have a good security system.

So I hope as we work to raise the level of interest in this issue and hold the VA accountable, we will make sure we are checking with every agency of the Government and making sure they are redoubling their efforts to ensure this does not happen in any other agency as well.

I yield back the balance of my time.

Chairman CRAIG. Thank you, Senator.

I am proceeding on the order with which Senators first came to the Committee, and I will turn to Senator Salazar.

Excuse me, he is not here.

In that case, it is Senator Lautenberg.

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thanks, Mr. Chairman, and I will join the race to the 3-minute mark and see if I can rush through.

Madame Chairman and our guest Chairman, thank you very much for arranging this joint hearing on such short notice. I appreciate the opportunity to learn about this alarming breach of security that has compromised the personal information of 26 million veterans and families.

I served at an earlier time and the records regarding my service and those who served at my time were destroyed in a fire in St. Louis in the Veterans Administration facility. So it does not install a lot of confidence when we see what has happened now.

In the next few days, we are going home for Memorial Day, a day we want to honor our veterans and their service. But this week we learned that the Government has failed them, put them at risk, at significant risk. Our veterans deserve the best in health care and other services. But what they got in this case is a security breach that puts them at risk for theft of their identity.

In recent years, we have all learned that identity theft has serious consequences for its victims. This incident, involving the VA, is the largest breach of Social Security numbers ever and it is appalling that something could happen. To make matters worse, the VA's response to the crisis has not been satisfactory. As a matter of fact, it really destroys confidence in the functioning of the VA.

They have a call center in New Jersey and veterans who call there do not think the VA call center is very helpful. These veterans will probably have to take some steps themselves to make sure that their credit information is not compromised and that they are not subjected to deep losses as a result.

We should make it simple for them as much as we can. And that is why I am joining Senator John Kerry in supporting his bill to help veterans to stay informed about their credit status in the aftermath of this incident.

Again, thank you very much, Mr. Chairman and Madame Chairman.

Chairman CRAIG. Senator, thank you very much. Now let me turn to Senator Thune.

John.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman and Madame Chair.

I appreciate, as well, very much your holding this emergency hearing to deal with the theft of personal information for millions of our veterans, and I want to thank Secretary Nicholson for appearing today.

Mr. Chairman, I share your commitment to understand all the facts of this case before taking action, and I hope this hearing will generate light that we can use to do that.

Having said that, this breach of information security at the VA is causing a lot of anxiety across the country among our veterans. And they are rightfully demanding that we act quickly on this issue. I have many veterans in my State of South Dakota who are justifiably concerned about identity theft, and they deserve to have peace of mind about their privacy.

That is why we have to work quickly here on these committees to learn all the relevant facts and then take the appropriate action. And that, I think includes, in the short term, finding out the exact proportions of the problem and developing a proportionate remedy. Also, looking at the long term, at what we can do to make sure that this thing never happens again.

As a number of Members of the Committee have already noted, the IG's most recent strategic plan indicated that one of the strategic goals was in the area of information management. It also noted many of the challenges the VA faces in the privacy of and the security of the information it manages. The strategic plan fur-

ther states that information systems security has been identified as a material weakness as early as 1998 within the VA.

And then there is this key passage on page 58, which I want to just read for you,

> The potential vulnerability of Federal information systems cannot be overestimated. Presently, VA systems are not protected from authorized access, risk of potential exposure, loss of sensitive data, fraudulent claims and disruption of critical activities remain. Security over VA IT resources needs to assure that only authorized users access VA resources and only authorized use is made of VA resources. Legal requirements such as the Privacy Act, the Federal Information Security Management Act of 2002, and the Health Information Portability and Accountability Act of 1996 impose detailed duties on the VA to protect sensitive medical and personal information it maintains on veterans, their families and its employees.

Clearly, what the Inspector General was concerned about in terms of information security has now become a reality that we must deal with. I believe that this event occurred at least in part because many of the VA's IT systems are compartmentalized within the VA's three administrations: health, benefits and cemeteries; and there is not a uniform policy in terms of information security across the entire VA.

That is why, Mr. Chairman, I introduced a bill, last fall, to improve the management of IT within the VA. My bill would provide for the VA's Chief Information Officer to have authority over resources, budget and personnel related to the support function of information technology. An identical bill has passed the House. I hope that this will give us an opportunity to pass it in the Senate.

I appreciate again, Mr. Chairman, your holding this hearing. We are here to understand the entire context of this situation and then to work on both short-term and long-term solutions. We must do all that we can to ensure the information privacy of our veterans who have sacrificed so much for all of us.

So thank you again and I look forward to the testimony.

Chairman CRAIG. Senator, thank you.

Senator Burr.

STATEMENT OF HON. RICHARD M. BURR, U.S. SENATOR FROM NORTH CAROLINA

Senator BURR. I thank both the Chairs.

Mr. Secretary, Senator Isakson and I have something in common, in the fact that we both participated in this before from the standpoint of our records being lost. Mine happened to be a stolen laptop with my pertinent information from the accounting firm that does my taxes. I remember vividly getting the call and being walked through exactly what they were doing to make sure that they minimized what was a huge mistake.

Fortunately, I have never had any repercussions from that over the several months that I have gone through. I am sure we can find a number of ways to tongue lash the system, and you and the Administration.

Let me suggest to my colleagues, that is not what we are here to do. We are here to figure out—to work with you—to try to figure out how to remediate a problem that we do not know the scope of yet, to once again remind the Veterans Administration and every branch of Government that it is unacceptable to have the delay in

notification to the Congress, to the Federal law enforcement folks, that these are policies that we need to look at, that this cannot be something we make up on the go.

I certainly commit myself to you and to the Chairs to work aggressively to find how we can adopt a policy that we all feel confident is structured in a way that minimizes the risk of this in the future.

But more importantly, a policy that we can communicate to all concerned of exactly what we do if it ever does. I think the belief that we can assure with 100 percent accuracy that we can eliminate this is a dream. We cannot. That is why it is just as important that we understand that we need a policy in place that everybody understands that helps us to remediate this.

Once again, I do want to say publicly to you that it is unacceptable to have had a 60-day delay or a 15-day delay between the time that notification went out to the Administration, the Congress and the FBI.

My hope is that through this hearing, it is the start of the road to a recovery from where we are.

I thank the Chairs.

Chairman CRAIG. Senator, thank you very much.

Senator Obama.

STATEMENT OF HON. BARACK OBAMA,
U.S. SENATOR FROM ILLINOIS

Senator OBAMA. Thank you very much to the Chairs for holding this hearing. I will try to be brief.

This episode raises so many questions, but I think maybe the most poignant one was raised by Sonny McQueen, a DC area veteran. He said, "How else can the country let us down?" And I think that is a feeling that may be pervasive among a lot of veterans.

I hope this hearing is the first step toward answering some of those questions. As has already been noted, why did it take 2 weeks for the VA to notify the FBI? That was a 2-week head start for criminals to potentially wreck havoc. Why did the VA wait nearly 3 weeks to notify the veterans who were at risk? That is a policy issue.

I have no doubt, Mr. Secretary, that you are as outraged as we are about this problem. But I am concerned about what is it structurally inside the VA that is preventing information from being dealt with properly? And what is preventing the VA from being forthcoming to veterans and the American people?

We have a duty to make this right. The average identity theft victim spend 40 hours, apparently, to clean up his or her finances after something like this happens. So as a first step, I am hoping that the VA is going to be thinking about how it is going to provide credit monitoring and counseling services to the veterans who may be affected. This is a problem that may take a lot of time and money to fix, but we are going to need to make our veterans whole.

Beyond that, I think it is important for us to understand that, although this may be a mistake of one employee, the reality is that this is a system that was destined to failure. Just a couple of quick facts. This is a system that scored an F in information security in 4 of the past 5 years on a House Committee report card. This is

a system that in 2001 allowed VA employees in Atlanta to steal $11 million in benefits. The VA Inspector General, as has already been noted, has argued for years that the VA needed to improve its IT security. The VA Chief Information Officer abruptly resigned a month ago because the agency was not moving fast enough on its IT reorganization.

So, we cannot pin this on one individual. This is a systemic breakdown. The system is so poorly designed that one employee could compromise the entire thing. That raises the question how could managers not realize that so many files were downloaded and brought offsite? And what steps is the VA going to take to secure veterans' data used in other programs?

I hope that through this hearing we can get to the bottom of this fiasco. I think we need to hold VA officials accountable. We also need to look forward and try to prevent identity theft across the private and public sector. It is estimated that 10 million consumers are affected annually.

I understand that Senators Specter and Leahy are going to be looking at ways in that Committee to deal with issues of identity theft. I hope that all of us work on this. In the meantime, we are going to have to figure out how to clean up this mess.

Thank you very much Mr. Chairman, Madame Chair. I look forward to the hearing.

Chairman CRAIG. Thank you very much, Senator.

Again on the order with which Senators came to the beginning of the hearing, let me turn to Senator Salazar and then to Senator Chafee. Thank you.

Ken.

STATEMENT OF KEN SALAZAR,
U.S. SENATOR FROM COLORADO

Senator SALAZAR. Thank you very much, Chairman Craig and Ranking Member Akaka and Chairman Susan Collins and Ranking Member Lieberman, for holding this hearing.

Let me just say I think my colleagues have stated the concerns that we all share. And I know that Secretary Nicholson has also stated his concerns and how appalled he is about what has happened here with the records of 26.5 million veterans. It is a huge issue that we need to address and we need to address effectively to make sure that we prevent this kind of thing from ever happening again.

Secondly, we need to make sure that we are taking every step in the world possible to safeguard the getting out of this information, from where ever this information happens to be today.

But I also think it calls into question, even beyond the VA, what is happening with respect to all other Government agencies that have huge amount of information and the safeguarding of that information in the new kind of technology.

I was thinking about 26.5 million names and records related to 26.5 million names. You know, 20 or 30 years ago you would never be able to put that into any kind of a file on a laptop. Well, that has all changed. And I think part of what we are seeing here is somehow the policies and oversight of information within our Government has not kept pace with the new technological capacities

that have been developed with the computer capacities that we currently have.

So I look forward to working with you, Secretary Nicholson, to get us to a solution that will address the issue within the VA, but also I think for all of us in Government, we need to understand that this is an issue that also goes beyond the VA.

Thank you and I have a more formal statement for the record, Mr. Chairman.

Chairman CRAIG. Without objection, it will be a part of the record.

[The prepared statement of Senator Salazar follows:]

PREPARED STATEMENT OF HON. KEN SALAZAR, U.S. SENATOR FROM COLORADO

I want to start by thanking Chairman Craig, Chairman Collins, Senator Akaka, and Senator Lieberman for bringing together this critical hearing on such short notice. As we all know, one of the central questions in this troubling incident relates to whether or not the VA could have responded more quickly to the news that the personal information of 26.5 million veterans had been compromised. In light of those concerns, I believe it is imperative for Congress to act as quickly as possible to address this situation, and I hope today's hearing will set an example.

I also want to thank today's panelists for agreeing to come before our committees today to discuss this important matter. I realize that many of you had to change your plans to be able to be here. But our veterans weren't planning on having their information put at risk, either, and it's important we do everything within our power to protect them during what must be a worrisome time. So, thank you.

I am extremely troubled by what we learned earlier this week from the Department of Veterans' Affairs. First and foremost, I share the concern of our Nation's veterans about the potential for misuse of their names, birthdates, and Social Security numbers, and the consequences—both personal and financial—that could result.

What is most troubling to me is the nature of the information that has been compromised. This is not like losing your keys or your credit card, where you can change your locks or your account information. These are the fundamental keys to a person's identity, and they could be used to open a bank account, take out a loan, obtain lines of credit, buy property—and the list goes on. The lives of millions of our Nation's veterans could be turned upside down as a result of this security lapse.

Second, this incident raises serious questions about the gaping holes in security that exist at VA, and about why more hasn't been done about them in recent years. We have known that VA's security safeguards are insufficient for years, and yet very little has been done to prevent the kind of theft we saw earlier this month. We need to know why, and we need to know what the VA plans to do now to ensure this kind of nightmare never happens again.

Finally, as I have mentioned, we need to know more about how this event and VA's response to this event unfolded, and why the department did not act more quickly to notify law enforcement, Congress, and most importantly, our veterans.

I look forward to working with my colleagues to address this issue. I have written to VA urging the department to do everything it can to protect our veterans and make sure it doesn't happen again. I am also a cosponsor of legislation introduced by Senator Kerry that would require VA to provide 1 year of free credit monitoring to affected individuals, and one free credit report each year for 2 years thereafter.

Our Nation owes a debt to our veterans that can never be fully repaid. It is deeply concerning to me that the very agency responsible for providing these veterans with the care and services they have earned failed to protect their most basic personal information. For that reason, I am hopeful that we can get to the bottom of some of these issues today.

Thank you.

Chairman CRAIG. Senator Chafee.

STATEMENT OF HON. LINCOLN D. CHAFEE, U.S. SENATOR FROM RHODE ISLAND

Senator CHAFEE. Thank you, very much, Mr. Chairman. Welcome, Secretary.

I share my colleagues great, great concern about what occurred and want to work with you, after appropriate investigations and reviews are done, to any legislative fixes or funding concerns you might have to rectify the situation.

I noticed in your opening statement, no specific requests at this point. But maybe after further reviews and investigations, there will be some concrete requests. I look forward to working with you on that, and also with Inspector General Opfer.

Thank you, Mr. Secretary. Thank you, Mr. Chairman.

Chairman CRAIG. Senator, thank you.

Senator Pryor.

STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

I think most of our colleagues here have covered my concerns with the VA and the bad news that we received in the last few days regarding the VA. But I do think that this is a reminder again, for Members of the Senate and Members of the House, that we need to act. And we need to spend time working through solutions for this so that the American public can protect itself.

One thing we passed last year, I guess or in the last several months, in the Commerce Committee is a security freeze bill. Basically what that would allow Americans to do is work through a credit bureau and freeze their financial information so that someone could not tap into that, get credit cards, loans, et cetera, in their name without their permission.

So, here you have a breach of 26-whatever million veterans and the security freeze would allow every person, if they chose to, to protect themselves in that way. So I think it is a good commonsense solution. It is something that has been through the Committee. Hopefully, Senator Frist and Senator Reid will work out some time on the floor. I would love to have you all look at it when it gets to the floor. I think it is something that once you understand what it does and once you see it, you will realize the American public would really like to have this option to protect themselves against things like this.

Thank you, Mr. Chairman.

Chairman CRAIG. Thank you.

Mr. Secretary, again welcome to the Committee. Please tell us you are mad as hell.

STATEMENT OF HON. R. JAMES NICHOLSON, SECRETARY, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY TIM S. McCLAIN, GENERAL COUNSEL, DEPARTMENT OF VETERANS AFFAIRS

Secretary NICHOLSON. You can count on that, Mr. Chairman.

Chairman CRAIG. Thank you.

Secretary NICHOLSON. Mr. Chairman, Members of the Committee, I appreciate having this opportunity to appear before you

to talk about this devastating occurrence that has happened in my agency and come to my attention only recently and was announced to the veterans and to the public and to the Congress this past Monday.

I am the person ultimately responsible to our veterans. And therefore, I am the person responsible for this situation. This responsibility rests on me.

A VA employee, a data analyst, took home electronic data files from the VA. He was not authorized to do so. His house was burglarized and the data were stolen. This happened on May 3rd.

If this were not bad enough, I was not notified about this event until May 16th. So I can tell you, as a 34-year veteran myself, I am mad as hell. I am outraged by all of this. I am outraged that this employee would do this so recklessly. And I am outraged that I was not notified of it sooner.

But I still must carry on and lead the efforts needed to get to the bottom of this and take the corrective actions to see that this does not happen again. My compass for this is the veterans. I feel so badly for them and what they are going through potentially and the anxiety that this is causing and what it could cause.

As has been said, these stolen data contained the information, including the names and date of birth, for 26.5 million veterans and some spouses. In addition, that information, plus Social Security numbers, were available for some 19.6 million of those veterans, of those 26.5 million. Also included possibly were some numerical disability ratings and the diagnostic codes that identify their disability.

It is good to note that the data did not include any VA electronic health records. Neither did it contain explicit financial information, although knowing a disability rating code could lead one to compute at least what that compensation payment was.

On May 3rd this employee's home was broken into and local law enforcement was notified immediately. They report that they think this was a routine breaking and entering. That is, it was not a targeted burglary. It was a random burglary.

The employee has been placed on administrative leave pending the outcome of this investigation, with which he is cooperating.

As I have said, I am a veteran and this is just incredulous. I am so damned mad at the loss of our veterans data and the fact that one person could put all of us at risk, one person in violation of VA policies.

I am just as mad and disappointed that I was not made aware of this before I was.

So, I am upset about the timing of our response. I will not tolerate inaction and poor judgment when it comes to protecting our veterans.

Appropriate law enforcement agencies, including local police, the FBI, and the Inspector General, have now launched full-scale investigations. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. It is possible that the thieves remain unaware of the information they possess and how to make use of it.

Because of that, we attempted to not be too specific about the description of the equipment stolen, the location from which it came

and other information in general. We do not want to provide information to the thieves that might be more helpful to the nature of what they have and we still hope this was a common theft and that no use will be made in this VA data.

From the moment I was informed, the VA began taking all possible steps to protect and inform our veterans. However, there were those in the law-enforcement community who wanted me to wait longer before announcing this theft, so as to pursue leads and to keep the burglars in the dark. I chose to inform our veterans nevertheless, but limiting the details of where and when initially so as not to tip our hand to the robbers.

Whether it is one veteran or the numbers we are talking about here today, the VA needed to act in a manner that maintained a balance between protecting them and informing the perpetrators. I chose to get the information out at that point to the veterans, in spite of the continuing investigations.

Another very disturbing aspect of this is that although it happened on May 3rd, and this employee informed his boss of this fact on that day, as I said, I was not made aware until May 16th. Equally disturbing is that Federal law enforcement head and investigating agencies were not informed immediately either. Local were, but not Federal. It was not until May 10th that the VA IG became aware of it.

I cannot explain these lapses in judgment on the part of my people. Most of them are really great, hard-working people. It makes me so angry and disappointed. And after the IG finishes his investigation as to exactly what happened, I plan to take decisive actions. I have to.

The VA now has also begun a relentless examination of our policies and procedures to find out how we can prevent something like this from happening again. We will stay focused on the problems until we get them fixed. I have formed a special task force to examine comprehensively all of our information programs and policies to bring about a ringing change in the way we do business.

I have begun recruiting to see if I can find the right individual to come into our agency to be the personal information security czar, if you will, who has nothing else in his or her portfolio, to focus on that and report directly to me.

As has been stated here, ever since 1999 the VA has gotten low marks from the IG on its information and cyber security programs. Last year the GAO flunked the VA on its cyber security system. This has got to change.

This situation is exacerbated by the fact that the Assistant Secretary for IT, who had been at the VA for about 2½ years, has just recently resigned. He had come to the VA from the private sector, from Dell. He has returned to the private sector. He did a very good job and I will say that I think we are off to a real solid start in the IT transformation that we are doing.

And this is beyond the scope here, but VA has gotten decentralized down literally to almost clinics, of which there are 900. We are pulling this back into a centralized format in this major IT transformation that we are in. And that is launched. But as is painfully evident, we have a great deal to do.

I was also pleased that just yesterday, President Bush announced his intention to nominate a brilliant, recently retired Navy Admiral that we have recruited to come into our agency to head up our Office of Policy and Planning, which is the office in which this transgression occurred. We hope to have him on board very soon.

Additionally, we are taking direct and immediate action to address and alleviate veterans' concerns and to regain their confidence. Those actions include that we have directed all VA employees to complete the VA Cyber Security Awareness Training Course and a separate General Employee Privacy Awareness course and to do so by June 30th of this year.

I have also directed that a memo be issued requiring all VA employees to sign annually an employee statement of awareness, including their awareness of the Privacy Act, their awareness as to unauthorized disclosing or using directly or indirectly information obtained as a result of their employment in the VA, which is of a confidential nature or represents a matter of trust, or other information so obtained of such a character that its disclosure or use would be contrary to the best interest of the veterans and of their awareness of the loss or damage or unauthorized use of Government property or its carelessness or negligence in its use therein.

Additionally, the Department will immediately be conducting an inventory and review of all current positions requiring access to VA data.

This, I think, is a very important point because, as it turns out, we do not know anything about these people. The person who took this data home, the last that I can tell, had a background check, just a National Agency and Inquiries Check, 32 years ago. Yet, we entrust this kind of data to people.

And I might say, by the way, and this is not said in anyway as some kind of an excuse, but this man or others, they do not have to carry this data out. They can send it out. If they have Internet Explorer on their computer, they can send it to their account and then get on their own computer and receive it.

I also would tell you, and please, this is not said in any way to excuse or mitigate what happened thus, but I am holding in my hand a hard drive. This is unrelated to the equipment in this incident. But that data that we are talking about for these 26.5 million veterans is 5 gigabytes. This little thing right here, that slips so easily into my vest pocket, holds 60 gigabytes. We could have 12 times the data that is the subject of this pain that we are in on this thing, this little hard drive.

This, as you probably all know, which most people that use these use them as a key chain, and call them most commonly a thumb drive, this would hold about three-quarters of the data that we are talking about, this size. Most people that use these in my agency have them hanging around their neck with their ID card and walk in and out.

There are lots of things that we are going to have to do as an agency, and I think as a Government. But the key, it seems like to me, is going to be the law. And by the way, this person did not violate any law, because there is no law. We have internal policies against what he did. But he did not violate the law, as near as I can tell.

And we are going to have to—for people that have access to this kind of data, we are going to have to know something about them. If they were in the military and they were privy to confidential information, they would have a background investigation. And a lot of that, you read in the paper what we are giving them access to.

So, I am proposing that we are going to do an updated National Agency Check on those. And for those that have special access, request a minimum background investigation.

I have directed the Office of Information and Technology to publish by June 30th a VA directive and revisions to security guidelines for single user remote access developed by the Office of Cyber and Information Security. This document will set the standards for access, for use and information security, including physical security and reporting.

We are working with Members of the Congress, the VSOs and the news media and other agencies to ensure that other veterans and their families are aware of this situation and the steps that they may take to protect themselves for the misuse of their personal information.

We are coordinating with other agencies to send individual notifications to all 19.6 million individuals whose Social Security numbers were stolen. That is, we are going to send a letter to each of these people, instructing them and asking them to be both vigilant in order to detect any signs of possible identity theft and how to protect themselves.

As you know, in the meantime, they can go to the Internet portal we have established, which is *www.FirstGov.gov*, for information on this matter. And this is a Federal site that is capable of handling a great amount of traffic.

Additionally, we have set up a manned call center that veterans can use to get information and learn more about consumer identity protections. You can reach that with a toll-free number of 1–800–333–4636. It operates 14 hours a day and will as long as it is needed. It can handle 20,000 calls per hour. By the end of the day yesterday, concerned veterans had made a total of 105,753 calls to this number.

I do want to acknowledge the significant efforts of numerous Government agencies in assisting the VA to prepare for the announcement last Monday. Agencies at all levels pitched in to ensure that our veterans had information on actions that they could take with respect to their credit. Hundreds of people worked around the clock, that is they worked through the night, in helping to set up these call centers and get the messages composed and out and did a yeoman's job. I want to thank each of them and these agencies for their efforts on behalf of our veterans.

The three national credit card bureaus have established special procedures to handle inquiries and requests for fraud alerts from veterans. Experian and TransUnion have placed a front-end message on their existing toll-free fraud lines, bypassing the usual phone tree with instructions for placing a fraud alert. Equifax has set up a new toll-free number for veterans to place fraud alerts.

The new procedures became operational on Tuesday. The bureaus report a spike in phone calls, 171 percent of normal, and in

requests for free credit report through the annual free credit report web site.

The Federal Trade Commission also experienced high call volumes about the incident earlier this week.

On Monday, the Office of Comptroller of the Currency notified its examiners of this theft. On Tuesday, the Office of Comptroller posted an advisory on an Internet network available to its banks and instructed the examiners to direct their banks to the advisory. It explains what happened and asks the banks to exercise extra diligence in processing veterans' payments. The advisory also reminds banks of their legal obligations to verify the identities of persons seeking to open new accounts and to safeguard customer information against unauthorized access or use and attaches a summary of relevant regulations.

I briefed the Attorney General and the Chairman of the Federal Trade Commission, the co-chairs of the President's Identity Theft Task Force, shortly after I became aware of this occurrence. They have been very cooperative. Task Force members have already taken actions to protect the affected workers, including—excuse me, to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive free credit reports that they are entitled to.

Additionally, the Task Force met on Monday to coordinate the comprehensive Federal response to recommend further ways to protect affected veterans and increase safeguards to prevent the recurrence of such incidents. On Monday following the announcement of this incident, I also issued a memorandum to all VA employees. The purpose was to remind them of the public trust that we hold and to set forth the requirements that all employees complete their annual general privacy training and cyber security for this current year by the end of next month.

Following that, all will be required to sign a statement of commitment and understanding which will acknowledge the consequences for noncompliance.

Information security is challenging business and ultimately it depends on the integrity and the ethics of the workforce. As has been said here, as technology has advanced, it has become possible to store vast quantities of data on devices no larger than one's thumbnail.

All of us carry a cell phone, a BlackBerry or a personal digital assistant, and each of these contains vast quantities of data. Someone intent on taking this data and using it inappropriately has many opportunities to do that.

It is also the fact that great numbers of people in this agency and in this Government telecommute. For example, yesterday I was talking to an employee of ours who is an information technology specialist. And he told me of needing some medical records. He asked for them to be burned onto a CD, and that was done and it was delivered to him very promptly and neatly.

And so he wrote the person an e-mail back saying thank you for this prompt, efficient work. He said, "By the way, where do you work here in the central office? Maybe we could have a cup of coffee some time." And the person responded by saying, "I do not work in the central office. I work in South Dakota."

It illustrates how far-flung and distended some of this has gotten. We need obviously to know who they are, know what kind of people they are out there with this data, and absolutely get better control over it.

And I promise you that we are going to do everything in our power to structure a regime at the VA that makes clear what is proper in the use of data by our employees and train our employees in those policies and enforce them.

We have already begun discussions regarding the immediate automatic encryption of all sensitive information. We will also work with the President's Task Force on Identity Theft. I am a member of the Task Force. And it will help to structure policies that will be put in place throughout the Government to help ensure that situations such as this do not occur at other agencies.

In summary, Mr. Chairman and Members of the Committees, I want to say that the VA's mission is to serve and honor our Nation's veterans, and we take it very seriously. I am also proud to say that most of the 235,000 people that work there are terrific and take it seriously and are dedicated to our veterans. So, I am so saddened by what has happened here, in this case by one person, and the anxiety and concern that this is causing to our veterans and our families because they have enough to deal with.

We honor the service of our veterans and we consider it a privilege to work for them at our agency. I want you and them to know that we are and are going to work hard to keep this most awful thing from happening again.

Thank you.

[The prepared statement of R. James Nicholson follows:]

PREPARED STATEMENT OF HON. R. JAMES NICHOLSON, SECRETARY, DEPARTMENT OF VETERANS AFFAIRS

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today to explain a devastating situation.

A VA employee, a data analyst, took home electronic data files from VA. He was not authorized to do so.

These data contained identifying information including names and dates of birth for up to 26.5 million veterans and some of their spouses. In addition, that information, plus social security numbers, was available for some 19.6 million of those veterans. Also possibly included were some numerical disability ratings and the diagnostic codes which identify the disabilities being compensated.

It is important to note that the data did not include any of VA's electronic health records. Neither did it contain explicit financial information, although knowing of a disability rating could enable one to compute what that implied in terms of compensation payments.

On May 3, the employee's home was broken into in what appears to local law enforcement to have been a routine breaking and entering, and the VA data were stolen. The employee has been placed on administrative leave pending the outcome of an investigation with which I understand he is cooperating.

I am outraged at the loss of this veterans' data and the fact an employee would put it at risk by taking it home in violation of VA policies. However, the employee promptly reported the theft to the local police and to the Department of Veterans Affairs. But it was not until May 16th that I was notified. I am gravely concerned about the timing of the Department's response once the burglary became known. I will not tolerate inaction and poor judgment when it comes to protecting our veterans.

Appropriate law enforcement agencies, including local police, the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. It is possible that the thieves remain un-

aware of the information they possess or of how to make use of it. Because of that, we have attempted to describe the equipment stolen, the location from which it was stolen and other information in very general terms. We do not want to provide information to the thieves that might be informative as to the nature of what they have stolen. We still hope that this was a common theft, and that no use will be made of the VA data.

From the moment I was informed, VA began taking all possible steps to protect and inform our veterans.

In our post-disclosure assessment, we have seen the gaps between what we said and the way we are seen.

VA has begun a top to bottom examination of our business, policies, and procedures to find out how we can prevent something like this from happening again. We will stay focused on the problems until they are fixed. In addition, we will take direct and immediate action to address and alleviate veterans' concerns and to regain their confidence.

I have taken the following actions so far:

• I have directed all VA employees to complete the annual "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by June 30, 2006.

This includes:

• The Privacy Act;

• Unauthorized disclosing or using, directly or indirectly, information obtained as a result of employment in VA, which is of a confidential nature or which represents a matter of trust, or other information so obtained of such a character that its disclosure or use would be contrary to the best interests of the VA or veterans being served by it; and,

• Loss of, damage to, or unauthorized use of Government property, through carelessness or negligence, or through maliciousness or intent.

• I have also directed that all VA employees sign annually an Employee Statement of Commitment and Understanding which will also acknowledge consequences for non compliance.

In addition the Department will immediately begin to conduct an inventory and review of all current positions requiring access to sensitive VA data. The inventory will determine whether positions in fact require such access. We will then require all employees who need access to sensitive VA data to do their jobs to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required and the responsibilities associated with their position.

And I have directed the Office of Information & Technology to publish, as a VA Directive, the revisions to the Security Guidelines for Single-User Remote Access developed by the Office of Cyber and Information Security. I have asked that this be done by June 30, 2006. This document will set the standards for access, use, and information security, including physical security, incident reporting and responsibilities.

VA is working with Members of Congress, the news media, veterans' service organizations, and numerous government agencies to help ensure that those veterans and their families are aware of the situation and of the steps they may take to protect themselves from misuse of personal information.

VA is coordinating with other agencies to send individual notifications to those individuals whose social security numbers were stolen, instructing them to be vigilant in order to detect any signs of possible identity theft and telling them how to protect themselves. In the meantime, veterans can also go to *www.firstgov.gov* for more information in this matter. This is a Federal Government Web site capable of handling large amounts of web traffic.

Additionally, working with other government agencies, VA has set up a manned call center that veterans may use to get information about this situation and learn more about consumer-identity protections. That toll free number is 1-800-FED INFO (333-4636). The call center is operating from 8 am to 9 pm (EDT), Monday–Saturday as long as it is needed. The call center is able to handle up to 20,000 calls per hour (260,000 calls per day). Through the end of the day on Tuesday, concerned veterans had made a total of 105,753 calls to this number.

I want to acknowledge the significant efforts of numerous government agencies in assisting VA to prepare for our announcement on May 22nd. Agencies at all levels of the Federal Government pitched in to ensure that our veterans had information on actions they could take to protect their credit. Hundreds of people worked around the clock writing materials to inform the veterans and setting up call centers and a website to ensure maximum dissemination of the information. I want to personally

thank each of those agencies and those individuals for their selfless efforts on behalf of our veterans.

The three nationwide credit bureaus have established special procedures to handle inquiries and requests for fraud alerts from veterans.

Experian and TransUnion have placed a front-end message on their existing toll-free fraud lines, bypassing the usual phone tree, with instructions for placing a fraud alert. Equifax has set up a new toll-free number for veterans to place fraud alerts. The new Equifax number is 1-877-576-5734. The new procedures became operational on Tuesday. The bureaus report a spike in phone calls (171 percent of normal) and in requests for free credit reports through the annual free credit report web site (annualcreditreport.com). The Federal Trade Commission also experienced high call volumes about the incident earlier this week.

On Monday, the Office of Comptroller of the Currency notified its examiners of the theft. On Tuesday, OCC posted an advisory on an internal network available to its banks and instructed the examiners to direct their banks to the advisory. It explains what happened and asks the banks to exercise extra diligence in processing veterans' payments. The advisory also reminds the banks of their legal obligations to verify the identities of persons seeking to open new accounts and to safeguard customer information against unauthorized access or use. It also includes a summary of relevant laws and regulations.

I briefed the Attorney General and the Chairman of the Federal Trade Commission, co-chairs of the President's Identity Theft Task Force, shortly after I became aware of this occurrence.

Task Force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report they are entitled to under the law. Additionally, the Task Force met on Monday to coordinate the comprehensive Federal response, recommend further ways to protect affected veterans, and increase safeguards to prevent the recurrence of such incidents.

On Monday, following the announcement of this incident, I also issued a memorandum to all VA employees. The purpose was to remind them of the public trust we hold and to set forth the requirement that all employees complete their annual General Privacy Training and VA Cyber Security Awareness training for the current year by June 30.

As technology has advanced, it has become possible to store vast quantities of data on devices no larger than one's thumb. All of us carry a cell phone, a BlackBerry or a Personal Digital Assistant, and each of these contains vast quantities of data. Someone intent on taking such data and using it inappropriately would have many opportunities to do that.

I can promise you that we will do everything in our power to make clear what is appropriate and inappropriate use of data by our employees. We will train employees in those policies, and we will enforce them. We have already begun discussions regarding the immediate automatic encryption of all sensitive information.

We will also work with the President's Task Force on Identity Theft, of which I am a member, to help structure policies that will be put in place throughout the government to ensure that situations such as this do not occur at other agencies.

VA's mission to serve and honor our Nation's veterans is one we take very seriously and the 235,000 VA employees are deeply saddened by any concern or anxiety this incident may cause to those veterans and their families. We honor the service our veterans have given their country and we are working diligently to protect them from any harm as a result of this incident.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. AKAKA TO HON. R. JAMES NICHOLSON

On February 11, 2005, Office of Management and Budget (OMB) Deputy Director for Management Clay Johnson issued a memorandum directing each agency to designate a senior official who would have agency-wide responsibility for privacy issues relative to information management.

Question 1a. Who is VA's senior privacy official? When was this position established at VA?

Question 1b. What training does VA's designated privacy official receive? Is this training then passed on to all agency personnel? Please provide a copy of the training documents VA provides its employees.

Question 1c. I understand that OMB meets with all the agencies' senior privacy officials and their teams to review the status of the agencies' privacy programs. Has OMB met with VA's privacy official, and if so, do you know what OMB found with

respect to VA's privacy program? If problems were found, how has VA addressed the problems identified? Are the problems identified by OMB still remain at VA?

Question 1d. If the privacy official has a concern about an agency practice or program, what enforcement authority does he or she have? To whom does the senior privacy official report?

Question 1e. What is the working relationship between the VA privacy official and Privacy and Civil Liberties Oversight Board?

Question 2. Recently VA announced the naming of Special Advisor for Information Security. What will be the role and responsibilities of the Special Advisor? How will the responsibilities and duties of this official differ from those assigned to the senior privacy official? How will this individual work with the senior official designated for privacy issues and the Chief Information Officer at VA?

Question 3. The Privacy Act does not require the VA to provide notice of a data breach. What Federal or state law required the VA to notify the public of the data breach?

Response. VA did not respond to the questions.

WRITTEN QUESTIONS SUBMITTED BY HON. NORM COLEMAN TO HON. R. JAMES NICHOLSON

The senior VA employee who took the sensitive information home was working on a project which involved improving telephone interactions between the Department and Veterans. While the employee was authorized to have access to this data in connection with the project, the employee was not authorized to take the data home to work on it. Although the employee received the required training on protecting the privacy and security of this kind of information and knew it was against VA policy, the employee still chose to take it home.

Question 1a. How confident are you that other VA employees do not similarly have confidential data in their homes? Can we be 100 percent confident?

Question 1b. Would you say it is routine for employees who have access to sensitive information to remove it from the VA to work on at home? Is it easy to remove this information?

Question 1c. Is there any way for you to know how many employees remove sensitive information from the VA?

Question 1d. Are employees aware of the penalties for removing sensitive information from the VA? Can you tell us what the penalties are?

Mr. Secretary, you found out about the security breech on May 16th, yet veterans were not informed until May 22nd. On May 19th, the Inspector General and your staff decided not to go public because the hotline being established by the FTC to handle veterans' calls had not been fully set up. However, when this type of security breech has happened in the private sector, consumers have been alerted very quickly, often in less than 24 hours.

Question 2a. Do you still think it was the right decision to wait to inform veterans that their information may have been compromised?

Question 2b. What would have been the downside to making an announcement so veterans could begin reviewing their financial information while putting information on your website and saying a call center would be up and running in a few days?

Question 2c. Are you getting any feedback on whether the call centers are helpful? Is the VA partnering with the Veterans Service Organizations to provide information to their members about what happened and what they can do to protect this information?

On May 3rd, the same day as the discovery of the burglary and theft, the VA employee called and reported to a supervisor and VA security officials the loss of sensitive privacy data. However, Mr. Secretary, you did not find out until almost 2 weeks later on May 16th.

Question 3a. Do you recall your reaction when you found out about this?

Question 3b. Did you inquire why something of this magnitude took almost 2 weeks to reach your desk?

Question 3c. When did you become aware that your Chief of Staff knew this information a week earlier?

Question 3d. Do you know why you were not told at that time of what had happened?

Question 3e. Is it customary for important matters such as this to be caught up in bureaucracy for 2 weeks or is there a system in place to get things to you quicker? If so, do you know why this information did not get to you sooner?

Since 2001, the VA Inspector General has warned that access controls were a "material weakness" in the department's security of information. Vulnerabilities cited included operating systems, passwords, and a lack of strong detection alerts. While this case involved a VA employee with authorized access to sensitive information, I am concerned the VA is also vulnerable to a cyber-attacker without authorized access that breaks into the system and removes sensitive information.

Question 4a. Mr. Secretary, how vulnerable is the VA to a cyber-attack from someone outside of the VA who has no authorization to any VA information?

Question 4b. Were you aware of the VA Inspector General's reports that were critical of the department's information protection systems?

Question 4c. What actions has the department taken to improve information security since you became Secretary in February, 2005?

Response. VA did not respond to the questions.

WRITTEN QUESTIONS SUBMITTED BY HON. PETE V. DOMENICI TO HON. R. JAMES NICHOLSON

Question 1. In recent years identity theft has become a major issue in this country. Given that the theft of personal information is nothing new, what policies and procedures did the Department of Veterans Affairs have in place prior to this incident to insure the personal data of our Nation's veterans was protected?

Question 2. It is my understanding that to date there is no evidence anyone has illegally used the missing data belonging to 26.5 million of our Nation's veterans including names, social security numbers, and dates of birth. However, I am particularly concerned for those veterans who are retired or nearing retirement and who may be on a fixed income and therefore less able to respond to the consequences of identity theft. How is the VA preparing to minimize the disturbance to their lives in the event this stolen information is improperly used? Furthermore, what steps has the VA taken to notify the 26.5 million veteran's involved in this incident?

Question 3. In light of this loss of information, I think it is clear the Department of Veterans Affairs must take steps to better protect sensitive personal data in the future. At this time, what changes has the VA implemented or plans to implement to insure veterans do not have to face the fear of their personal information being misused in the future?

Response. VA did not respond to the questions.

WRITTEN QUESTIONS SUBMITTED BY HON. LINCOLN D. CHAFEE TO HON. R. JAMES NICHOLSON

Question 1. Members of our military have risked their lives in service of our country. Our grateful Nation fully supports veterans programs, including medical, educational, employment, and other assistance. I too support these important programs. In all times, and especially in a time of war, ensuring our veterans receive the best medical care is our Nation's duty. Earlier this year, in his budget request, the President proposed higher fees and co-pays for certain veterans receiving VA assistance. In my view, a policy that leads to increased denial of service to veterans is simply unacceptable, which is why I cosponsored an amendment to the Budget allocating money for the government to cover these costs. Secretary Nicholson, what are you doing to make sure quality VA care remains accessible to all veterans who need it?

Question 2. Battlefield medicine has made huge strides in the last few decades. The result has been a much higher percentage of wounded soldiers living through their initial injuries, able to return home to their families. These wonderful advances in medicine deserve our praise, but they mean that the VA will be caring for more and more injured soldiers as they return home. Many of these injuries, such as burns, amputations, blindness, and PTSD, are of the type that will require care for a lifetime. How is the VA preparing for an increase in the number of veterans who will require long term medical assistance? Furthermore, how is the VA making sure it immediately cares for returning Iraq War veterans, but does not forget about those older veterans who continue to require medical assistance?

Response. VA did not respond to the questions.

Chairman CRAIG. Mr. Secretary, thank you very much.

As you have noted, the Secretary is accompanied by Tim McClain, who is General Counsel for the Department of Veterans Affairs.

You will notice there are two empty chairs. George Opfer, Inspector General for the Department of Veterans Affairs, I do not know if he was held hostage. At least he was detained in the U.S. House of Representatives. And I understand he is en route or nearly here. So the moment he arrives, we will allow him to make his statement before we go to questions. In the meantime, I will ask the Secretary a question.

Mr. Secretary, you have mentioned, as many of our colleagues here have mentioned, that there has been a long history of Inspector General review and litany recommending greatly improved informational technology security at VA. In fact, a grade of "F" and the word flunk have been used.

I do not know if this is the ultimate wake-up call, but it most assuredly appears to be.

Does VA have some legitimate reason why it ignored IT security recommendations from the IG for 4 years running?

Now I know your watch has not been during all of those periods of time. But I am greatly concerned that it took something like this to begin to unravel the rigidity of a bureaucracy that would deny the legitimate approach of an overall encompassing IT system that now we must get at the business of doing.

Your reaction.

Secretary NICHOLSON. My reaction, Mr. Chairman, is that there is no excuse for this. I have been there 15 months and I am aware of those previous years' reports and the assessment that we got. We did launch this significant change in the way that we are going to do IT business by pulling it back and centralizing it, which would give us considerably more control and accountability. But that is just in the launch phase.

I also have discovered that there have been directives that have been issued by my predecessor to which there has been no attention given. There are directives that have come out which are called guidelines, which some employees do not interpret as being mandatory or operative to them, because they are a guideline. I have had that discussion just yesterday with some employees in that respect.

So the whole thing needs to really be tightened up. We are on that path, I will say, and give the recently departed CIO credit for getting us there. But it is nascent, just starting.

Chairman CRAIG. Mr. Opfer, we appreciate your being able to make it.

We will allow you to sit down and take a deep breath, and we would ask that you—the Secretary has just completed his statement and we were just starting into a round of questions. But we want you to make your statements so that the questions of my colleagues can be directed to either of you.

You are accompanied by Jon Wooditch is that correct?

Mr. OPFER. Yes, sir.

Chairman CRAIG. Deputy Inspector General, Department of Veterans Affairs.

So Mr. Inspector General, please proceed with your statement, if you would, please.

STATEMENT OF HON. GEORGE J. OPFER, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY JON A. WOODITCH, DEPUTY INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS

Mr. OPFER. Thank you, Mr. Chairman and Members of the Committee. Thank you for the opportunity to testify today on the loss of VA sensitive data.

I am prepared to give a short statement and request that my full statement be submitted for the record.

Chairman CRAIG. Without objection, it will.

Mr. OPFER. I am accompanied, as you said, Mr. Chairman, by Jon Wooditch, the Deputy Inspector General, and Mike Stanley, the Assistant Inspector General for Audits.

My statement will focus on the incident involving a VA employee who took home sensitive data and confidential information which was stolen from the employee's home when it was burglarized.

Our involvement in this matter from the IG perspective is threefold. One, an ongoing criminal investigation into the theft of the data. Two, an administrative investigation. And three, a review of the VA policies and procedures for using and protecting privacy data.

In addition to discussing each of these reviews, my statement will also provide an overview of the OIG reports that have shown the need for continued improvements in addressing information security weaknesses in VA and the status of those OIG recommendations for corrective action.

On May 3rd, the home of a VA employee was burglarized. According to the employee, information stolen included the names, birth dates and Social Security numbers of approximately 26.5 million veterans that was stored on his personally owned computer hardware. The employee said that he routinely took sensitive data home to work on and has been doing so since 2003.

On Wednesday, May 10th, an Information Security Officer of the OIG, while attending a routine meeting at VA, heard that a VA employee's home had been burglarized and that VA electronic records may have been stolen. Following the meeting, the OIG employee gathered additional facts about the incident. On the following day, he submitted a written report to alert the Office of Investigations of the Office of Inspector General.

On May 12th, the OIG opened a criminal investigation and initiated efforts to locate and interview the employee and those others that had information regarding the theft of the sensitive data.

On May 15th, we interviewed the employee. The employee advised us that he believed several electronic files containing veteran information stored on his personally owned computer hardware had been stolen during a burglary. He thought that stolen information included the names, birth dates and Social Security numbers of approximately 26.5 million veterans.

On May 16th, we met with the Montgomery County Police Department, who had initiated an investigation of the burglary. We informed the Montgomery County Police Department of the suspected loss of millions of veterans' personal identifiers. We learned that the detectives were actively pursuing leads developed in a number of recent burglaries in the employee's neighborhood.

On May 17th, we advised the FBI and the Assistant United States Attorney of the details of the burglary and the possible loss of the data. On the next day, we also faxed a letter listing these details to the FBI.

Since then we have been conducting a joint investigation focused on the recovery of the stolen data. To date, we have received no indication or information that the data has been further compromised.

In the administrative investigation, our investigation will determine if notifications of the incident were made, and if those notifications were pursued in an appropriate and timely manner. We are developing a chronology of when key staff and managers were informed of the incident, what information was conveyed to these individuals, and what actions they took.

As part of the investigation, we will determine if the work the employee was performing at home was related to his official duties and if he had appropriate authorization to take individually identifiable data to his residence. We will also determine if the employee complied with relevant policies and procedures.

The recent incident also raises concerns about whether VA has adequate policies and procedures in place to protect confidential and privileged information maintained in VA electronic databases. To address this issue, we have initiated a review to determine whether VA has effective policies to ensure compliance, whether VA employees are aware of these policies, and whether there is an effective mechanism for reporting violations and taking appropriate actions.

The review will identify strengths and weaknesses in VA policies. We will make recommendations for improvement to ensure the data maintained by VA is protected from unwanted intrusion and disclosure.

In closing, I would like to assure the Committee that this matter will remain the highest priority in the OIG until it is resolved. I will assure you that all of the resources that we have that are needed to complete our reviews in a thorough and timely matter will be dedicated to the goal of recovering the stolen data and protecting the Nation's veterans.

Mr. Chairman and Members of the Committee, thank you again for the opportunity to appear and to answer any questions.

PREPARED STATEMENT OF HON. GEORGE J. OPFER, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS

INTRODUCTION

Mr. Chairman, Madam Chairman, and Members of the Committees, thank you for the opportunity to testify today on the loss of Department of Veterans Affairs (VA) sensitive data. I am accompanied by Jon Wooditch, Deputy Inspector General, and Mike Staley, Assistant Inspector General for Auditing. My statement will focus on the incident involving a VA employee who took home sensitive and confidential information, which was stolen when the employee's home was burglarized. The Office of Inspector General's (OIG) involvement in this matter involves a three-pronged approach including (1) a criminal investigation, (2) an administrative investigation of the handling of this matter once reported to the Department, and (3) a review of VA policies and procedures for using and protecting privacy data. In addition to discussing each of these reviews, I will also provide an overview of the OIG reports that have shown the need for continued improvements in addressing information security weaknesses in VA, and the status of OIG recommendations for corrective action.

On May 3, 2006, the home of a VA employee was burglarized. According to the employee, the information stolen included the names, birthdates, and social security numbers of approximately 26.5 million veterans that was stored on personally owned computer hardware. The employee, a data analyst, was authorized access to sensitive VA information in the performance of his duties and responsibilities. He said that he routinely took such data home to work on it, and had been doing so since 2003.

CRIMINAL INVESTIGATION

On Wednesday, May 10, 2006, our Information Security Officer (ISO), while attending a routine meeting at VA Central Office, heard another ISO mention that a VA employee's home had been burglarized and that VA electronic records may have been stolen. Following the meeting, our ISO gathered additional facts about this incident. On the following day, he submitted a written report to his supervisor for the purpose of alerting our Office of Investigations. On May 12, 2006, a criminal investigation was initiated and efforts commenced to identify and interview the employee.

On Monday, May 15, 2006, we interviewed the employee. The employee advised us that he believed that several electronic files containing veteran information stored on personally owned computer hardware had been stolen during the burglary at his home on May 3, 2006. He thought the stolen information included the names, birthdates, and social security numbers of approximately 26.5 million veterans.

On May 16, 2006, we met with the Montgomery County Police Department who had initiated an investigation of the burglary when notified on May 3, 2006. We informed them of the suspected loss of millions of veterans' personal identifiers. We learned that detectives were actively pursuing leads developed in a number of recent residential burglaries in the employee's neighborhood.

On May 17, 2006, we apprised the Federal Bureau of Investigation (FBI) and an Assistant United States Attorney of the details of this burglary and possible loss of data. The next day, we also faxed a letter listing these details to the FBI. Since then, we have been conducting a joint investigation with the FBI and the Montgomery County Police Department focused on the recovery of the stolen data. To date, there has been no indication that this data has been further compromised.

ADMINISTRATIVE INVESTIGATION

We have also initiated an administrative investigation to determine if notifications of the incident were made, and if those notifications were pursued in an appropriate and timely manner. We are developing a chronology of when key staff and managers were informed of the incident, what information was conveyed to these individuals, and what actions they took. We are also identifying what VA electronic data the employee stored at his home, whether the employee had an official need for the data, why he took it to his home, and who in his supervisory chain approved or had knowledge that he had done so.

We have interviewed the employee, his supervisors, project managers, and coworkers; privacy, information security, and VA law enforcement officials; Office of General Counsel attorneys, including the General Counsel; and the VA Chief of Staff. We are also reviewing electronic mail messages pertinent to the incident; notes and memoranda prepared by the employee, General Counsel, and other staff; documentation of the employee's access to VA databases; and other pertinent documentation.

According to the employee, he likely had VA electronic data stolen during the burglary of his residence, but he was not certain of the type and extent of the specific information taken. He said he believed it contained approximately 26.5 million veterans' names, social security numbers, and dates of birth, extracted from a VA database, and possibly other smaller files containing information about individual veterans was also taken. We are currently reviewing the computer discs he used to take data home to determine what other information may have been stolen.

The employee, a data analyst, had an official need to access the records believed to have been stolen. The nature of his work was project-focused and involved manipulating large quantities of data to address certain policy issues. The employee told us he took the data home for work-related purposes. However, none of his supervisors we talked to said they were aware that the employee had taken the file containing approximately 26.5 million veterans' records to his residence.

As part of our investigation, we will determine if the work the employee was performing at home was related to his official duties, and if he had appropriate authorization to take individually identifiable data to his residence. We will also determine if the employee complied with relevant policies and procedures in taking this infor-

mation home and properly protecting it. Our report will identify what breakdowns occurred that may have hindered timely notification and follow-up of this incident. Based on our investigation, we will make recommendations for appropriate action, if warranted.

REVIEW OF LAWS, REGULATIONS, AND VA POLICIES AND PROCEDURES ON SAFEGUARDING CONFIDENTIAL INFORMATION

The recent incident raised concerns about whether the VA has adequate policies and procedures in place to protect confidential and privileged information maintained in VA's electronic databases. Our concerns are whether VA policies are adequate to ensure compliance with information security laws, the Privacy Act and other confidentiality laws and regulations, and to identify and take action when there is a violation of law or policy. There are two sets of laws and implementing regulations to protect the integrity of confidential data—computer security laws and confidentiality statutes. While the intent of both sets of laws is the same—the protection of information—the approach is different. Computer security laws ensure that the system infrastructure on which the data is maintained electronically is protected against unauthorized intrusions such as viruses and unapproved access. The Privacy Act and other confidentiality laws and regulations protect information by limiting access, use, and disclosure of records without authorization from the individual about whom the record is maintained.

To address the issues, we initiated a review to determine whether VA has effective policies in place to ensure compliance with computer security laws, the Privacy Act and other confidentiality laws and regulations, whether VA employees are aware of the policies; whether VA has adequate procedures in place to monitor compliance with the policies; and, whether the policies include an effective mechanism for reporting violations and taking appropriate action. Two areas that we are addressing in our review are policies relating to the transfer of electronic information from an employee's VA computer to his home or alternative work site and the impact centralization versus decentralization of VA policy has on ensuring that the integrity of VA computer systems and the information stored on those systems is maintained.

The review includes identifying and reviewing applicable laws, regulations and policies, including Department-wide policies; policies issues by the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and other VA entities, policies issued by local VA facilities; and mandatory training modules. We are also reviewing how policies are disseminated to VA employees; whether VA employees are aware of the policies, and whether VA procedures for identifying, reporting and taking action when data has been improperly accessed or improperly used are adequate.

This review will identify strengths and weaknesses in VA's policies implementing the provisions of computer security laws and the Privacy Act, and other confidentiality laws. We will also identify strengths and weaknesses in ensuring that VA employees are knowledgeable regarding their obligation to protect VA computer systems and information and that they will be held accountable for violations. We will make recommendations for improvement to ensure that data maintained by VA is protected from unwarranted intrusion and disclosure.

SUMMARY OF OIG REPORTS ADDRESSING INFORMATION SECURITY WEAKNESSES

We have conducted a number of audits and evaluations on information management security and information technology (IT) systems that have shown the need for continued improvements in addressing security weaknesses. My office has reported VA information security controls as a material weakness in its annual Consolidated Financial Statement (CFS) audits since before fiscal year (FY) 2001. Our Federal Information Security Management Act (FISMA) reviews have identified significant information security vulnerabilities since fiscal year 2001 that place VA at risk of denial of service attacks, disruption of mission-critical systems, and unauthorized access to sensitive data. We continue to report security weaknesses and vulnerabilities at VA health care facilities and VA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews.

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

Pursuant to the Chief Financial Officers Act of 1990, the VA consolidated financial statements are audited annually. We contract with an independent public accounting firm to perform this audit. As part of the audit, the contractor follows Government Accountability Office methodology to assess the effectiveness of computer

controls. The contractor conducts audits at VA's three information technology centers and selected regional offices and medical centers.

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

As a result of these weaknesses, we made recommendations that VA pursue a more centralized approach, apply appropriate resources, and establish a clear chain of command and accountability structure to implement and enforce IT internal controls. We also recommended that VA improve access control policies and procedures for configuring security settings on operating systems, improve administration of user access, and detect and resolve potential access violations. Finally, we recommended that VA conform access privileges to the user's level of responsibility and position.

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

Evaluations of VA's Information Security Program Have Identified Serious Vulnerabilities for Several Years That Remain Uncorrected

FISMA requires us to annually review the progress of the information technology and security program of the Department and report the results to the Office of Management and Budget. As part of the FISMA review, we conduct scanning and penetration tests of selected VA systems to assess controls for monitoring and accessing systems, and reviews of physical, personnel, and electronic security. We visit all three major IT centers and selected VHA and VBA sites.

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

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

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

wireless devices, and (16) electronic transmission of sensitive veteran data. As of May 23, 2006, all recommendations from this report remain open.

Finally, in fiscal year 2006, after Congress mandated full centralization of IT security under the CIO, as we advocated in our reports since 2001, VA is now moving out on a truly empowered centralized CIO. We have provided our draft fiscal year 2005 audit report to the Department and are working with the Department to resolve all outstanding recommendations. We have grouped our recommendations into two categories—the CIO's authority under centralization and longstanding vulnerabilities. With a centralized CIO with direct line authority to implement the needed fixes, we believe VA has a unique opportunity to successfully address all the vulnerabilities and weaknesses discussed in our reports since 2001.

We believe centralization is essential because standardization is the key to fixing VA information security weaknesses. As long as three stove-piped administrations and other smaller component organizations are free to operate in the IT environment on their own within VA—accountable not to the CIO but to other line managers who themselves are not accountable to the VA CIO—the vulnerabilities cannot be effectively resolved.

CAP Reviews Continue To Show Information System Security Vulnerabilities Continue To Exist

We continue to identify instances where out-based employees send veteran medical information to the VA regional office via unencrypted e-mail; system access for separated employees is not terminated; monitoring remote network access and usage does not routinely occur; and off duty users' access to VA computer systems and sensitive information is not restricted. We continue to make recommendations to improve security and contingency plans, control access to information systems, complete background investigations and annual security awareness training, and improve physical security controls.

While individual and regional managers have concurred with these CAP recommendations, and our follow-up process confirms actions to resolve the specific conditions identified at these sites, we continue to find that corrective actions are not applied to all facilities to correct conditions nationwide. Consequently, we continue to find these systemic conditions at other sites we visit. For example, between FYs 2000 to 2005 the CAP program identified IT and security deficiencies in 141 of 181 VHA facilities. We identified IT and security deficiencies at 37 of 55 VBA facilities.

CLOSING

In closing, I would like to assure the Committee that this matter will remain a very high priority for the OIG until it is resolved. I will ensure that all the resources that are needed to complete our reviews in a thorough and timely manner will remain dedicated to the goal of recovering the stolen data and protecting our Nation's veterans.

Mr. Chairman, Madam Chairman, and Members of the Committees, thank you again for this opportunity and I would be pleased to answer any questions that you may have.

Chairman CRAIG. Mr. Opfer, thank you for being here and thank you for that testimony.

Let me turn to Chairman Collins.

Susan.

Chairman COLLINS. Thank you, Mr. Chairman.

Mr. Secretary, first let me say to you that I do not doubt in any way your personal pain and your sense of outrage over what has happened. I know you are sincerely upset and that you are dedicated to remedying the problems.

The chronology that you gave us in your testimony is absolutely baffling. This was not a minor security breach. It involved personal information about 26 million veterans. And it is just inconceivable to me that there were such long delays in informing you personally and in informing the veterans who were affected.

The concern I have, however, with your testimony, is that you seem to be saying that it was just one employee. It was one employee who breached the trust of our Nation's veterans. But in fact,

it is not just one employee. You have a high risk vulnerable system that has been identified time and again as vulnerable.

I have a stack of just some of the reports from OMB, from the House, from the GAO, from the Inspector General's office. Over and over again, it is the same warning, the same conclusions, the same recommendations.

For example, in this 2003 annual audit by the IG, it states, "The security vulnerabilities identified represent an unacceptable level of risk." And then the IG goes on to make many recommendations.

But here is what is most startling to me. For almost every recommendation, there is a notation that says the following: "This is a repeat recommendation from the fiscal year 2001 and 2002 information security audit."

Similarly, a report by the IG just last year states,

> Our last four annual audits, as well as this year's, continue to show significant security vulnerabilities. We continue to find that the VA systems remain vulnerable to unauthorized access and misuse of sensitive information and data.

It seems to me that you and the leaders in your Department were on notice. Were you aware of these repeated audits and reports that identified such serious vulnerabilities?

Secretary NICHOLSON. Yes, I was, Senator Collins.

And as I said earlier, that is one of the compelling reasons that we have really taken the steps we did to centralize our systems, our information system, so that we have tighter central control over these. Because it has gotten very decentralized, very loose and undisciplined. We have really taken some very significant steps, and there is just a change. I mean, the reassignment of thousands of people, the rebudgeting, the creation of a career field for IT personnel at the VA, which had not existed.

But it is just underway. But it has taken, in response to this situation that was very evident, and other deficiencies that have existed there which are not germane things like business accounting, inventory control reports and so forth, that you get out of a centralized IT system that the VA has just gotten away from over the last couple of decades.

Chairman COLLINS. Mr. Opfer, are you satisfied with the response to your office's recommendations?

Mr. OPFER. Senator Collins, I have recently been appointed to the Inspector General since November. Jon Wooditch is the Deputy Inspector General, who also served as Acting IG, and has much more familiarity with the series of reports over the years. I am going to refer to Jon to respond to this.

Chairman COLLINS. Mr. Wooditch.

Mr. WOODITCH. Thank you.

No, we have not been satisfied with the response in the past. As you mentioned, we have repeated these recommendations year in and year out. The IT system has been considered a material weakness in the Department for 5 straight years.se on.

In the last report that we put out, which was March 2005 of fiscal year 2004 activities, we listed 16 recommendations and many of those are repeat recommendations.

I would like to add that in Mr. Opfer's statement for the record, we do recognize that Congress took efforts this year to centralize

IT in the VA. We think that presents a very unique opportunity now for VA to address these recommendation.

Chairman COLLINS. Thank you, Mr. Chairman.

Chairman CRAIG. Thank you, Madame Chair.

Senator Akaka.

Senator AKAKA. Thank you very much, Mr. Chairman, Madame Chair.

Mr. Secretary, VA seems to believe that it is unlikely that the lost data will be used by the thief, and you mentioned that in your statement. Is that the judgment of law enforcement officials?

Secretary NICHOLSON. Senator Akaka, if I gave you that impression, I did not mean to, that we think it is unlikely. What I was trying to say was that we think it was unlikely that the burglary was committed to get after that data.

Senator AKAKA. Mr. Secretary, it is my understanding that typically VA will scramble Social Security numbers based upon an encryption formula. Access to files that translate scrambled Social Security numbers is only possible with special authorization. Realizing the sensitivity of this data that was burglarized, was this data not scrambled?

Secretary NICHOLSON. That is correct, Senator Akaka, it was not scrambled. There is a requirement for those who are authorized to take data home or to work with data at home that it should be encrypted, and this was not.

Senator AKAKA. Can you tell me, Mr. Secretary, what years of veterans this data covered? Does it date back to 1970 or 1960?

Secretary NICHOLSON. My understanding of it is that it is all veterans that were discharged from the services since 1975, plus veterans receiving disability compensation from our Department. The reason that we have that data is that there is a form that—I do not know if you remember—but when you are discharged the Department of Defense issues a form called a DD–214. And that is the record of your service, time, awards, so on.

And we, the VA, are an addressee on a copy of that for everybody that gets discharged. All of these veterans in this file are not receiving benefits from the VA, but we have them in our data file.

Senator AKAKA. I am asking that just so that veterans out there realize if they were discharged before that date, that their records were not in this 26.5 million data. Thank you.

Mr. Opfer, can you reveal anything more about the criminal investigation that would comfort the Nation's veterans that the employee and the data were not targeted?

Mr. OPFER. Yes, Senator Akaka, without compromising the investigation, I can say that the evidence to date indicates that the perpetrators of the burglary were specifically targeting computer hardware. There were a number of similar burglaries in the area where storage devices and computers, hardware, CDs, et cetera, were stolen. And it matches the similarity of a number of burglaries, including petty change, but very valuable items were left in the house. This fits the same pattern that Montgomery County Police have been seeing in a number of burglaries in the area.

Also, our investigators have interviewed the employee a number of times and have gone to his house. We recovered a number of

CDs and other equipment that contained VA sensitive data that was left in the house.

So appearing from the similarity of the burglaries, with other regular house burglaries, and the fact that VA data that we are able to secure was still there, we do not believe there was any information that has been developed by the Montgomery County Police, the Office of the Inspector General Investigators, or the Federal Bureau of Investigation that would indicate that that employee himself was targeted for the fact that he was in possession of that VA data.

Senator AKAKA. The Secretary did mention that it appeared this burglary was at random. What is your reading on that?

Mr. OPFER. From our conversations with the police and from my own experience, I have been in law enforcement since 1969, this fits the pattern that would be, that they would do some surveillance of residences to see when people come in and out, and if you work a routine. And this employee and his spouse were on a very regular routine. It fits the pattern of the burglaries in that area.

So, I would say they kind of identified residents who would be vulnerable during certain periods of time and then committed those crimes.

Senator AKAKA. Thank you very much, Mr. Chairman.

Chairman CRAIG. Danny, thank you very much.

Senator Murray.

Senator MURRAY. Mr. Secretary, I am trying to reconcile the numbers here. You are talking about 26.5 million records compromised. We have about 25 million veterans who are alive in the U.S. today. Six million of them are enrolled in the VA. So I want to get something straight. Does the lost data include spouses of veterans that would account for those number misconceptions?

Secretary NICHOLSON. Senator Murray, some of the veterans on this list would be deceased, but would not have been expunged from the rolls, and that explains most of that.

There were, however, some spouses.

Senator MURRAY. Whose spouse has passed away and they are in the database?

Secretary NICHOLSON. Yes, I am told.

Senator MURRAY. That raises two questions. First of all, how are you doing outreach to all of these 26.5 million names, particularly—I mean, we have had a lot of press about veterans themselves. But I am certain that there are spouses out there who have no idea that their name is part of this.

I would like to know if we are getting outreach to them to notify them.

Secretary NICHOLSON. Well, we are doing all we can to get the message out the way we have, through the use of the media. And we are preparing a mailing that will go to everyone.

Senator MURRAY. To all 26.5 million names?

Secretary NICHOLSON. Yes, because we do not know those that have died.

Senator MURRAY. And the cost of that?

Secretary NICHOLSON. We are working on that. We are trying to buy envelopes right now, for example. There is not immediately available 26 million envelopes.

Senator MURRAY. What account are you taking that from?

Secretary NICHOLSON. We have been in and asked for reprogramming of some administrative money, and that was $25 million, which was to cover the mailing plus, the cost of the phone centers. The mailing itself, we think, will be in the range of $10 million to $11 million.

Senator MURRAY. That is significant in a very tight budget, so I am certain we will be hearing from you on the need for additional funds for the VA?

Secretary NICHOLSON. You will be hearing from us, I think on different levels, because I think we also have things we have to do for our veterans with respect to trying to find a monitoring system that is practical for watching over this for our veterans to try to alleviate the anxiety that they have about it, we have something in place to watch, working with the three major credit bureaus.

Senator MURRAY. I expect this will cost a great deal. I want to make sure that our veterans do not get a double whammy of not only losing their records, but then being denied services because costs are not covered. I want to make sure we are providing the additional dollars to cover this. So I hope we can hear from you soon.

Let me ask you, as well, are you reaching out to VSOs to help our veterans?

Secretary NICHOLSON. Yes, we are.

Senator MURRAY. And give them the training that they need to deal with this?

Secretary NICHOLSON. We have certainly been in communication with them. We have not initiated any training with them so far. We are trying to use them and they are cooperating to be a communicator.

Senator MURRAY. I would suggest we look at some kind of training for the VSOs. That is usually who the veterans call first. And they, I am positive, do not have some of the training they need to do that.

I would also like to ask how you are dealing with veterans who do not have access to the Internet, who do not know how to use the technology. Many of our older vets who struggle with this kind of information, how are we dealing with them?

Secretary NICHOLSON. I think that is a very important question. I have been talking about that myself. My father was a veteran. He did not know how to boot up a computer.

So we obviously have the phone banks in the mailing that we will be sending out. There will be other information that they can use and ways to communicate outside of the computer.

Senator MURRAY. Have you ever gotten your credit checked, as you suggest, on the VA Web site?

Secretary NICHOLSON. I have not, no.

Senator MURRAY. It is not easy to do. So I am hoping that you are looking at additional staff to be able to answer the questions and work their way through that. It is not the easiest system, particularly for anybody, but for our vets who are personally worried right now, as well.

Mr. Chairman, I also think we need to be very conscious that we are reaching out now to 26.5 million veterans. We have about 5

million who are using VA services now. We are essentially notifying 20-some million veterans that they are eligible for services. There will be the impact. We have a responsibility to make sure they get the services they need.

And I hope we are looking critically at the impact on our budget, not only for the outreach, the additional training, making sure everybody gets the information they need, but also on the impact to our VA budget as more veterans are notified that they do have access to services.

Chairman CRAIG. Senator, thank you for that concern. It is our concern. It is the Committee's concern. Obviously, by actions taken, it is the Secretary's concern.

We will monitor it closely as this progresses to make sure that the resources are available to outreach in the appropriate fashion.

You mentioned widows and it is obvious to me, I think and others, that there are widows on this list. This morning I was doing C–SPAN on this issue and the call-in and I got a call from a widow who was obviously very concerned that in some way her financial statements and records might have been compromised. So that certainly is a legitimacy to this kind of list and the size of the list involved.

Thank you.

Secretary NICHOLSON. Could I comment on that, Mr. Chairman?

Chairman CRAIG. Please.

Secretary NICHOLSON. My technical people just handed me a note that says that the only spouses on that file, we think right now, were the spouses in a file of people involved with mustard gas. And that involves a number of less than 100.

Senator MURRAY. Then the discrepancy between the 25 million veterans who are alive today and the 26.5 million records that you are talking about, that is 1.5 million people and only 100 are spouses. Who are these people?

Secretary NICHOLSON. They are probably deceased, Senator Murray, 1800 veterans die every day in our country.

Senator MURRAY. OK, and so does somebody else—I mean, I am assuming that their records can be used and compromised, as well. Are we notifying relatives or anybody else to be aware of that? I am not sure how this technically works, but it does raise concerns.

Secretary NICHOLSON. What we plan to do is to mail that entire list in the hopes that if there is an address and a survivor at that address, they will get that notice.

Senator MURRAY. If it goes to the person, it will be returned, I am assuming, so how would their families know?

Secretary NICHOLSON. That is a good question. We will have to look at that. Your concern being the use of the identity of a deceased veteran.

Senator MURRAY. Right.

Secretary NICHOLSON. That is a good question, and I cannot answer it right now. We will have to look at that.

Chairman CRAIG. Those are very legitimate questions.

I think as you are able to unravel this, Mr. Secretary, it becomes very important for all of us, and especially for you, to understand those kinds of nuances and details, and that that information flow go public. I have to think that is very important.

Thank you, Senator.

Senator Isakson.

Senator ISAKSON. Inspector Opfer, do the Inspectors General of the various agencies of the Federal Government ever meet together?

Mr. OPFER. Yes, all the Inspectors General of the agencies are members of what is called the President's Council on Integrity and Efficiency. We meet formally once a month. And the chairman of that is the Deputy Director for Management for OMB. And one of the Inspectors General is selected as the vice-chair. Then there are various committees of the PCIE, the Investigations Committee, Audit Committee, and Inspections, Evaluations, and Legislative.

Senator ISAKSON. I have two suggestions. One is it would seem to me the Secretary has outlined his disappointment at being notified 13 days after the fact, that we should immediately install in the various agencies of the Government a rule that any breach of secure information and data is to be immediately reported to the person in charge. And I am talking about the secretary of the agency. I am not talking about the Department.

Something like this should never go unknown by the boss. The Secretary, to his credit, accepted the blame, the buck stops here, and I appreciate his doing that. But I also acknowledge how tough it is to find out 13 days after the fact what you are going to have to take the blame for.

So I would suggest that you all talk about what ought to be a Governmentwide policy, if there is any other breach. All that takes is a policy change.

The second thing is that if, in fact, other agencies have information as accessible as the Secretary has described the information at the VA is, then I think the inspectors general need to make recommendations to the appropriate agency or authority, which is probably the Appropriations Committee of the U.S. House and Senate, as to what should immediately be done to put blocks and security on that information, so it cannot be accessed from the outside nor be portable enough to be taken out.

So I would just recommend you do that. That is important. We have inspectors general to hold us accountable, to find discrepancies, to point things out that we need to do. We have a situation here that clearly demonstrates that a couple of changes need to be made.

Any comments you have?

Mr. OPFER. Yes, Senator. Just on this issue alone, I have been contacted by a number of inspectors general of these various agencies themselves, and including some deputy secretaries of departments. So when we conclude our review, I would be willing to discuss that with them and the individual things.

In the normal process, I am a member of the Investigations Committee of the President's Council on Integrity and Efficiency and also the Inspection and Evaluation. We would make this available and make a presentation on to all of the inspectors general, including the officials of OMB at the PCIE meeting, as well as giving them the reports and briefing the appropriate members of the Appropriation Committee on both sides of the Hill and the Oversight Committees.

Senator ISAKSON. Mr. Secretary, this is really a comment. Having had my identification taken, and having been notified by the company that lost it or allowed it to get out, I am aware of what happens in the private sector. What happens is they provide a means of protection for a period of time in the event the theft of the information actually gets in the wrong hands and is accessed.

As you are investigating your cost to deal with the mailing and with the czar, or whatever else you do in the Department, I would suggest that you consider in the hopefully unlikely circumstance that if we find this information is accessed, we need to know how to deploy immediate security measures for these 26.5 million people and what that cost would be.

From talking with the Chairman yesterday, that type of product is available. And its cost, in the volume like this, is not as insurmountable as one might initially think.

So, I think as we are planning for how to prevent this from happening in the future, and we are budgeting for notification, there should be some investigation by the VA as to what we are going to do if the unlikely event happens and the information actually gets used inappropriately.

So, I would appreciate your thinking about that.

That is all I have, Mr. Chairman. Thank you, Mr. Chairman.

Chairman CRAIG. Johnny, thank you very much.

Senator Thune.

Senator THUNE. Thank you, Mr. Chairman. I appreciate that suggestion, as well as some of the others.

I think a lot of the questions that have been raised today are very good questions, particularly with respect to the short term, notifying veterans how the agency, the Department intends to do that, as well as it just seems like this was a tremendous breakdown in the chain of command when it came to reporting the incident, considering the magnitude of this breach. So, I think the suggestion that my colleague from Georgia made regarding the IG and how that is reported is a good one. And it seems to me, at least, there has got to be some change in that area, as well.

I am also concerned, obviously there are a lot of short-term implications to this and many of those have been raised and touched upon. I also am concerned about, as well, the long term. As has been noted already, many of the reports that have been done in the past by the IGs and other agencies of Government, watchdog and audit agencies, have suggested weaknesses and flaws in the IT system at the VA.

What I would like, Mr. Secretary, just to get you to comment on, is because one of the things that we have been talking about a lot up here is centralization of that function at the Department, rather than having these compartmentalized different databases out there that contain information on our veterans.

I know that recently here the VA CIO, Mr. McFarland, resigned because the VA was not moving fast enough on the IT organization. My understanding is, as well, that he was brought on board specifically because of his expertise as a former executive at Dell Computer, and was supposed to be an agent for change for the VA when it comes to reform of the IT programs.

At least the reports I have read suggest that he became frustrated beating his head against the wall of the bureaucracy at the VA and that, as a consequence, decided to leave. But I think it points to this broader question of IT management centralization and the privacy of the 26 million records that we are talking about today.

But could you just talk a little bit about the context of his departure and your view about whether or not the VA is moving quickly enough when it comes to adopting the federated model of IT management centralization?

Secretary NICHOLSON. I can, Senator.

It is hard to say what Bob McFarland is feeling when he is not here. I had lunch with him shortly before he left, and I think that he feels quite satisfied about what he achieved at the VA. The statement about his getting tired of bumping his head against the wall, I think he got tired of doing what he had to do to break through to get done what we were doing.

It did not become a totally adopted model that Mr. McFarland wanted because there is one exception in there, which is the developers of IT. These are the people that work to customize the applications of software for research going on at different hospitals and so on.

But short of that, he achieved everything he set out to do. So, I think he made a monumental contribution to the VA.

He wanted to get back and spend more time fishing. He thought he probably bumped enough heads and wrangled enough people doing what he got done, that maybe it was time for him to leave. I tried to talk him out of it.

The important thing though is what he is leaving behind, with respect to what is going on now. It gives us a chance to be very hopeful.

Now you ask me are we moving fast enough? I would say to that, no. I do not think anything, frankly, moves in the Government fast enough. Because there are both the embedded cultural resistances to this in the bureaucracy and there are a lot of regulations and laws that inhibit speed.

But having said that, I will say that something very important has happened, and that is that the institutional resistance that was there to this big change has gone away. Those leaders are now very supportive of this and are working honestly and harmoniously in getting this done.

But it involves the reclassification of thousands of people and the upheaval and anxiety that goes with that. As I said, I think I said, that it also will result in a new career field in the VA for information technology, which would give those people a chance to go up in their own field without having been piggybacked into IT from some other field that they came from. So it is a real advantage to them for that, as well.

We have a team of really young, bright IT people who have the responsibility for this implementation. And they are underway.

Senator THUNE. I appreciate that, and Mr. Chairman we have had this discussion. I hope that you can continue to push the pace. I know there is resistance to change in every agency of Government and bureaucracy. It is just human nature as much as anything

else. But the stakes in this debate are so high and the relative speed with which this transition has occurred seems to me to suggest that we are not doing enough.

I am glad to hear you say that the culture is changing, because I think that is important, too, to recognize that this is where we are going. And once you get over that hurdle, then how do we get there in the quickest, most efficient way possible.

But this incident obviously focuses a lot of light on the importance of that transition happening, particularly in light of many of the reports and suggestions and recommendation that have come previously that appear not to have been adhered to.

So, we are obviously all looking for not only trying to determine exactly what caused this breach, but also, more importantly now, what we must do to fix it. So I thank you, and Mr. Chairman I have another question, but I am out of time and I think we have a vote on. So I yield back the balance of my time.

Chairman CRAIG. We do have a vote underway.

Gentlemen, I do have a couple more questions. I think Senator Collins does. We will ask you, if you would please, we will be brief. We should be able to get you out of here within the next 15 or 20 minutes. I will run and vote and come back.

So we will ask the Committee to stand in recess until Senator Collins returns and then she can bring it to order.

Thank you.

[Recess.]

Chairman COLLINS [presiding]. The Committee will come back to order.

Mr. Secretary, I do expect some of our colleagues to return, in particular the Chairman. While we are waiting for that, I am going to proceed to a couple of additional questions that I have for you.

For the past 7 years, it is my understanding that the VA and the Department of Defense have been working to achieve the exchange of patient health information electronically. The goal is to have an interoperable electronic health record.

In addition, the Department of Veterans Affairs is working with the IRS and with the Social Security Administration on compiling and comparing some means test income data to ensure that non-service connected veterans receiving VA health care have the correct eligibility.

I bring these two projects up because both involve a massive exchange of data, personal data, sensitive data in the case of the health care and income data. How much confidence do you have that there are appropriate safeguards, encryption, limits to access the information that is being compiled through these two projects?

Secretary NICHOLSON. Senator, I would like to tell you that I have a lot of confidence, but I am not going to because I do not. I think that we have 7.5 million enrolled patients for health care at the VA. Every one of them has an electronic health record, which is exemplary, and it is one of the main reasons, I think, that we are such a very good integrated health care provider. It gives portability and safety.

But I have worries about the fact that people can access this from remote stations and whether or not we have the controls in

place to limit that access, and what are the possibilities for the downloading of it?

Now I know that we have controls and we have codes and we have things that protect that. But I am not going to tell you that I think that it is what it should be.

Chairman COLLINS. That is something that I hope the Department will act very quickly to take a look at.

As I understand it, so far there has been no indication that the stolen data has been used for identity theft or financial fraud. And of course, all of us are hoping that that pattern will hold. There is a concern, however, that con artists could take advantage of this situation without having access to this data. I would like to give you a scenario that my staff had mentioned to me.

It would be very easy for a scam artist to call up a veteran, refer to this loss of data, pretend to be a VA representative and ask for the veteran to verify his or her Social Security number and date of birth.

Are you doing anything through your Web site or the Veterans Service Organizations to try to educate veterans on identity theft, in general, and that they should be very careful about giving out information, and perhaps to inform them that the VA is not calling to ascertain this information?

I just worry that even if this information miraculously is not misused by anyone, that there are clever con artists who could use the fact of this information's exposure to take advantage of our veterans.

Secretary NICHOLSON. I think it is a good point and we are not doing that, to my knowledge. It sounds like something we should be and can and will, yes.

Chairman COLLINS. I think that would be very helpful and maybe it is something—Mr. Opfer?

Mr. OPFER. Senator, actually you are right on target. We have been made aware of something like that yesterday and have reported it to the Department senior management. I think that needs to be very aggressively put out to the public. But something similar like that was reported and I had us bring it to the senior level of management. The Chief of Staff is aware of it and the other senior officials in the Department.

Chairman COLLINS. So your concern is that may already be happening?

Mr. OPFER. Yes, it would be a usual thing to happen in an event like this.

Chairman COLLINS. It would. I have done work in this area on identity theft and the financial fraud and people will take advantage and exploit every vulnerability. It would be ironic if the stolen information were never used for this purpose, but then con artists use the fact of this incident to compromise our veterans.

Mr. OPFER. A recent example of that was the tragedy in Fairfax, Virginia a few weeks ago, with the two police officers killed. Right before they were even buried, they were calling saying that they were calling on behalf of the police associations, generating funds. So as you have a tragedy, people are ready to come in.

In my previous experience, I was the Inspector General at the Federal Emergency Management Agency. And every time you had

a disaster, you had the people, as I referred to them the vultures, ready to come down.

Chairman COLLINS. There are always the fraudulent charities that pop up, people who are willing to exploit any tragedy. I think the fact that you already have reports of that suggests the VA needs to be proactive.

It seems to me one thing you might want to do with the notification letters is to include a flyer on protecting yourself from identity theft. The FTC, for example, has developed some very good materials on financial fraud in that area. So that is something that I would recommend.

Mr. Secretary, you mentioned that you are working cooperatively with the credit bureaus, which I commend you for. In addition to educating veterans that they can receive a free copy of their credit report, is the VA looking into other ways to connect veterans with their credit reports?

Secretary NICHOLSON. We are, Senator Collins. We also have been looking at some proposals from private sector, proprietary companies that are in this business. And our goal would be to see if we could create some kind of an overlay over the veteran community that could allay some of their fear and anxiety about this, knowing that there is somebody watching it and there is sort of a continual alert about them.

It would work with these three major reporting bureaus. There are people in that business and we are looking at it. The cost of it is something we are not yet sure of, but I am pretty confident that given the volume that we have, that we are dealing with here, that we could get a pretty good deal, which would still be a substantial amount of money. But I think it is something that our veterans deserve.

Chairman COLLINS. I agree and I am pleased you are pursuing that.

Mr. Secretary, I want to go back to my initial statement to you when I said that I found the chronology that you gave in your testimony to be baffling. I think you find it to be baffling also. And I understand how frustrated and angry you must be that it took some 13 days before you were notified of such a serious breach.

What is your theory on that? How do you think it was possible for there to be such long delays in bringing this incident to your attention? As I said, it was not minor. It did not involve just a few records. It is just so obviously urgent and serious that it is so hard for me to understand the failure of those in the Department to inform you.

Secretary NICHOLSON. It is an appropriate question. It is difficult for me to answer because some of the people along the line are some of the most competent, dedicated people I have ever worked with anywhere. It is hard to answer, frankly.

So I am only speculating. We have discussed it. They feel terrible. They have offered resignations. They were trying to deal with it themselves and get their arms around it and handle it. It is not clear.

Chairman COLLINS. Thank you.

Mr. Chairman.

Chairman CRAIG [presiding]. I have one last question and before I do that, if you are leaving us.

Chairman COLLINS. I do not have anything else. Thank you.

Chairman CRAIG. Again, thank you for working with us for this joint hearing. I think it is obvious the problem that are now appearing in VA, and as we started this hearing, the question remains are these same problems system wide? The work you are doing in your Committee is critical and important. And we will monitor this and work with you to make sure that—you never say never, but we ought to have systems in place where that argument can at least be placed.

Thank you very much, Susan.

Chairman COLLINS. Thank you, Mr. Chairman. And again, thank you for taking the initiative on this very serious problem. I have enjoyed working with you on this hearing.

Chairman CRAIG. Thank you very much, Madame Chair.

Mr. Opfer, the Inspector General Act requires you to keep the Secretary and Congress fully and currently informed about any serious problem regarding VA's operation. In this case, it appears that the Secretary was not notified of the massive data security breach until 6 days after the IG Office was alerted to the incident, and Members of the Congress were not notified for several days after that.

Again, this question has been asked, but for the record, given the magnitude of the data security breach, do you believe the IG's Office acted with sufficient haste in reporting the incident to the Secretary and ultimately to the Congress?

Mr. OPFER. Yes, I do. Mr. Chairman, let me go through the chronology again.

The IG Office was never notified of the security breach. It was a normal monthly meeting when an Information Security Officer from the IG was attending. It was not talked about. It was mentioned that an employee had some data stolen from a burglary at his residence. No information was given to that employee of the significance of it.

He followed up on his own to try to find out what information he could. That was on the information of May 10th. There was no information given to the IG.

He wrote it up and gave it to our Office of Investigations that went to the Department on Friday, May 12th to try to locate this Information Security Officer. The officer was not at work. The agents did not just wait. They tried to contact him at home. He was on leave. They were not able to contact that Information Security Officer that had the information until Monday the 15th. That is when they interviewed him, gave the preliminary information. We had no knowledge of anything other than an employee had some data stolen from the home, the residence.

It was not until we interviewed the employee on the 15th that we realized that we had a significant problem developing there. That interview went for hours upon hours of interviewing the employee. That is where the information came to the IG.

With the story what he was saying he had access to this type of information, that first thing you need to do is ask, is it credible?

Would an employee have that much access to that type of sensitive information? And would he be able to take it to his residence?

The second part was then to look if there were other issues with that employee? The investigators went through the background, doing name checks, record checks, reviewing his official personnel folder, looking at any issues that we may have had in the IG's Office, trying to determine, contacting their local police. Was there a burglary? Was it reported? Was it similar to others? Or was this a staged burglary? Were there issues with the employee? His family, with the police?

It was not until the morning of the 16th of May that they spoke to the police. But they had to get to the detective that was doing this to see what we had. It was then immediately that the agents told the detective of the seriousness of what we were looking at, of the possible breach of millions of personal identification information.

On the 16th, they came to me in the morning to brief me. I immediately, before he even finished the briefing, got on the phone to the Chief of Staff who was with Tim McClain, the Counsel, and explained to him what we had. We had a serious problem. The information only was coming to us from the interview of the agents with the employee.

On the 16th, in the morning, this was about 9:30, when I spoke to the Chief of Staff, he told me that he was aware of an incident but did not realize the magnitude of the incident. It was after they had the 11 o'clock meeting, that I again spoke to the Chief of Staff and told him that I requested that he brief the Secretary on the severity of this.

The Secretary was out of town attending the funeral service of former Congressman Sonny Montgomery. The Chief of Staff told me the Secretary would be back at 7 o'clock that night and he would brief him on it. The next morning, every day from then on, I had constant contact.

So when it came to my attention, the Secretary was notified immediately from the Chief of Staff on the 16th.

On the 17th, we again were confirming and working with the Montgomery County Police through the 15th, 16th and 17th. On the 17th, this is one day now from when we are verifying that we had a serious problem which was verified to us on the 16th, not only from the employee's interview, but verified that he did have access to this material, we notified the Federal Bureau of Investigation both from field office to field office, as well as the Acting Assistant Director for Criminal Division. So notifications were made in a very serious and coordinated effort.

I had to balance a decision of whether or not to release that information. During all of these periods of conversations that I was having with senior level officials within the Department, I was advising them of my statutory responsibility both to Congress and both to notify the appropriate Federal law enforcement agencies, which we did within a day.

The decision not to go public was one, and I kept using the phrase we are on borrowed time. As the IG's Office was ratcheting this up, as we were going out doing interviews, more people were

going to become aware of what we are looking at. And I was concerned it was going to be released.

Right from the beginning, on the 17th, I had conversations with the Chief of Staff that somehow along the line I was going to start these notifications. But the Chief of Staff agreed that we needed to be proactive and the Department was being proactive to reach out to try to look at what lessons they could get from the Federal Trade Commission, the Commerce Department, to establish the 800 number, the Web site and all these initiatives that went in.

I had to balance where along the line does that come to with what we had as investigative leads which were quickly evaporating. We were very aggressively investigating every investigative lead that we had. And during that whole period of time, I was saying I am coming to the point I cannot justify legally or morally not making those notifications relative to investigative leads because they just were not there as we were knocking them off.

On Thursday evening, I had a conference call with the Secretary, the Chief of Staff and the Counsel, and I do not know if anyone else was present. We talked about this. I talked about my position that we came to the point now, from the Inspector General's position, we should go public. It was time to make the notifications.

We talked about do we balance that with the panic that we could cause for the veterans?

I still said this did not outweigh my obligation and I would not delay that notification any longer. I felt from an investigative standpoint we have gotten to the point we were exhausting all of the leads that were available.

It was agreed that the next morning I would receive a copy of a draft statement making the announcement. My staff contacted the appropriate Members of the Committee staff. I was prepared to make that notification on Friday.

And I would like to ask Jon Wooditch then to talk about what happened Friday afternoon to try to convince us then to hold off.

Mr. WOODITCH. I was contacted by the VA General Counsel, who asked us to talk to the Director at the Federal Trade Commission because they were not quite ready with the Web sites and the hot lines and all of the other tools that they were going to use to satisfy the veterans calling in. It seemed to be a legitimate request. If we went out prematurely and we were not ready to deal with all of the calls that we were going to get, it could cause panic.

So, I agreed to talk to the FTC Director and she convinced me that they would work feverishly over the weekend and have it done by Monday. Monday it was completed and the Secretary did, in fact, make the announcement on Monday.

Mr. OPFER. I would also add on Sunday, that Sunday, I had two telephone conversations with the Associate Attorney General asking me if my position was still that. And I said I was concerned that we could not wait any longer. And I needed to verify, he was going to a meeting at the White House to verify that the FTC and all of these operations were going to be in place for Monday. He called me back later. He wanted to know, from my perspective as lead investigator for the OIG, and we discussed that he would reach out to the FBI to see if they had any additional leads. I said

I was not aware of any, but I would reach out again to my supervisor and the agents working to see if there were any leads left that would justify withholding going public at that point.

So, I do believe it was done in a timely manner.

Chairman CRAIG. I mean, I find that fascinating. I am not here to challenge your judgment. I think I have, we probably have a better picture of what did and did not happen.

I would hope that you all collectively look at what you did and how you did it with the hindsight you now have. It appears to me to be a fascinating case study. I do not know whether I am overreacting or under reacting. I do not know whether you overreacted or under reacted as it relates to the knowledge you had and how you handled the knowledge.

I know one thing, that it was not until May 22 that I found out about it. And I do not believe I or this Chairman can be called public. We are not the public.

Mr. OPFER. I was not talking about that. I was also talking about notifying Congress. It was whether or not, even again on Sunday I was requested by the Justice Department if I would reconsider my position.

Chairman CRAIG. And yet, at the same time, I appreciate having the tools in place to handle response to an announcement of this magnitude. I can hardly question that because obviously you were getting a great concern and there is a lot of—as the information flows out, there is a growing concern amongst veterans as to whether they, in fact, have been compromised or not.

That is part of why we are here today. But it is also why we are here to review, and in some instances to criticize.

I hope that both of you recognize the importance of a constructive dialogue that gets us, as I said, not ever having this happen again. I do not believe in nevers. They just do not exist. But certainly we have had a record of problems here, not of this magnitude, and clearly one now that I trust will move forward on.

Certainly this Committee, and I know that Susan's Committee will do the same thing. And as we look beyond VA to other agencies of Government to make sure that similar protocol and certainly similar policy is put in place. And my guess is with the legislation that is out there, legislation that will become law passed by Congress in relatively short order as it relates to these kinds of things.

Susan, do you have any additional things you want to say?

Chairman COLLINS. No, thank you.

Chairman CRAIG. Again, gentlemen, thank you very, very much for being here this morning and being as cooperative as you now are. We appreciate that a great deal as we work our way through this. It is a joint effort.

And Mr. Secretary, I appreciate your responses and obviously taking the responsibility that a person in your position must take to deal with these kinds of issues.

But again, you have a cooperating Committee here that wants to make sure we deal with this in the appropriate fashion and, where necessary, to provide the resources, if necessary, to make sure that this goes away as quickly as possible and that no veteran is injured.

Gentlemen, thank you both. Thank you all very much.

The Committee record will remain open. Several of my colleagues have asked to submit questions in writing and, of course, we will allow that to happen. We will keep the record open for at least 2 weeks.

Thank you.

VOICE: Will you take a statement from an affected veteran?

Chairman CRAIG. I will be happy to visit with you afterwards and anything you want to submit to us, we will be happy to put in the record.

Thank you very much.

The Committee will stand adjourned.

[Whereupon, at 12:41 p.m., the Committee was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. NORM COLEMAN, U.S. SENATOR FROM MINNESOTA

We are witnessing a disturbing trend in the Federal Government recently in which problems have been identified, warnings and recommendations have been issued and then no action takes place. The news delivered Tuesday that up to 26.5 million veterans, the very people we have asked to sacrifice so much for this Nation, were now vulnerable to identity theft because a VA employee was able to just walk out of the building with highly sensitive information is appalling.

Equally outrageous is that after a third-rate burglary took place and put veterans at risk on May 3rd , we learned yesterday that Secretary Nicholson was not notified of the breach for 13 days, and the FBI was not notified for 14 days. And if that weren't enough, since 2001 the VA Inspector General has reported security vulnerabilities relating to the operating system, passwords, a lack of strong detection alerts, and the need for better access controls.

Mr. Secretary, while it was unfortunate you were not informed earlier of the burglary, identity theft is not a new problem and the blunt assessment the VA was given from its Inspector General should have immediately been addressed. It is also unfortunate and troubling that while the VA employee who was robbed informed the VA of what happened that same day, it took the VA 19 days, almost 3 weeks, to inform Veterans that they may be at-risk to identity theft.

Additionally, identity theft and fraud is a national problem that has affected more than 10 million Americans and this case raises the question of what the Federal Government is doing to protect all sensitive information so it does not fall into the wrong hands. The Federal Government is responsible for maintaining and protecting sensitive information that Americans are required to provide for a wide array of reasons, including paying taxes, receiving medical and disability benefits, and obtaining retirement compensation.

In order to determine the extent of the vulnerabilities in information security across the Federal Government, yesterday I sent a letter to the Government Accountability Office requesting a governmentwide review of the current policies and practices in place meant to protect the sensitive identity information of Americans, and whether these policies may allow for a similar type of security breach at other Federal agencies.

The bottom line is that American citizens deserve to know if their sensitive information is safe.

PREPARED STATEMENT OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

The Center for Democracy and Technology is deeply troubled by the revelation that the Department of Veterans Affairs carelessly allowed the personal data of millions of men and women who've served this country to fall into the hands of a simple burglar. Yet, it is our view that this breach is not the failure of one employee or even one agency. It is symptomatic of a larger failure of data management across the Federal Government.

Until we bring the aging laws and policies that protect our personal information up to date with modern technology, these catastrophic data "spills" will only get worse.

Attorney General Alberto Gonzalez responded to the breach—the latest in a series of private and public sector privacy gaffes—by vowing to closely monitor for any signs of identity theft and to aggressively pursue offenders. This is an appropriate and necessary response, now that the data has been compromised, but it doesn't come close to providing the comprehensive protection for personal information expected when the Privacy Act was passed in 1974.

A growing body of research, supported by years of Government Accountability Office reports, makes clear that it is time to bolster the protections in that law and dramatically improve enforcement.

In 2003, GAO made clear that "the government cannot adequately assure the public that all legislated individual privacy rights are being protected." This report and others made clear that the problem is not with an individual agency but rather an endemic lack of leadership from the White House and its Office of Management and Budget over Privacy Act enforcement. In the absence of strong Administration leadership individual agencies have been left to fend for themselves in bringing their information practices in line with the Privacy Act.

CDT's discussions with agency privacy officers support the GAO findings. One chief privacy officer for a key agency told us that half of the agency's Privacy Act systems of records—the databases most likely to have sensitive information on Americans—were simply missing.

To address these serious concerns, GAO correctly recommends that agencies be given better guidance and follow best practices. The Office of Management and Budget's Privacy Act guidance was written in 1975 and has never been comprehensively updated. Technology has evolved enough in the past 3 years, let alone the past 30, to warrant a thorough rewrite of that guidance. Such a rewrite alone would send a clear message to agency heads and privacy officers that they will be held responsible for the sensitive data in their care.

Although renewed leadership on Privacy Act compliance would be an important first step, it's also the case that the law itself is in need of renovation, given the technological revolution that has taken place in the decades since its passage. Congress must patch the holes in the aging laws intended to protect the personal information that Americans entrust to the government before more massive data breaches occur.

Because of the rash of high-profile data breaches in the private sector, Congress has focused its legislative efforts on establishing data breach rules for the private sector and has not given the same attention to the serious privacy and security problems in government agencies that collect and maintain databases of personal data on Americans. Indeed, only one of the data-breach bills under consideration even begins to address the Federal Government's use of personal information. The measure, S. 1789, The Personal Data Privacy and Security Act" sponsored by Senators Arlen Specter (R-Pa.) and Patrick Leahy (D-Vt.) would, among other things, require greater oversight over the government's use of personal data and would limit the government's ability to augment its data with additional information purchased from private-sector companies like ChoicePoint. Today, many government agencies are using this commercial data in ways that violate the spirit of the Privacy Act, but not the letter of the law. These practices have encouraged an atmosphere that suggests that the law is not as relevant as it was at the time that it was passed.

Enacting those provisions would be a valuable step toward safeguarding our personal data, but Congress should go further and enact comprehensive legislation to bring Privacy Act into the 21st century. The law, written during the age of the mainframe computer, must be updated to respond to new technologies. Today, a smart phone can hold as much data as computers that occupied an entire room in 1974. Congress can start by updating the basic definitions of the Act and limiting the routine exemptions on the data.

As early as 1977, a Congressional commission found that the Act's central definition—"systems of records"—was already outdated. Particularly on the Internet, where multiple databases can be linked, searched, copied and reconfigured, the concept simply does not work. Moreover, privacy advocates and policymakers have long complained that the "routine use" exemption is being used in ways going far beyond its original intent. That definition also needs to be reconsidered.

Congress may also want to review the effectiveness and applicability of sections of the Taxpayer Browsing Protection Act of 1997, which was passed after abuses by IRS employees, including improper removal of taxpayer records from the agency, were revealed.

Americans entrust the Federal Government with significant amounts of our personal information in order to deliver benefits and services. Updating privacy oversight, policy and law in this area is the first necessary step to ensuring that this information is not simply left vulnerable to common thieves.

PREPARED STATEMENT OF THE DEPARTMENT OF VETERANS AFFAIRS

The Department of Veterans Affairs (VA) has recently learned that an employee, a data analyst, took home electronic data from VA, which he was not authorized to do. This behavior was in violation of our policies. This data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. Importantly, the affected data did not include any of VA's electronic health records nor any financial information. The employee's home was burglarized and this data was stolen. The employee has been placed on administrative leave pending the outcome of an investigation.

Appropriate law enforcement agencies, including the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items because of any knowledge of the data contents. It is possible that they remain unaware of the information which they possess or of how to make use of it. However, out of an abundance of caution, VA is taking all possible steps to protect and inform our veterans.

VA is working with Members of Congress, the news media, veterans service organizations, and other government agencies to help ensure that those veterans and their families are aware of the situation and of the steps they may take to protect themselves from misuse of their personal information. VA will send out individual notification letters to veterans to every extent possible. Veterans can also go to *www.firstgov.gov* to get more information on this matter. This website is being set to handle increased web traffic. Additionally, working with other government agencies, VA has set up a manned call center that veterans may call to get information about this situation and learn more about consumer identity protections. That toll free number is 1–800–FED INFO (333–4636). The call center will be open beginning today, and will operate from 8 a.m. to 9 p.m. (EDT), Monday–Saturday as long as it is needed. The call center will be able to handle up to 20,000 calls per hour (260,000 calls per day).

Secretary of Veterans Affairs R. James Nicholson has briefed the Attorney General and the Chairman of the Federal Trade Commission, co-chairs of the President's Identity Theft Task Force. Task Force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report they are entitled to under the law. Additionally, the Task Force will meet today to coordinate the comprehensive Federal response, recommend further ways to protect affected veterans, and increase safeguards to prevent the reoccurrence of such incidents. VA's mission to serve and honor our Nation's veterans is one we take very seriously and the 235,000 VA employees are deeply saddened by any concern or anxiety this incident may cause our veterans and their families. We appreciate the service our veterans have given their country and we are working diligently to protect them from any harm as a result of this incident.

VA'S NOTIFICATION TO VETERANS

Dear Veteran: The Department of Veterans Affairs (VA) has recently learned that an employee took home electronic data from VA, which he was not authorized to do and was in violation of established policies. The employee's home was burglarized and this data was stolen. The data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. As a result of this incident, information identifiable with you was potentially exposed to others. It is important to note that the affected data did not include any of VA's electronic health records or any financial information.

Appropriate law enforcement agencies, including the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items because of any knowledge of the data contents. It is possible that they remain unaware of the information which they possess or of how to make use of it.

Out of an abundance of caution, however, VA is taking all possible steps to protect and inform our veterans. While you do not need to take any action unless you are aware of suspicious activity regarding your personal information, there are many steps you may take to protect against possible identity theft and we wanted you to be aware of these. Specific information is included in the attached question and answer sheet. For additional information, VA has teamed up the Federal Trade Commission and has a website (*www.firstgov.gov*) with information on this matter or you

may call 1–800–FED–INFO (1–800–333–4636). The call center will operate from 8 a.m. to 9 p.m. (EDT), Monday–Saturday, as long as it is needed.

We apologize for any inconvenience or concern this situation may cause, but we at VA believe it is important for you to be fully informed of any potential risk resulting from this incident. Again, we want to reassure you we have no evidence that your protected data has been misused. We will keep you apprised of any further developments. The men and women of VA take our obligation to honor and serve America's veterans very seriously and we are committed to seeing this never happens again. Sincerely, R. James Nicholson Secretary of Veterans Affairs.

Sincerely,

R. JAMES NICHOLSON,
Secretary of Veterans Affairs.

FOR IMMEDIATE RELEASE

May 22, 2006

FREQUENTLY ASKED QUESTIONS ON VA'S LETTER TO VETERANS

Question 1. I'm a veteran, how can I tell if my information was compromised?

Response. At this point there is no evidence that any missing data has been used illegally. However, the Department of Veterans Affairs is asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved and contact the Federal Trade Commission for further guidance.

Question 2. What is the earliest date at which suspicious activity might have occurred due to this data breach?

Response. The information was stolen from an employee of the Department of Veterans Affairs during the month of May, 2006. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that veterans may notice suspicious activity during the month of May.

Question 3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

Response. The Department of Veterans Affairs strongly recommends that veterans closely monitor their financial statements and visit the Department of Veterans Affairs special website on this, *www.firstgov.gov* or call 1–800–FED–INFO (1–800–333–4636).

Question 4. Should I reach out to my financial institutions or will the Department of Veterans Affairs do this for me?

Response. The Department of Veterans Affairs does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

Question 5. Where should I report suspicious or unusual activity?

Response. The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

Step 1.—Contact the fraud department of one of the three major credit bureaus: Equifax: 1–800–525–6285, *www.equifax.com*, P.O. Box 740241, Atlanta, GA 30374–0241; Experian: 1–888–EXPERIAN (397–3742) *www.experian.com*, P.O. Box 9532, Allen, Texas 75013; TransUnion: 1–800–680–7289, *www.transunion.com*, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834–6790.

Step 2.—Close any accounts that have been tampered with or opened fraudulently.

Step 3.—File a police report with your local police or the police in the community where the identity theft took place.

Step 4.—File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by telephone: 1–877–438–4338, online at *www.consumer.gov/idtheft*, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington DC 20580.

Question 6. I know the Department of Veterans Affairs maintains my health records electronically; was this information also compromised?

Response. No electronic medical records were compromised. The data lost is primarily limited to an individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of potential use to identity thieves and we recommend that all veterans be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

Question 7. What is the Department of Veterans Affairs doing to insure that this does not happen again?

Response. The Department of Veterans Affairs is working with the President's Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate this data breach and to develop safeguards against similar incidents. The Department of Veterans Affairs has directed all VA employees complete the "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by June 30, 2006. In addition, the Department of Veterans Affairs will immediately be conducting an inventory and review of all current positions requiring access to sensitive VA data and require all employees requiring access to sensitive VA data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the Inspector General of the Department of Veterans Affairs, have launched full-scale investigations into this matter.

Question 8. Where can I get further, up-to-date information?

Response. The Department of Veterans Affairs has set up a special website and a toll-free telephone number for veterans which features up-to-date news and information. Please visit *www.firstgov.gov* or call 1–800–FED–INFO (333–4636).

(a) CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet and new communications technology. Since its founding in 1994, CDT has tracked government information technology privacy and security policy to ensure that it has been kept up to date. This has included reports and testimony on the Privacy Act, the privacy provisions of the E-Government Act and the Federal Information Security Management Act.

(b) GAO, Privacy Act: OMB Leadership Needed to Improve Agency Compliance, GAO–03–304 (Washington, DC; June 30, 2003).

(c) CDT has championed the return of the Chief Privacy Counselor, or similar position, to OMB. At the end of the Clinton Administration, Chief Privacy Counselor Peter Swire produced regular guidance to agencies that, while not comprehensive, at least moved many agencies toward positive progress on important privacy matters.

(d) OMB, "Privacy Act Implementation: Guidelines and Responsibilities," Federal Register, Volume 40, Number 132, Part III, pp. 28948–28978 (Washington, DC.: July 9, 1975). There has been irregular guidance such as that issued on May 22, 2006 (the day of the public announcement of the breach).

(e) Privacy Protection Study Commission, Personal Privacy in an Information Society, July 1977. An electronic version is available at *http://www.epic.org/privacy/ppsc1977report/fPL 105-35.*

○