LEGISLATIVE HEARING ON VETERANS IDENTITY AND CREDIT PROTECTION LEGISLATION

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 18, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-60

29-564.PDF

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2007

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

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, *Indiana, Chairman*

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

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

JAMES M. LARIVIERE, *Staff Director*

CONTENTS

July 18, 2006

	Page
Legislative Hearing on Veterans Identity and Credit Protection Legislation	1

OPENING STATEMENTS

Chairman Buyer	1
Prepared statement of Mr. Buyer	66
Hon. Bob Filner	3

STATEMENTS FOR THE RECORD

Hon. Corrine Brown	70
Hon. Cliff Stearns	71
Hon. Stephanie Herseth	74
Hon. John Boozman	76
Hon. Tom Udall	77
Hon. Ginny Brown-Waite	78

WITNESSES

Hooley, Hon. Darlene, a Representative in Congress from the State of Oregon	5
Prepared statement of Ms.Hooley	79
Blackburn, Hon. Marsha, a Representative in Congress from the State of Tennessee	7
Prepared statement of Ms. Blackburn	82
Salazar, Hon. John T., a Representative in Congress from the State of Colorado	9
Prepared statement of Ms. Salazar	84
Capito, Hon. Shelley Moore, a Representative in Congress from the State of West Virginia	11
Prepared statement of Ms. Capito	87
Gauss, Hon. John A., Ph.D., President and Chief Operating Officer, FGM, Inc., and Former Assistant Chief Information Officer, U.S. Department of Veterans Affairs	15
Prepared statement of Mr. Gauss	89

Page

WITNESSES (CONTINUED)

McFarland, Hon. Robert, Former Assistant Secretary for Information and Technology and Former Chief Information Officer, U.S. Department of Veterans Affairs 18
Mansfield, Hon. Gordon H., Deputy Secretary, U.S. Department of Veterans Affairs 35
Prepared statement of Mr. Mansfield 93
Williams, James A., Commissioner, Federal Acquisition Service, U.S.General Services Administration 37
Prepared statement of Mr. Williams 99
Gaytan, Peter S., Director, Veterans Affairs and Rehabilitation Commission, American Legion 50
Prepared statement of Mr. Gaytan 106
Norton, Col. Robert F., USA (Ret.), Deputy Director, Government Relations, Military Officers Association of America 52
Prepared statement of Col. Norton 110
Irvin, Louis, Acting Deputy Executive Director, Paralyzed Veterans of America 53
Prepared statement of Mr. Irvin 114
Madison, Msgt. Larry, USAF (Ret.), Deputy Legislative Director, Retired Enlisted Association 55
Prepared statement of Msgt. Madison 119

MATERIAL SUBMITTED FOR THE RECORD

Draft Bill Summary for the "Veterans Identity and Credit Protection Act of 2006" 123
Discussion Draft for the "Veterans Identity and Credit Protection Act of 2006" 125

LEGISLATIVE HEARING ON VETERANS IDENTITY AND CREDIT PROTECTION LEGISLATION

TUESDAY JULY 18, 2006

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

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

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

The Chairman. The Committee on House Veterans' Affairs will come to order July 18th, 2006.

This morning, we will review draft legislation prepared in response to the theft in May of personal data belonging to as many as 26.5 million veterans and 2.2 million servicemembers as well as family members.

The stolen computer's recovery and the FBI's determination the files were not accessed do not reduce the importance of improving information security and management at the VA. We have been sufficiently warned.

We also have the Minneapolis and Indianapolis data breaches and others. We have challenges requiring the ongoing stewardship as we work with the VA on securing its information management systems.

I want to commend the members of this Committee and our staff. To get here, we conducted three weeks of a series of five Committee and two Subcommittee hearings and that layer by layer, these last five weeks have allowed us to build our knowledge and equipped us to examine this issue in its totality so we may have a greater understanding of the problems. And the VA has equally moved out in the same manner.

We brought in 18 witnesses and senior VA officials including for-

mer VA Chief Information Officers who answered questions on the data loss itself and the current and potential structure of VA's IT system of lack thereof.

We have learned from experts how the best firms in industry manage their information and data security, and we have heard from the academic world as well. This work is undergirded by six years of hearings conducted by this Committee up to this point. I expect that when we introduce this legislation, its quality will reflect this approach.

Eight legislative proposals have been introduced and referred to this Committee since the May 3rd data theft. Proposals have included requirements that the VA notify veterans of data loss and provide free credit monitoring.

Additionally, at first, they envisioned a claims process, but the Secretary spoke with me about insurance, and Mr. Bilbray has also introduced legislation to address this issue which calls for credit insurance as well as monitoring. At least one bill requires VA to implement the GAO data security recommendations.

We have reviewed proposed legislation to limit the use of Social Security numbers and create personal identification numbers for veterans, and we received a proposal to create a new Office of Identity Protection within the VA.

There is much here worthy of our consideration. Today we will review draft legislation that draws on many of these ideas. The draft bill and a summary are before the members.

[The draf bill summary and draft legislation appear on p. 123]

THE CHAIRMAN. First, the bill adds government-wide requirements to FISMA for agency procedures in the event of data breaches and for notice to individuals for whom personal information has been compromised.

Further, the bill would also make it clear that under FISMA, agency CIOs have enforcement authority for information security policy.

For the FISMA provisions on this bill, I want to thank Chairman Davis and Ranking Member Waxman, of the Government Reform Committee, as well as their staffs. Their staff haave attended our hearings. They have been good listeners and recognize the challenge in all departments and agencies, and they are working with us in a cooperative spirit to move these FISMA improvements to the floor without delay.

Our goal must be to determine how best we can make whole any person harmed by a data compromise at the VA. As important, we must address and ensure the Department's policies and organizational structure work to efficiently manage and safeguard the information.

But without a good organization guided by sound policy, we will

be revisiting the tragedy of the compromised personal data all too often.

I look forward to our discussion today, and I wish to commend Mr. Filner and other members of the Committee for your perseverance and your hard work in dealing with a very difficult issue.

I now recognize Mr. Filner for an opening statement.

[The statement of Chairman Buyer appears on p. 66]

MR. FILNER. Thank you, Mr. Chairman. I thank our colleagues for being here this morning.

As the Chairman said, and I appreciate his leadership on this issue, we have gone through a real process of hearings, oversight hearings, of bringing experts in, of asking our colleagues for information, working with other committees, and in a bipartisan way, as this bill reflects, coming up with a product in a rather quick amount of time.

Mr. Chairman, I am sure you do not think it is a quick amount of time given your seven years of history on this concern, but obviously since May 3rd, we have finally moved very quickly.

We have learned a lot about the VA. We have learned a lot about the specifics of the data theft itself and the underlying information technology and management problems that contributed to it.

We have been dismayed and even shocked at the dysfunctional manner in which veterans' personal information has been handled, sometimes without any governing policy. While VA claims to have received a wake-up call, I believe it is incumbent upon this Committee and this Congress to follow through, and that is what we are doing with the legislation.

Our respective staffs have closely collaborated on this bill. You have drawn on Democratic as well as Republican ideas. Our colleagues, Mr. Salazar and Ms. Hooley, from this Committee have felt that their input has been very well-respected, and we certainly appreciate the joint working of this Committee.

I am interested in hearing from our witnesses on two matters in particular, both the adequacy of the protection that veterans will be afforded by this legislation and the triggers for those protections. We have gone back and forth to get a good bipartisan product.

I do have a question, Mr. Chairman, although I am willing to go along with you, but I wonder about the need to elevate the Chief Information Officer from an Assistant Secretary to Under Secretary, placing this position on the same plane as the Department's mission objectives of health, benefits, and memorial affairs.

It has been obviously demonstrated in an all too real manner the dangers and complexities of technology and protecting sensitive information, but IT is still a support function, although a very important one.

I would like also to hear from our witnesses regarding the CIO el-

evation proposal for another reason as well. It was abundantly clear from the testimony of more than 20 witnesses in the seven hearings that we had about the failures in reporting the data loss that, it came down largely to ambiguous or nonexistent policy, ineffectual communication, and poor leadership. Putting a bigger badge on a CIO will not do anything to change those problems, so I hope we will look at that very closely.

Mr. Chairman, your work for the past seven years on this and the sincerity of your desire to fix this cannot be underestimated. Thank you for your determination in bringing this Committee analysis of the problem.

We will have a bill on Thursday. It will reflect our mutual commitment to protecting sensitive information, providing essential services veterans will need in the event of a data breach, and responding to the cavalier manner in which this breach and others were handled.

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

Is someone else having any opening remarks? Thank you.

[The statement of Corrine Brown appears on p. 70]

[The statement of Cliff Stearns appears on p. 71]

[The statement of Stephanie Herseth appears on p. 74]

[The statement of John Boozman appears on p. 76]

[The statement of Tom Udall appears on p. 77]

[The statement of Ginny Brown Waite appears on p. 78]

THE CHAIRMAN. We will now proceed with our first panel. It is comprised of members who have introduced various legislation following the announcement of the May 3rd data loss at the VA.

Two of these members come from our own Committee. Our first witness is Ms. Darlene Hooley of the 5th District of Oregon. Ms. Hooley is also a member of the Committee and has two VA facilities in her District.

Next we will hear from Ms. Marsha Blackburn, who represents the 7th District of Tennessee. The bill introduced by Ms. Blackburn, House Resolution 5464, shows her experience from serving on the Energy and Commerce Committee and has provided some guidance in the draft of this bill before us in dealing with cyber security issues.

We will then hear from Mr. John Salazar, who represents the 3rd District of Colorado. He is the only veteran in the Colorado Delegation. Mr. Salazar has been a member of this Committee since February of this year and was one of the first to introduce a substantive piece of legislation on this issue, and we appreciate your expertise.

We will also then hear from our last witness, Ms. Shelley Moore Capito, representing the 2nd District of West Virginia. She has traveled twice to Afghanistan, once to Iraq where she has been able to meet with our troops fighting the War on Terror and the rebuilding efforts in both countries. Her sincerity for the concerns and well- be-

ing of veterans is evident and real.

I will now yield. Ms. Hooley, you are now recognized.

STATEMENTS OF HON. DARLENE HOOLEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON; HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE; HON. JOHN T. SALAZAR, REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO; AND HON. SHELLEY MOORE CAPITO, REPRESENTATIVE IN CONGRESS FROM THE STATE OF WEST VIRGINIA

STATEMENT OF HON. DARLENE HOOLEY

Ms. Hooley. Good morning, Mr. Chairman, Ranking Member Filner.

First of all, I want to thank you for all the hearings that you have had on this issue and all the work you have done and for allowing us the opportunity to appear before the Committee.

The Chairman. Ms. Hooley, and to each of the witnesses, do each of you have a written statement?

Ms. Hooley. Pardon?

The Chairman. Do all of you have written statements?

Ms. Hooley. Right.

The Chairman. They all nod in the affirmative. Do you all wish they to be submitted for the record?

Ms. Hooley. Yes.

The Chairman. Hearing no objections, so ordered.

Ms. Hooley, you are recognized.

Ms. Hooley. As one of millions of former credit card fraud victims and as a member of the House Financial Services Committee, I have long had a very strong interest in identity theft and threats to financial crimes.

Identity theft represents a fundamental threat to e- commerce, to our overall economy, and to our homeland security. No longer are we facing just hobbyist hackers looking to create a nuisance. Increasingly these attacks are driven by skilled criminals and ID theft has become big business.

For the past six years, I have worked on the Financial Services Committee to protect consumers from the threat of ID theft. We have made significant progress in the recent past including signing into law the FACT Act of 2003. That bill, I was a proud co-author with Congressman LaTourette which provides consumers with landmark new protections including the right to a free annual credit report and the right to place a red flag fraud alert on their credit reports.

Last February, after data security breaches at ChoicePoint and

Lexis Nexis, I began working on legislation to prevent future data breaches, to provide meaningful notification when consumers could be harmed by a security breach, and to provide consumers with additional protections when they are placed at risk of identity theft.

The need for such legislation was made crystal clear by the massive data security breach suffered at the VA in May. The details of that breach, which have been highlighted many times in this Committee, underscore the glaring weaknesses in data security policies and procedures not only in the VA but throughout government agencies and in the private sector.

Any data security bill passed by Congress must include a number of key ingredients if we are going to be effective. First, it must mandate data security safeguards and require all businesses and government entities that handle sensitive personal information to have a robust data security policy and procedures in place.

Currently many businesses and most government agencies are not required to employ such protections leaving consumers at risk. Mandating protection of sensitive information is the first step in protecting consumers.

Second, legislation must mandate that all businesses and government entities immediately conduct an investigation upon learning that a breach of security might have occurred. That investigation should determine the information involved, whether or not that information is usable, and determine the likelihood that the information has been or will be misused.

Third, legislation should require that upon discovering a breach, the business or government entity notify Secret Service immediately and their functional regulator, if they have one, each of the credit reporting agencies, and any third party who must take steps to protect consumers from resulting fraud or identity theft.

Fourth, legislation should include a system restoration requirement that requires any business or government entity to repair any breach and restore the security and confidentiality of that sensitive personal information and to make improvements in its data security policies and procedures.

Finally, legislation should require meaningful consumer notice. That notice should contain vital information to aid the consumer in protecting themselves. In addition, that notice should provide consumers who are put at risk of identity theft with an opportunity to sign up for free-of- charge credit monitoring services.

Legislation I have co-authored, House Resolution 3997, the Financial Data Protection Act, would accomplish exactly that. However, the breach suffered by the VA highlighted two additional components needed to address any massive government breach like the VA that were not included in the bill as it was passed out of Financial Services.

In order to address those two needs, I introduced legislation shortly after the massive VA breach that would supplement House Resolution 3997. That legislation, the Veterans ID Theft Protection Act, would first of all authorize funding as necessary to the Secretary of Veterans Affairs to provide credit monitoring as required, and, two, make certain VA has all the necessary negotiating power to secure the best possible price for credit monitoring services.

In conclusion, Chairman Buyer and Acting Ranking Member Filner, I would simply state that now is the time to act. The need for Federal action on data security is clear. We should not wait for the next catastrophic breach to prod us into action.

I am so happy that we are going to be marking up a bill on Thursday. I think we need to do it and need to do it now.

Again, I thank you for the opportunity to testify before the Committee and look forward to working with each of you to pass commonsense data security legislation. Thank you.

THE CHAIRMAN. Thank you, Ms. Hooley.

Ms. Blackburn.

[The statement of Darlene Hooley appears on p. 79]

MS. HOOLEY. Mr. Chair, I would apologize. I do need to leave for another meeting, and I will be back for questions.

THE CHAIRMAN. If any member would like to grill her before she leaves, you can question her right now.

All right. You are excused, Ms. Hooley.

MS. HOOLEY. Thank you.

THE CHAIRMAN. Your colleagues are nice to you.

STATEMENT OF HON. MARSHA BLACKBURN

MS. BLACKBURN. Thank you, Mr. Chairman, and thank you for the hearing. Ranking Member Filner, thank you also. And I congratulate the two of you on a bipartisan draft and attention to a much-needed issue.

I also want to thank you for inviting me to testify today regarding the legislation that I introduced with Representative Simmons.

We drafted our Veterans Identity Protection Act as you referenced it, House Resolution 5464, this May in the days after Congress learned that the personal information of millions of the nation's veterans had been stolen from a Department of Veterans Affairs' employee.

As representative to a large military post and a district with tens of thousands of veterans, this issue has clearly been a source of concern. I know that Representative Simmons, who is a veteran himself, has also heard the same thing from his constituents.

The idea that your identity can be stolen, your credit ruined, and your life impacted in such a negative way is absolutely unsettling,

and it is our responsibility to bring as much reassurance and assistance as possible to those veterans who have been touched by this theft.

The situation is very similar to the information breaches that have occurred with data brokers over the past year. Those instances led to Energy and Commerce Committee hearings that exposed just how easy it is to steal a person's identity by acquiring their financial information.

After the data breaches occurred, brokers addressed the situation by sending a notice to affected customers informing them that they could request, they could request a free credit report and free credit monitoring. Approximately ten percent of the affected people chose the option.

The bill Representative Simmons and I introduced follows a similar course of action. Instead of mandating a costly 100 percent coverage of free monitoring and reports, veterans would be provided a notice from which they would opt for the items. These keep the cost down to millions instead of billions of taxpayer dollars. The provisions in our bill are similar to provision 5725 in your Committee draft.

The legislation would also allow the VA to contract with credit agencies for reports and monitoring which further keeps down the cost. It would provide a free credit report every three months for the next year.

It has been reported the stolen laptop containing the veteran information was not accessed or compromised. While that may be so, now is the time for the VA to coordinate with credit agencies for future data thefts which we hope will not occur, but as we have seen are increasingly becoming a fact of life.

A recent report by VA's Inspector General shows many shortcomings with the Department and its security practices and its vulnerabilities. We would be wise to remain concerned about the ability of the VA to secure the personal information of our veterans, and it is my hope every step will be taken to prevent future thefts and prepare contingency plans should a breach occur.

I will end by requesting that the Committee consider including a provision to the salaries and expenses at the Department to the implementation of the IG recommendations. The recommendations are valid. They deserve consideration and they deserve implementation.

I believe these steps are necessary to focus the Department on this critical concern and ensure the appropriate steps are taken to protect veterans' personal information.

Mr. Chairman, that concludes my statement, and I am available to answer any questions you may have. Thank you. I yield back.

THE CHAIRMAN. Thank you very much.

Mr. Salazar, you are recognized.

[The statement of Marsha Blackburn appears on p. 82]

STATEMENT OF HON. JOHN T. SALAZAR

MR. SALAZAR. Thank you, Mr. Chairman.

Chairman Buyer, Acting Ranking Member Filner, I want to thank you for the opportunity to come before the House Committee on Veterans' Affairs to testify with regard to the provisions of the Veterans Identity and Credit Protection Act of 2006.

I wish there was no need for this bill, but the simple fact is that on May 3rd of this year, personal computer equipment containing the personal information of some 26 and a half million veterans and 2.2 million active-duty and reserve-component servicemembers and their spouses were stolen from the home of a VA employee.

This theft, while alarming on its own merit, brought to light a deep and more troubling tragedy regarding cyber security and the communications of the Department of Veterans Affairs.

In the two months since the theft of the computer equipment, this Committee has held five oversight hearings in which we heard from current and former VA employees, private sector experts on IT security, academics, and the Secretary himself. The hearings opened the Committee's eyes to numerous problems that have already been discussed.

The purpose of my testimony today is to discuss provisions of the bill related to new notification requirements of the Secretary. I, like many of my colleagues on this Committee, was outraged when I learned that there was a 19-day gap between the date of the theft and the day Congress and the public was notified.

In response to the theft of this data and the revelation that such delays in notification occurred, I introduced House Resolution 5588. This comprehensive bill, much of which is adopted before the Committee today, addresses a notification structure and requirements within the Department should another data breach occur.

There are a few differences between the bill and House Resolution 5588, so I will address the similarities between the two bills.

Both House Resolution 5588 and the Veterans Identity and Credit Protection Act of 2006 codify in Federal statute the manner in which the Secretary of Veterans Affairs is to notify Congress and affected individuals involved in a data breach.

By outlining the manner, content, and time frame under which the notification of a data breach takes place, it is my hope that we can prevent a repeat of the 19-day delay that we witnessed in May.

Under the provisions of both bills, this Committee and our counterparts in the Senate are to receive notice of any breach without unreasonable delay following the discovery of a data breach and the implementation of any measure necessary to determine the scope of

that breach, to prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

More importantly, however, House Resolution 5588 prescribes the way in which the Secretary is to notify affected individuals. Each individual whose information has been compromised shall be notified in writing without unreasonable delay and that notification will include the following:

A description of the personal information that was acquired during the breach;

A telephone number that the individual may use at no cost to make inquiries about the breach;

Toll-free contact numbers for the major credit reporting agencies;

Toll-free telephone numbers and web site addresses for the Federal Trade Commission;

And information regarding the right of an individual to place a fraud alert, obtain a security freeze, and receive credit monitoring where applicable.

There are relatively few differences between House Resolution 5588 and the Veterans Identity Credit Protection Act in this section of the bill.

Mr. Chairman, I would hope that you in the next two days would address some of these minor differences and come to an agreement on any amendments that may need to be made.

Mr. Chairman and Acting Ranking Member Filner, I would like to thank you for holding this hearing today. And I also want to thank you for providing the last five oversight hearings. I feel this Committee can work in a very bipartisan manner to pass a finely crafted, comprehensive piece of legislation that I think will serve the veterans well.

This bill makes much needed changes to the VA culture of indifference that we heard so much about during our five oversight hearings.

Mr. Chairman, I want to thank you for inviting me to testify today. Your work and your dedication for fixing the bureaucratic inefficiencies and problems within the VA as well as your commitment to protecting veterans is very much appreciated. Thank you.

THE CHAIRMAN. Thank you, Mr. Salazar.

When you referred to five committees, you were referring to the five full committees, not the two subcommittees or round-table; is that correct?

MR. SALAZAR. The oversight committees that we heard.

THE CHAIRMAN. Five full committee?

MR. SALAZAR. Right.

THE CHAIRMAN. When you said five committees, you were referring to five full committee?

MR. SALAZAR. Right, sir.

THE CHAIRMAN. All right. Thank you.

Ms. Shelly Moore Capito, you are recognized.

[The statement of John T. Salazar appears on p. 84]

STATEMENT OF HON. SHELLEY MOORE CAPITO

MS. CAPITO. Thank you, Chairman Buyer, and thank you, Ranking Member Filner and members of the Committee, for inviting me here today and for holding this very important meeting and for giving me the opportunity to testify.

My State of West Virginia has long had one of the highest per capita rates of military service, making veterans' issues and the protection of personal data an issue with direct implication for tens of thousands of my State's residents.

The loss of the personal data of over 26 million veterans and service personnel last month has highlighted the need for this legislation to protect the credit of all those who have bravely served our nation.

Identify theft can be extremely negative, we have heard in testimony and I am sure you have heard in all your testimony, for those impacted. Because the government handles large amounts of personal data, it is vital that we have policies to protect information from theft and help victims cope.

Later this week, we will celebrate the 75th anniversary of the Department of Veterans Affairs. As the Department carries out its mission of caring for our veterans, we must ensure that the Department is adequately protecting veterans from identity theft.

First, I commend the Department for offering free credit reports to those veterans whose personal information was exposed. It is important that government take responsibility for the mistakes.

The legislation I introduced would establish an Office of Veterans Identity Protection within the Department to prevent the loss of personal data and to work with credit reporting agencies, law enforcement agencies, and veterans to mitigate the impact if data is lost.

I commend the Committee's draft for its creation of the Under Secretary for Information Services who would serve as the Chief Information Officer for the Department.

Advances in technology open up exciting possibilities for using information, but the complexities involved in technology often make it that much easier for those who want to access data for illegal purposes.

It is important that the Department of Veterans Affairs and other governmental agencies have a proper management structure in place to protect personal information.

It is important and appropriate that a mandate to properly report information losses to law enforcement entities, the Federal Trade Commission, this Congress, and the public be included in any legisla-

tion that we pass.

In the recent security breach, the VA initially attempted to resolve the situation internally. Clearly the best chance we have to prevent loss or stolen data from being used by criminals is to get law enforcement involved as quickly as possible as they begin recovery efforts.

Veterans themselves should be notified as quickly as possible that they can immediately begin to monitor their bank accounts and credit activity. Congressional Committees should be notified so that proper oversight can be exercised and, if necessary, legislation to provide additional protections or help to prevent future data losses can be considered.

We must also remember that in the recent security breach, the personal data of up to 1.1 million active-duty personnel, 430,000 National Guard members, and 645,000 reserve personnel were also compromised. My legislation would require that the Department of Veterans Affairs work closely with the Department of Defense to ensure that these active-duty personnel have access to credit reporting services.

Our nation's military forces, particularly those deployed in combat regions, the regions of Iraq, Afghanistan, and elsewhere around the globe, already bear a heavy burden as they bravely defend our nation. The last thing they need to worry about is whether someone is illegally accessing their credit or their identity.

I believe strongly that anyone removing personal data without authorization should be punished, and this is where my bill differs from your bill. My bill contains a provision that would allow for criminal penalties for anyone who removes personal data without proper authorization.

We can and should establish a structure within the Department to protect personal data, but these policies will not do much good if they are ignored.

My bill would make it a felony, punishable by fines of up to two years in prison for removing personal data without proper authorization. I believe stiff penalties are important as a deterrent to violating data security procedures.

I agree with the provision of the Committee's draft that would prohibit the release of personal data by any Department contractor and require contracts to include penalties for data breaches that would pay for credit protection services. It is crucial that any contractor with access to personal data be a strong partner in protecting the identities of our veterans.

Mr. Chairman, I want to thank you and I want to congratulate you on the bipartisan bill that you have put together. I want to thank you for your willingness to tackle this important issue for our nation's veterans. I look forward to working with you and the rest of the Committee to pass legislation to provide these vital identity protections.

And I thank you.

THE CHAIRMAN. Thank you very much for your testimony.

[The statement of Shelley Moore Capito appears on p. 87]

THE CHAIRMAN. This has been a genuine team effort, not only members of the Committee working with the VA, but also with the input from members who are not on the Committee because you also bring other expertise.

So I want to thank you, Ms. Blackburn, dealing with this issue on the Energy and Commerce Committee and your expertise reflected in your bill. We are going to be taking some of the provisions of your bill and incorporating them, but not its entirety. And we are doing that with everyone.

And so what we are doing is, you know, sometimes in Congress somebody comes up with an idea and somebody else tries to claim credit for it. I do not claim credit for other people's work product. And so we are incorporating some of your ideas, and we appreciate what you have done.

So, Mr. Salazar, I noted your disappointment that we did not incorporate some more parts of your bill. Please continue to work with staff in a bipartisan basis. We are working all these things out. You may not get total satisfaction. I enjoy your spirit. We all were there at one point.

Ms. Capito, with regard to your criminal penalties provision, as you know, that is the Judiciary Committee. We cannot do legislation in this Committee with regard to Title 18.

When we passed the bill protecting military funerals, Mr. Sensenbrenner did waive jurisdiction to this Committee. It is the only time he has ever waived jurisdiction, and I am not anxious to push it again. You know what I mean?

MS. CAPITO. I know. I got it.

THE CHAIRMAN. All right. You really should, though, also talk with Mr. Davis and Mr. Waxman because even the Secretary spoke with regard to what you did about increasing his ability and law enforcement's ability with regard to FISMA. And the Secretary had noted to us about these penalties are in the Privacy Act, but they are not in FISMA.

And so just because we are marking up and we are trying to give certain authorities on the civil side and making sure that he can take particular actions, it even goes beyond that. So when you not only just want to do criminal penalties, it is making sure that as a management tool, managers have the ability to do certain things within the system.

If someone has done something wrong or violated a policy, whether they are to be disciplined is a managerial decision, but that is all set in the Civil Service Act and union contracts and the like. So I wel-

come your work.

I want to thank each of you for your testimony today. I will now yield to Mr. Filner if he has any questions or comment.

MR. FILNER. We appreciate all of your testimony.

There has been a lot of emphasis on credit monitoring and free credit reports and credit freezes. We have learned from the testimony before this Committee that if a professional is involved with a theft, it probably will not show up on a credit report for at least a year.

What is more important are the analyses that can now be done of the complete data against other files to see if there was identity theft that is traceable to this breach. We have included that in the legislation to go beyond just the credit reports because they may not show up a potential identity theft for a long time.

So it will go beyond just the credit monitoring, credit reports.

Thank you all for your work here.

THE CHAIRMAN. Thank you.

Any other colleagues have any questions?

Thank you very much for your testimony. This panel is now excused.

Our second panel also appeared at our June 28th hearing with Chief Information Officers. We have brought them back to receive their input on the draft legislation the Committee is reviewing.

Mr. McFarland, Admiral Gauss, please come forward.

Robert McFarland is an Army veteran who was nominated by President Bush to serve as the Assistant Secretary for Information and Technology in the Department of Veterans Affairs on October 15th, 2003, and he was confirmed by the Senate on January 22nd, 2004.

Prior to his appointment, he served as Vice President of Government Relations of Dell Computer Corporation. Mr. McFarland left the Department of Veterans Affairs on May 18th, 2006.

Dr. John Gauss was nominated by the President and confirmed by the Senate and served as the Assistant Secretary for Information and Technology and Chief Information Officer of the Department of Veterans Affairs from August 2001 through June 2003. In January of 2005, Admiral Gauss founded Gauss Consulting Services, Incorporated. And in February 2006, he joined FGM, Incorporated as the company's president.

Gentlemen, I want to thank you for your work with the Committee, your testimonies. You do not have to do this. You are doing it because of the work that you have done in the past, and your genuine commitment to service to others. And I know that there are a lot of other things you could be doing out there, but you continue to come back.

And so on behalf of the country, on behalf of veterans and this Committee, I want to thank both of you for being here and taking the time that you are putting into this. It is very meaningful.

So, Admiral Gauss, you are recognized.

STATEMENTS OF HON. ROBERT MCFARLAND, FORMER ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND FORMER CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS; JOHN A. GAUSS, PRESIDENT AND CHIEF OPERATING OFFICER, FGM, INC., AND FORMER ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND FORMER CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF HON. JOHN A. GAUSS

ADMIRAL GAUSS. Thank you, Mr. Chairman, good morning, and members of the Committee. Thank you for inviting me here today to discuss some of the important issues related to the draft legislation to enact the Veterans Identity and Credit Protection Act of 2006.

My comments today are focused on those elements of the draft legislation relating to the management of the Department of Veterans Affairs' Information Technology and Information Security programs.

As a private citizen interested in the welfare of our nation's veterans and the efficient operation of government, I would like to commend the Chairman and this Committee for exercising such bold leadership by moving forward with this ground-breaking piece of legislation.

By elevating the positions of the Chief Information Officer and the Chief Information Security Officer at the VA to Under Secretary and Deputy Under Secretary positions respectively, you are blazing a trail for the rest of the Executive Branch of government to follow.

Based on 34 years of government service in the Department of Defense and at the VA, it has become clear to me that until the position of CIO is elevated to an Under Secretary position within all departments of the Executive Branch of government, the authors of the Information Technology Management Reform Act of 1996 will remain disappointed.

As an Under Secretary, the CIO will have a seat at the table where the real decisions are made with respect to the operation of the Department and he or she will not be relegated to subordinate working groups that can only recommend and not decide.

I know the Committee is struggling to determine the appropriate level of legislative direction to enact into law. Too little direction will allow the advocates of the status quo to find loopholes in the law or legal interpretations to preserve business as usual. Conversely, too much detail becomes legislative micromanagement which I know is not the intent of this Committee.

With that said, although some of the recommendations I put forth in my statement for the record are aimed at proposing changes to the

draft legislation, other recommendations should be considered for direction to be placed in appropriations bills, policy to be implemented by the Office of Management and Budget, and/or discussion points that could be used during future Senate confirmation hearings.

Mr. Chairman, since the remainder of my testimony is lengthy, I would like to request that it be entered into the record and with your permission, I would like to highlight six of the ten recommendations made as part of that testimony.

THE CHAIRMAN. Hearing no objection, so ordered.

ADMIRAL GAUSS. The first I would like to highlight is in Section 4 of the draft legislation, several new sections to Title 38, United States Code relate to contracting activities associated with the handling of sensitive personal information.

In my review of the draft legislation, I was unable to find any prohibitions for off-shore storage of or access to the sensitive information from companies that might operate outside the United States. I recommend the Committee consider adding such prohibitions to the draft legislation.

Second, a CIO must be more than just the IT person for a department or agency. I believe the CIO must also be the change agent of the organization from a business perspective. The CIO working with the administrations and departments' offices must lead the cross-functional integration of business processes in order to improve mission effectiveness and gain efficiency.

A single 1-800 number for a veteran to call to obtain service and one integrated registration process are but two examples of improvements that should be pursued.

The CIO must establish plans and have the authority to implement those plans to control the growth of information technology spending.

The CIO must understand that data is a strategic capital asset. He or she must understand how to best store the information and make it available only to those who must use the data to service our nation's veterans in a secure and protected manner. Many of these traits are discussed in the Information Technology Management Reform Act of 1996.

Mr. Chairman and members of the Committee, I most strongly recommend that future nominees for the newly- established position of Under Secretary for Information Services be required to have these skills and demonstrate during the confirmation process how they will apply these skills at the VA.

Third, the qualifications for the Deputy Under Secretary for Security are equally as important as the qualifications for the CIO. I believe this person must be a certified information systems security professional and demonstrate a comprehensive understanding of cyber security in general, information security, details of FISMA, and

be thoroughly versed in physical and personal security related issues as they pertain to electronic and information security.

I most strongly recommend that future candidates for the newly-established position of Deputy Under Secretary for Security be required to have these skills and demonstrate during the hiring process how they will apply these skills at VA.

Four, with respect to accessing sensitive and critical information, I believe it is imperative that the CIO be responsible for electronic identity management at VA and that electronic identity management be implemented with a sense of urgency to comply with Homeland Security Presidential Directive 12. Electronic identity management will not only strengthen access controls for electronically stored data, it can be also used to strengthen physical access controls throughout VA.

Five, policies need to be implemented and funding must be provided to encrypt data while in motion or at rest. The implementation of data encryption must be closely coupled with the electronic identity management process just discussed.

And, finally, I once had the privilege to meet Mr. Louis Gerstner when he was the Chief Executive Officer of IBM. He shared with me the actions he took to transform IBM's business processes and information technology from a collection of stovepipes to a highly-integrated machine. He reorganized the management of all of IBM's information technology by centralizing the authority with the corporate CIO in less than 90 days.

Over the next two years and on a global basis, IBM transitioned its IT stovepipe infrastructure to a modern, integrated, corporate-wide infrastructure. During the same two-year period, he and his Chief Information Officer led the modernization of IBM's business processes focusing on eliminating duplication, improving productivity, increasing efficiency and effectiveness, and reducing IT cost.

Mr. Gerstner emphasized the need for speed. He believed that the absence of speed would allow the inertia of the status quo to prevail. Since this legislation is clearly focused on effecting real change at the VA, this change must be implemented with lightning speed to be effective.

Therefore, I recommend the Committee consider including two additional items in this legislation to enable a high- velocity change at VA.

First, the VA should be given 90 to 180 days to fully implement this legislation. The advocates of the status quo will argue that speed will create too much risk and that deliberate thought and study is necessary to avoid creating problems.

Given the current situation at the VA, isn't the risk associated with the status quo significantly greater than whatever damage might be caused by moving forward with lightning speed?

Second, the VA should be given the same hiring authority to support the implementation of this legislation that was given to the Department of Homeland Security in the legislation that formed that department. If VA uses the business as usual hiring processes, it will take months or even years to properly staff the offices established by this legislation.

I hope the information I have provided in this opening statement will help the Committee in its deliberations, and thank you for this opportunity to discuss this landmark legislation. I will be happy to answer any questions you might have.

[The statement of John A. Gauss appears on p. 89]

THE CHAIRMAN. All right. As I understand, the mental framework of the man at the trout stream has remained unchanged, so he shows up to the Committee without a statement; is that correct?

MR. MCFARLAND. Mr. Chairman, I have a short opening statement—

THE CHAIRMAN. Oh, you do?

MR. MCFARLAND. —that I would be happy to give to you, sir.

THE CHAIRMAN. This is rather exciting. We are in anticipation. You are recognized.

STATEMENT OF HON. ROBERT MCFARLAND

MR. MCFARLAND. Thank you, sir.

Good morning, Mr. Chairman and members of the Committee. Thank you for the opportunity to comment on the Committee's draft bill to enact the Veterans Identity and Credit Protection Act of 2006.

I have given my suggestions to Committee staff and I have consulted with my colleague, Dr. Gauss, on his testimony and agree with the suggestions and comments.

As always, I appreciate the work this Committee continues to do on behalf of veterans, and I am pleased to contribute whatever I can to this important legislative effort.

I will be happy to answer any questions that any of you or any of the members may have regarding these issues. Thank you.

THE CHAIRMAN. This is not in the bill itself, but trying to be a good listener here, we had some testimony by Dr. Spafford who is one of the nation's leading experts in cyber security. He runs a program called SIRUS at Purdue University and he produces 25 percent of the nation's Ph.D.s in cyber security. And I do not remember the exact number, if anybody can remember. It was like 75 or 80 per year. That is all the Ph.D.s we are producing in cyber security.

So when you think about all of the hacking that is going on and trying to make these systems more sophisticated, we really do not have programs out there to help this curriculum.

And so let me ask if both of you were still in your positions and we were to create a new position. So we have some scholarships under the Health Agency for doctors.

What if we were to create a scholarship for Ph.D.s in cyber security within the VA, you know, two positions, one position, whatever the need is going to be here, and we fund that? Estimated cost of that could be 60,000 per student, maybe double that for a private school. Just give me what your thoughts are for creating a lane, and then we can do a two- for-one service to country.

I mean, we need to generate some levels of expertise here and the country needs to embrace where we need to go. I mean, we could take that and move it to other departments and other legislation, but we have an opportunity to address a particular problem here. And I know I am catching you cold, but what are you thoughts to that?

MR. MCFARLAND. Mr. Chairman, I think that would be an exceptional idea. I think it is very difficult for government to compete with the private sector on these very sophisticated positions. I think that if you were able to be the benefactor of some good talent towards that kind of expertise, I think you would have a leg up.

I think you would be closer to competing with the private sector in trying to get these kind of people which are necessary if you are going to enact the kind of controls that you need to enact to avoid these kind of problems in the future.

THE CHAIRMAN. So whether it is by scholarship or by grant, when you used the word benefactor, immediately I thought of a grant. Even if it were a grant program to a particular university, we somehow then become a benefactor of that individual for years of service.

MR. MCFARLAND. I think it is an excellent suggestion and I think it would help you attract those kinds of people because it is very difficult to do it without those kind of people.

THE CHAIRMAN. Most importantly, though, you believe it is going to be helpful to the VA to bring that level of expertise in because of having to compete for it because everybody is competing for it, right, whether it is Google or Microsoft or everybody else?

MR. MCFARLAND. It gets worse every day. I mean, as you pointed out, there is a limited number of these professionals that are available, and it is very difficult to get them into government service. I think this would be certainly an advantage.

THE CHAIRMAN. If they are only producing, even if the number is less than a hundred, less than ninety, the level of competition into such limited programs, these are the geniuses. These are real geniuses in a very narrow lane and trying to attract them will be very challenging.

Admiral Gauss, what are your thoughts?

ADMIRAL GAUSS. Mr. Chairman, I think the idea of some grants for education is an excellent idea. One of the things for consideration is

that there are many Ph.D.s that graduate annually with electrical engineering degrees. Each Ph.D. has to have some kind of minor.

I think you could also incent educational institutions to take some of their main line double Es and have them achieve additional skill levels as a minor in cyber security. Many of the disciplines you need to have to understand how to deal with this threat are disciplines you would learn in the double E curriculum.

THE CHAIRMAN. All right. Well, I mean, it is something I have just been thinking about. I have not even had a chance to share it with everyone. And we can talk about it here over the next couple of days. But I wanted to get your reactions.

If you were in charge and you had that type of program, would it be helpful to you? Would you utilize it?

Let me ask this. To create a pipeline, of necessity, how many of these per year do you think would we need, if we were to incorporate it in this bill? One, Two, three?

MR. MCFARLAND. I think in the case of the VA, for an agency the size of the VA, I think you would want to do at least two or three per year and try to build yourself up a cadre over a period of four or five years of a staff of people that could be dispersed.

And one of your problems is not all the problems are in one place. So being as dispersed as the VA is, I think you are going to need more than a couple of these over the next few years.

THE CHAIRMAN. And because it may take me three years or four years to get a dividend from that, I could in the first three or four years do a loan repayment. I could do a student repayment in return so we could get an immediate attraction perhaps.

Okay. I yield to Mr. Filner.

MR. FILNER. I think the virtue, Mr. Buyer, of such a proposal is enhanced if, you incorporate it with veterans' preference, and we try to encourage veterans going into that field.

And to just take it one step further, I will support a Buyer Chair in Cyber Security at Indiana University or Purdue if you support a Filner Chair at San Diego State University. Okay? Is that a deal?

We have talked in many of the hearings, of centralization versus decentralization. Does this legislation deal with those tensions in a reasonable fashion? Shall we proceed in this way?

Do we come to grips with the necessity on one hand of centralization versus a need to have some decentralized approaches to the various reaches of the VA? Do we meet that balance somewhere in this legislation in your view?

ADMIRAL GAUSS. Yes, sir, I believe you do. In my testimony, I did not include that recommendation. I tried to stay focused on the objectives you were trying to achieve in terms of elevating the position, establishing the new Deputy Under Secretary positions, and the Credit Act.

But, actually, yes, sir, I do think that it would be important to have it in legislation that all of IT needs to be centralized.

At the last hearing, Mr. McFarland and I shared a differing view on the operations and maintenance. Subsequent to that hearing, I have had the opportunity to intellectualize what Mr. McFarland said. We have discussed it subsequently, and I have shifted my view. And he and I are in complete agreement that all of the resources should be centralized within the Department underneath the Under Secretary for Information Services.

MR. FILNER. And you are both pretty clear on this issue of elevating the CIO to the position of Under Secretary?

MR. MCFARLAND. I am clear on it, and I have agreed with Dr. Gauss on that issue. I think it is important because there is something called the VA Executive Board which I believe is a governing body that is made up of the three Under Secretaries, the General Counsel, the Deputy, and the Secretary. That is a very important body in governing and managing the VA.

I believe given that information technology is really the railroad that most of the delivery of services to veterans run on, I think it is imperative that this new position be on that VA Executive Board in order to be there when decisions are made about how the Department is going to be managed and how that technology will be used to manage the Department.

MR. FILNER. Well, of course, if you have not changed any of the culture, the CIO could just left off the Executive Board. I think the Executive Board must be just an informal designation by the Secretary, is that correct?

MR. MCFARLAND. No, sir, I do not believe it is informal. I believe it is a very formal board.

MR. FILNER. Okay. But you could easily let that person off or on with or without any title, I assume. But, no. I hear what you are saying. The title does mean something to the whole organization and provides a sense of how important we think that position is.

MR. MCFARLAND. Well, sir, it also puts the CIO at the table and additionally from where they are at the table with the normal Assistant Secretary position. So it is another chance to be at the table when decisions are made. That was my point.

MR. FILNER. So, You think it is important, for a title that will lead to other more formal kinds of responsibilities.

ADMIRAL GAUSS. Sir, may I add to that?

MR. FILNER. Yes. Please.

ADMIRAL GAUSS. Having spent most of my professional career in the Defense Department, my observation is that the real decision making within the Department lies with the Under Secretaries, the Deputy Secretary, and the Secretary.

And I watched the CIO within the Defense Department try to be

the change agent, try to lead the modernization of the business processes. And every forum that he would call, the principal Deputy Under Secretaries would show up and it was an inertia that prevented change, that prevented moving forward.

The CIO has to be more than the IT person because IT is a value when you apply it to improved ways of doing business, to cut costs, to gain efficiency, to improve service. IT should be applied to the business rules. Someone has to have a seat at the table who can be the advocate of that change and the driver of the integration of those processes to gain some efficiencies and help get the IT budget on a negative slope rather than the constant sharp increase slope that it is on today.

MR. FILNER. I appreciate it.

Yield back, Mr. Chairman.

THE CHAIRMAN. Mr. Stearns?

MR. STEARNS. Yes. Thank you, Mr. Chairman.

When you give notices out to veterans and lots of times, a lot of these veterans might not be in the United States, so they might perhaps be in Iraq. They might be in the Pacific Rim.

I have a bill, House Resolution 4127, the Data Accountability and Trust Act through the Energy and Commerce. And we approved it on the 29th of March in Subcommittee and it went to full Committee and passed too. And in the bill, and I am reading from it, we had that a possible direct notification could include e-mail notification.

So I was just wondering how you feel about the possibility of having e-mail as a way to solve the problem of notification for veterans. I mean, is that just something that is easy to do in your opinion?

ADMIRAL GAUSS. As a means to notify, yes, sir, I think that would be a very convenient means. However, I would respectfully offer a caution—

MR. STEARNS. Yes.

ADMIRAL GAUSS. —that personal privacy information not be included in the content of the e-mail. The Social Security number, the date of birth, or any other identifying information must not be included with the e-mail because it is too easy to capture as it floats its way through cyber space.

MR. STEARNS. How about if it was encrypted?

ADMIRAL GAUSS. Then the veteran would have to have this encryption device.

MR. STEARNS. But how would you—

ADMIRAL GAUSS. Notification, you know, if it came from VA to me as a veteran—

MR. STEARNS. Right.

ADMIRAL GAUSS. —to my home e-mail address that said this is to advise you that personal privacy information might have been compromised, please call such and such a number, that would certainly

be an expedient notification method.

MR. STEARNS. And it might be a way to notify him. Otherwise, I guess just sending it through the mail to him would be the alternative.

Yes.

MR. MCFARLAND. I think it is an excellent way to do it, and I agree with Dr. Gauss' statements on it. I can tell you that I did receive a letter obviously.

MR. STEARNS. Right.

MR. MCFARLAND. I was in the 26.5. I would have received an e-mail much faster than I received that letter. So I think it is an added method of communication that is important to get the word out quickly.

MR. STEARNS. I do not know, Mr. Chairman, what finally the Veterans spent in mailing out their notifications because of the loss of data. Does anyone know? I mean, Mr. Chairman, does counsel know? I am just curious what the final figure came in. I had heard about $7 million it was.

THE CHAIRMAN. I do not know. The VA turned to the IRS.

MR. STEARNS. And they sent it out?

THE CHAIRMAN. They sent it out.

MR. STEARNS. Yeah. But any way that could be used more inexpensively for the veterans. E-mail might be certainly done in a way which they could be notified but without the personal identifiable information with it.

All right. Thank you, Mr. Chairman.

THE CHAIRMAN. Mr. Michaud.

MR. MICHAUD. Thank you very much, Mr. Chairman. I want to thank you for having this hearing. I want to thank all the panel members who have spoken and will be speaking later on today.

I just have one question, Mr. McFarland. I gather you agree with all of Dr. Gauss' comments. Do you have any additional recommendations above and beyond what the doctor has suggested or what is in the legislation that we should be looking at?

MR. MCFARLAND. Well, sir, having had reasonable recent exposure into the operations of the VA, I would recommend along with authorities and responsibilities that you talk about in the legislation that you make clear this issue of enforcement and be sure that there is clear authority to enforce these rules and regulations that you want to be put in place to try to control access and control the leakage of data.

One of the issues I wrestled with is this whole issue of enforcement, and I know this Committee has dealt with this through some past testimony and past hearings. Without an ability to enforce, authority does not mean anything. So I do not think you can be too careful in pointing out that enforcement is a part of granting authority.

MR. MICHAUD. Great. Thank you very much once again for your

testimony.

With that, Mr. Chairman, I will yield back the balance of my time.

THE CHAIRMAN. Dr. Snyder, you are recognized.

MR. SNYDER. Mr. Chairman, I was not here at the gavel. I think Mr. Salazar was here. Thank you.

THE CHAIRMAN. Would you like to yield?

Mr. Salazar.

MR. SALAZAR. Dr. Gauss, in your testimony, you talk about the VA using—if you use the business as usual hiring process that it will take months or even years to staff your offices.

How many staff members are you going to have to hire to implement this legislation?

ADMIRAL GAUSS. There are several key staff members that you would need. You would need the Deputy Under Secretaries and maybe one or two other people. So it would not be to do a replacement of eight or nine thousand folks, but rather for those key positions, with key skills that are needed to enact the legislation, the process has to be more than classify the job, write a position description, advertise it, have a board, have another board, have another board, have interviews which takes 15 to 18 months. So it's the key five or six positions that my comment was really aimed at.

MR. SALAZAR. Okay. But it would not be hiring a thousand new people that are qualified in IT?

ADMIRAL GAUSS. No, sir. For example, in my testimony, I recommended some qualifications for the Chief Information Security Officer. If we could go out and canvas, if VA could go out and canvas industry, find a candidate, do a direct hire, you got the position filled.

MR. SALAZAR. Thank you, Mr. Chairman. I yield back.

THE CHAIRMAN. Dr. Snyder.

MR. SNYDER. Thank you, Mr. Chairman.

Mr. Gauss, in both your oral and your written statement, you refer to this data information as being, I think your words were a strategic capital asset. And I wanted to explore that just a minute.

I saw the movie the Pirates of the Caribbean over the weekend in which Davy Jones loses his key. And so they fight over this key. It seems like he should have gotten a cell phone and say change the lock on my treasure chest.

If I lose my credit card and I throw it in the hallway, I guess you would define that as a strategic capital asset until I pick up the phone and notify someone that my credit card has been lost and at that point becomes essentially of no value.

I think there was a lot that I saw in the last few days that said why is it that the only thing that can never be changed in society is our Social Security number.

What are the practicalities or is that something that we ought to explore, that if a person is—you know, let us say 26 million, that we

actually had evidence that that information was lost permanently and 26 million losses of strategic capital asset.

Why shouldn't government be available to say, hey, no problem, we will change that number, issue you a new random, distinctive number that will only be yours for all time? And what are the problems? Have you explored that or thought about that much?

Admiral Gauss. Let us see. Sir, I actually have not given a lot of thought to your question. But I do agree with you. Having once been an identity theft victim myself, it would have been very nice to have a new Social Security number rather than living with the risk.

But then there is chains through all sorts of databases, through IRS, through VA, my case through the Department of Defense, and how one would administer that across government would require some thought. But I do agree with you that that makes a lot of sense.

Mr. Snyder. Obviously I am mentioning that not—that is not something we could do in this bill because then we get into jurisdiction issues. But one thing we are doing in this bill there is asking for, I think, a six-month study to explore like why does the VA even use Social Security numbers. Why does it not do a distinctive personal identifying number so that, you know, no credit card company is going to say, oh, good news, I got your VA number. Well, that is not your Social Security number. It would be a separate issue. So we are going to explore that.

It seems like that there may need to be a broader government look at if somebody has had an identify theft problem, why can't that number be immediately declared, hey, we have given this person a new number and that number is no longer recognized as related to that person. But that would have to be a study for another bill or another time.

The Chairman. Would the gentleman yield?

Mr. Snyder. Yes.

The Chairman. We have had testimony. As a matter of fact, one of our colleagues has a bill out there just to do that, so you can no longer use the Social Security number.

And during the July break, I went and met with Dr. Spafford who serves on PITAC. It is the Presidential's Information Advisory Committee. And he said he felt that there would be a massive upheaval in the systems right now for us to just go blanket you are no longer permitted to use the Social Security number.

And immediately I asked him, I said what is your identification number here at Purdue University. Is it your Social Security number? Let me see your ID. And he started smiling. He said, well, eight years ago, we moved away from that. And so they went through that judgmental process. And he said, please, I think it is best for you to examine all the alternatives and what the issues are rather than just do a blanket change. And that is the reason it is in the bill. So I

wanted the gentleman to know.

MR. SNYDER. No. And I agree with what we are doing in the bill. When we talk about massive upheavals, a massive upheaval would have been if we had found out that those 26 million names had been sold in batches of 200,000 all over the world and that there were already 13.7 million credit cards that had been actively activated based on—I mean, that would have been an upheaval.

THE CHAIRMAN. True. But the reference of massive upheaval is the seamless transition that we are doing between two of the largest departments of government—

MR. SNYDER. Yeah. No. I understand.

THE CHAIRMAN. —and patient medical records and trying to figure out how to do that if one department is going to change and DoD does not.

MR. SNYDER. No. I understand.

The issue of speed, Mr. Gauss, and you put a lot of emphasis on speed, and isn't this something—and I understand the importance of doing things with rapidity, but we have had several false starts through the years thinking that the Department of Veterans Affairs was going to get this right and that has not worked out.

I mean, isn't this the time to say we want to have it done right even if it takes longer than six months?

ADMIRAL GAUSS. I share a different view. When I was at VA, I convinced the Secretary to centralize the IT within the Department in August of 2002. I testified in front of the Oversight Subcommittee at the end of September of 2002 that we would have it in place by the end of November.

Well, what happened between it was those that wanted to ensure there was no collateral damage done put it into the VA concurrence process and it just dragged and dragged, and the advocates of the status quo put up obstruction after obstruction.

I have experience, personal experience in effecting change. I was the commander of a Navy material acquisition command. I found a major structural problem with the organization within 60 days of taking command. I restructured an 8,500 person organization on one afternoon with the senior leadership on a Thursday, and we put it into effect the following Monday.

Now, granted, the first week was chaotic, but it took two months to sort out what needed to be done to do things right and results were seen on the waterfront within six months.

I am an advocate of speed even if in the process you do some collateral damage, else the advocates of business as usual will drag this thing out until there's a new Congress, a new Administration, new political appointees, and it will be the year 2010 before—and there will be more hearings just like this.

So it is time to strike and it is time to strike fast in my opinion.

MR. SNYDER. Thank you.

MR. STEARNS. [Presiding] Yes, Mr. Udall. We show Mr. Udall after Dr. Snyder.

MR. UDALL. Just following up on what you said about moving quickly, I mean, would you make any suggestions to us in terms of the bill that is before the Committee, how to get this into place as quickly as possible, and are there any pitfalls in doing that?

ADMIRAL GAUSS. One of my recommendations was to implement the legislation within 90 to 180 days, and there are specific portions in there like establish the offices for the Deputy Under Secretaries and fill them with qualified personnel and have a series of reports back to the Congress on progress made. Transitioning the people from their current organizations to the new Under Secretary should happen within the same 90 to 180 days.

Since the government cannot move quite at the speed that industry does, there are certain things that will take time in order to move through the personnel system. But in my opinion, this can be done within 180 days, and hold VA accountable for execution.

MR. UDALL. The idea of creating and then filling the positions quickly, have there been problems with that in the past and how do you cut through that?

ADMIRAL GAUSS. I try to recruit some people that I knew and trusted from outside of government, only a handful, two or three. And if it was not for me personally sitting on people's desks through the HR system, what turned out to be a six-month ordeal would have turned into a year to 18- month ordeal.

MR. UDALL. So basically you are saying it takes a lot of personal commitment by the managers to make sure personnel are put in place and that it is moved on quickly?

ADMIRAL GAUSS. My experience with the VA is that they take the most conservative interpretation of HR policies and that perhaps with the assistance of the Office of Personnel Management with some forward thinking, OPM people helping VA, they could expedite the process.

MR. MCFARLAND. I would like to add to that if I could.

MR. UDALL. Please, please, Mr. McFarland.

MR. MCFARLAND. One of my consternations in coming into government from the private sector with no previous experience was the speed of execution on the employment side, personnel side.

And for the first few months I was there inadvertently blamed OPM until I had an opportunity to sit down with an OPM executive one evening and talked about the consternation I had faced in my first three or four months at VA over these hiring policies and the things we had to go through to get simple positions filled.

And he made it very clear to me that these were not OPM problems, and he pointed out the fact that VA has its own set of very anti-

quated, old rules of procuring people and their own HR policies which are not OPM's issues. They are VA's policies.

And I believe that until you fix some of those policies inside the agency, you will continue to have a long tenure in trying to fill personnel requests.

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

MR. STEARNS. Will the gentleman yield?

MR. UDALL. Yes, I will. And I was going to say to the Chairman I think this is a good area that we ought to focus on. But, please, I yield.

MR. STEARNS. Well, I think what you have brought up is very important. Can you go so far as to indicate what you think should be done? You said these changes should be made. If you could wave a magic wand, what would you do? Can you specifically outline them?

MR. MCFARLAND. Well, one of the issues I struggled with is I believe OPM has electronic access to resumes, a repository that you can get on. They have an arrangement with monster.com to recruit people. None of those techniques are ever used at the VA that I am aware of.

MR. STEARNS. And why wouldn't they be used?

Mr. McFarland. Because VA has its own policy out of the HR Department on how the process of hiring goes. It is VA's policy and that is the way it is.

MR. STEARNS. So is it actually written in VA's policy that you cannot use an outside personnel to assist or get advice?

MR. MCFARLAND. Every time I tried, I was told that was unacceptable. It was not VA policy.

MR. STEARNS. So not VA policy is sort of a blanket that chills across the board if a person wants to be innovative in trying to recruit is what you are saying?

MR. MCFARLAND. One of the most frustrating points of my two and a half years there was that process.

MR. STEARNS. Now, besides personnel, is it also true in procurement of supplies and things like that? You sort of used the word procurement. Well, it was primarily in the personnel.

MR. MCFARLAND. Primarily in the area of personnel. The procurement aspects, sir, I am not sure we have enough time to delve into that.

MR. STEARNS. But you also feel—I am not trying to push you into dangerous ground for yourself—but you are also saying today that in the procurement process, the same type of blanket policy has sort of chilled the innovation that is needed for procurement? Would that be a fair statement to say?

MR. MCFARLAND. That would be fair in my opinion, sir.

MR. STEARNS. And the same type of innovation that we need in the recruitment of personnel, we need in the innovation and procurement

policies, too, for supplies and things like that?

MR. MCFARLAND. I would agree.

MR. STEARNS. Okay.

MR. FILNER. If the gentleman will continue to yield.

MR. UDALL. Yes.

MR. FILNER. Those are, I think, subjects for further oversight. I would tell Mr. Udall that in terms of your opening line of questioning, Mr. Buyer and I were talking with the staff here and we agreed to put these time lines, some of these time lines into the legislation that we will mark up on Thursday. It is really important to have those in the bill and I appreciate your getting that on the record.

MR. UDALL. Thank you, Mr. Filner, and I can see that. And then I was just following up on the problems that might occur as a result of that.

Thank you very much and yield back.

MR. STEARNS. The gentleman yields back.

If the members will indulge me just for a moment, we would like to welcome our newest Committee member, Mr. Brian Bilbray.

Mr. Bilbray returned to Congress following a June 6th special election in the 50th District in California. A native of San Diego, he brings to his constituency a unique level of experience, having served the people of San Diego County as a Mayor, County Supervisor, and then as a Congressman.

His two decades of business and local government service were instrumental in developing San Diego's aggressive initiatives regarding environmental protection, pollution control, and economic development.

Mr. Bilbray has been at the forefront of the battle to protect the Mount Soledad Veterans War Memorial, and he has cosponsored legislation with Congressman Duncan Hunter to make this a national war memorial, allowing it to remain for San Diego to enjoy for generations to come. I believe it will be on the floor tomorrow, if I understand right.

So with great admiration, we welcome you, Brian, to our Committee. It is a wonderful and bipartisan Committee. This morning, we will draft legislation prepared in response to the theft in May of personal data belonging to as many of 26.5 million veterans and 2.2 million servicemembers as well as family members.

You are welcome to join us this morning, and we just welcome having you the opportunity to serve with us.

MR. BILBRAY. Thank you.

MR. FILNER. Will the gentleman yield?

MR. STEARNS. Be glad to yield.

MR. FILNER. When the Congressman was a Supervisor in San Diego County, I was a City Councilman in the City of San Diego and our districts completely overlapped. We worked together on virtually

everything. He taught me how to ride horses and to surf. I taught him how to read and write, I think. So we will bring a new spirit of comradeship, as he likes to call it, to this Committee.

MR. STEARNS. Well, that is a high commendation, Mr. Bilbray, to get from Mr. Filner, or low as we might want to consider it. So you are certainly welcome. And just delighted on behalf of Mr. Buyer, who is the Chairman, to have you sit with us today.

MR. BILBRAY. Thank you, Mr. Chairman. And before you take that as a compliment, you have not seen my literary accomplishments or Mr. Filner surfing or horseback riding.

MR. STEARNS. Mr. Bradley, I think has just left.

And, Ms. Herseth.

MS. HERSETH. Thank you, Mr. Chairman. And welcome, Mr. Bilbray. I thank the two of you for being back to the Committee and answering some of the questions that I know my colleagues have already asked about some of what the Committee has been working on.

And I appreciate Chairman Buyer's leadership here and getting a piece of legislation that all members of the Committee can evaluate to address some of the very difficult challenges we clearly face with information security in the Department of Veterans Affairs.

But let me go a bit further because you may have heard me in a prior hearing ask a little bit beyond what we have here at the Department of Veterans Affairs, what we may have at other Federal agencies.

You may have seen the article in the Post today about all of these other agencies that have had some problems. I also serve on the Agriculture Committee and even the Agriculture Department is subject to these attempts to hack into the system or the potential that information is compromised.

And my question, I guess, goes to whether or not you think that the Congress, not necessarily this Committee, can use the draft bill here as perhaps a model for what other committees could do, but should we be looking beyond this to a broader act or action by the Congress to address compliance with FISMA across agencies, and should we try to do this for all agencies at the same time or in light of some of the unique issues we have at the VA that Mr. McFarland talked about, should we focus in on the Department of Veterans Affairs, try to achieve within 180 days the type of organizational change that you suggest, Mr. Gauss, that we could do to hold up then as a model for what needs to be done and using the types of professionals that we bring in to effectuate this change for other agencies then to follow?

So I guess my question is, should we try to do this all at once or should we focus in and try to do this quickly with speed at the VA and then move to address this problem and other challenges that exist at other Federal agencies?

ADMIRAL GAUSS. I believe the points that you make about it apply to a broader part of government are right on target. My personal recommendation is to use this as the model for expanding and move out with speed to fix the problem.

MR. MCFARLAND. My feeling is the same. I do not think there is anything necessarily unique at VA about the potential problems that you deal with in this area. I think they are the same in every agency.

So I think that if you move out with speed as Dr. Gauss says and deal with the VA's issues, I think you have the ability to move those changes and that experience across the rest of government very easily.

MS. HERSETH. I very much appreciate your responses because even as this article points out, the potential of compromised data at the VA got the most attention nationally. And I think that in light of an attempt to do this across the government in every agency may be a bit overwhelming because I think to do this with the speed that I think it needs to be done is going to be a challenge enough.

And if we are able to do it and with this Committee's focus on the issue with the aggressive oversight we have been exercising the last few weeks, if we keep the heat on, we make sure it gets done, then as you both say, it can serve as a model that we then share with our colleagues and other committees or on those that we also serve on, but also that broader action that may be necessary in light of what every other agency seems to face and keeping a pace with the need to secure this type of information.

So I appreciate it. That is the only question I have. I would yield back. And, again, appreciate your testimony and your expertise.

THE CHAIRMAN. Ms. Herseth, you and I have not had an opportunity to talk, and we discussed it right before we came into the room. Mr. Filner and I and staff are working with government reform and oversight. The FISMA provisions would have a joint referral upon introduction to government oversight, and they are working with us. And the intention would be that they are going to waive jurisdiction over the FISMA provisions to use, and we are going to mark up this bill on Thursday and try to get it to the floor next week.

Does that meet your approval?

MS. HERSETH. Well, it certainly does. I mean, I wanted to get their perspective based on, I think, other folks they have worked with and other agencies, and appreciate, understanding that there would be joint referral over some of the provisions in the bill.

But I think that we have been the most aggressive under your leadership and working with Mr. Filner and people on both sides of the aisle of staying on this issue, knowing that other agencies are similarly affected. It just has not gotten the same kind of attention that some of the problems we have had here at the VA. And that rather than trying to address this government-wide, we address it at the VA

first and use it as the model as both of the witnesses suggested.

Thank you.

THE CHAIRMAN. And your line of questioning, when I look back to the seven hearings we did with regard to the General Counsel and his operations, you are going to have latitude and freedom in a hearing we will have with the General Counsel's Office with regard to the last lost backup tape and the laisser-faire attitude and lack of policies within the General Counsel's Office. And we are going to take that up in September. So I look forward to your expertise.

Mr. Bilbray, you are recognized.

MR. BILBRAY. Mr. Chairman, I pass at this time.

THE CHAIRMAN. Mr. Stearns.

MR. STEARNS. Mr. Chairman, I wonder if I could have additional time just to ask both yourself, your counsel, as well as the Democrats if they would allow or consider making a part of the base bill my suggestion that would include e-mail as a part of method of notification.

And this notification could be worked out in such a way that the personal identifiable information is not included in it, but it would at the same time give conspicuous notice that some of their data was lost and so that they would be notified of it. And it might be such that this e-mail might be in lieu of or in combination of the written notification.

So if it is possible at this late date, whether you and your counsel, Mr. Chairman, think this should be appropriate as an amendment or it could be part of the base bill. Maybe this would be appropriate since we heard a little bit from our witnesses today to get a comment.

THE CHAIRMAN. Well, Mr. Stearns, I listened to counsels respond to you, and I appreciate your work in the Commerce Committee that you have done and you are grappling with the same issues that we are.

You are correct. In our draft legislation, we do not go with specificity under the notification provisions. We can go exactly as you are recommending, first written and then secondly e-mail if it is available. I do not have objections to that.

I will yield to Mr. Filner.

MR. TUCKER. Regarding the concern with e-mails being implicated in so-called "phishing" schemes, there could be protections incorporated into that provision.

THE CHAIRMAN. I do not know even what that means.

MR. STEARNS. Well, sometimes when you send an e-mail, it requires a reply and sometimes that reply is used to identify who the person is and then they try and steal the identity. But there is a lot of ways to do this. In fact, you could send it encrypted and then it could be decrypted at the site.

But I think after hearing these folks talk about the antiquated pro-

cedures with procurement of personnel and supplies, and we have this internet and it is going to be broad band, it is going to be probably ten or fifteen years from now, not only will everybody have an e-mail and it will be broad band, but that will be the form of communications.

So I do not think we should rule out the possibility of the internet being used and e-mail being used too. So it is just my suggestion that I think the bill would be ahead of everybody else.

THE CHAIRMAN. I think, Mr. Stearns, you should please offer the amendment that was incorporated in your bill in the Commerce Committee, give that to our staff, and we will work this out. I do not think there should be a problem here.

MR. STEARNS. Okay. That is good. I appreciate your concern.

THE CHAIRMAN. Okay. To authorize a second round, if anybody has it, only because of the level of expertise we have in front of us.

During one of the hearings, we had testimony that VHA was granted a waiver for laptops in the name of patient safety and healthcare delivery.

Gentlemen, do you believe that this will affect patient safety and healthcare delivery?

MR. MCFARLAND. No, I do not.

ADMIRAL GAUSS. The only possible way it could adversely affect patient care is if the money to buy the PCs necessary to comply with the policy came out of patient care dollars. If on the other hand, it came out of their development pots of money, there would be no adverse impact to patient care.

THE CHAIRMAN. So doctors and their laptops, they need to bring them in and they need to have them checked? Is that what you are telling us?

ADMIRAL GAUSS. I am going one step further that doctors should be given VA laptops that are properly configured with all the security devices for any connection into the VA network and that the use of home computers should be prohibited.

THE CHAIRMAN. Would this be an example when you say that the CIO needs to be at the table rather than subordinated? I mean, if you have the attention, the Secretary has resources. He has the Secretary Deputy. He calls in his three Under Secretaries.

But the CIO presently is in a subordinated position and he is not at that meeting. And the Under Secretary for Health makes an argument on patient safety as to why his doctor should be exempted from a particular policy, yet the CIO is not even at the table.

ADMIRAL GAUSS. The argument, I believe, needs to be heard by the Secretary and not subordinated in staff work that is then withheld from the Secretary's view. And putting an Under Secretary at the table with the Secretary would get these issues in the open, I believe.

THE CHAIRMAN. All right. I am going to be a good listener here.

Admiral Gauss, you talked about the implementation. What would be a reasonable time table for the implementation of this bill?

ADMIRAL GAUSS. Mr. Chairman, I believe that establishing the office, establishing the offices of the Deputy Under Secretaries, recruiting and placing people into those positions, realigning the personnel under the new structure should all be done within 90 to 180 days. If this were industry, it would be less than 90 days. But there are some procedural things in HR that may take longer.

While you were out, I related a story of where in government, I reorganized a command of 8,500 people, and the new structure was defined on a Thursday afternoon and it was implemented the following Monday.

THE CHAIRMAN. Mr. McFarland, would you concur? Would it be prudent for us to put in this legislation a specific time period for implementation?

MR. MCFARLAND. Sir, I not only think it is prudent, I think it is necessary.

THE CHAIRMAN. All right. In one of our other hearings—gosh, in my mind, they all kind of run together; they came so fast—Ms. Herseth, I think it was the Secretary, it was the Secretary who was testifying, and at the time the laptop and the storage device had been found, we did not know what the forensic results were. We kind of knew at first blush it appeared as though it was not accessed. Her chief concern was, you know, should we cover the 26.5 million, give them their assurances, and go ahead and spend the dollars.

We have learned subsequently. Congress has received a letter from the Director of OMB withdrawing now the request for the $160 million from Congress. And at the time, in direct response to Ms. Herseth, I mentioned the ID/IQ contracting process.

And GSA is going to be following you and your testimony here today about these blanket purchase agreements whereby we can take care of these breaches of the past, and we sophisticate and implement a centralized model recognizing that breaches are going to occur in the future because we are dealing with humans.

Are we going on the right path, gentlemen? Are we proceeding? Is this the best way, you think, to handle this?

MR. MCFARLAND. Yes, sir, I believe it is.

THE CHAIRMAN. Good.

ADMIRAL GAUSS. I concur.

THE CHAIRMAN. All right. Well, Ms. Herseth, you were an impetus to good change by your questions, so I want to thank you for that.

MR. FILNER.

MR. FILNER. No further questions. In your absence, I had assured Mr. Udall that we had discussed and had committed to putting time frames into this legislation.

Also, there are some things that we might even have more speci-

ficity.

THE CHAIRMAN. More specificity?

MR. FILNER. On some of them, very specific things to even give lesser time and have reports back to us on a regular basis. I think that will probably be in the draft legislation or legislation for markup on Thursday.

Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you.

Any other members seek recognition of this panel?

My last question would be this new directive that the Secretary has implemented, have either of you gentlemen seen the new directive with regard to authorities of the CIO?

MR. MCFARLAND. No, sir, I have not.

THE CHAIRMAN. 6504?

ADMIRAL GAUSS. No, sir, I have not either.

THE CHAIRMAN. Okay. Well, all right. I think if you had seen it, you would have said I wish I could have had it.

I want to thank you very much for your testimony. It is valuable. And I appreciate your support of the bill and your counsel to us in the drafting of the legislation. Thank you very much.

Admiral Gauss, you may go back to work.

Mr. McFarland, you may go back to fishing.

Our third panel represents the views of the Administration. We have before us the Deputy Secretary for the Department of Veterans Affairs, Mr. Gordon Mansfield. From the General Services Administration, we have Mr. James Williams, the Associate Administrator for the Federal Acquisition Service, who will discuss what offerings they are providing under their contract.

Mr. Secretary, welcome back. You are recognized.

STATEMENTS OF HON. GORDON H. MANSFIELD, DEPUTY SECRETARY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY JOHN THOMPSON, DEPUTY GENERAL COUNSEL, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND JAMES A. WILLIAMS, COMMISSIONER, FEDERAL ACQUISITION SERVICE, U.S. GENERAL SERVICES ADMINISTRATION

STATEMENT OF HON. GORDON MANSFIELD

MR. MANSFIELD. Thank you, Mr. Chairman. I am pleased to provide the Department's views on eight bills all intended to protect the personal privacy of veterans and others affected by the May 3rd, 2006, theft of computer equipment containing veterans' personal data.

While you had also invited our views on the draft bill your staff shared last week, I regret that time has not permitted us to have

cleared positions on its many provisions. We will supply those for the record once the necessary Executive Branch coordination is completed.

Initially I wish to point out that the eight bills covered in my testimony were introduced before the stolen computer hardware was recovered. As you know and as mentioned, the FBI has concluded with a high degree of confidence that, based upon its forensic examination and other evidence developed during its investigation, the veterans' data were not accessed or compromised prior to their recovery.

The actual communication says that on June 28th, 2006, the stolen laptop computer and external hard drive were recovered intact. Based on the facts gathered thus far during the investigation as well as on the results of the FBI and the VA OIG computer forensics examination, the FBI and the VA OIG are highly confident that the files on the external hard drive were not compromised.

That development has eliminated the need for much of what is proposed in the legislation, and while we understand the concerns that engendered these eight bills, we do not support their enactment.

Mr. Chairman, with concern for time, I can go ahead and summarize, I think, all of the bills in three categories. That is, some of them that deal with the credit monitoring or insurance or other notifications, as I said, are now not required, we believe, based on the FBI information.

The other area is penalties for either criminal or civil areas. The Secretary, as you know, has testified that he believes that we need further assistance in that area, and I know you are proceeding. However, I have no cleared positions on those that were presented.

And then the last issue that has been discussed here deals with the personal identifier. And, again, while I do not have an Executive Branch position, I can tell you that it is a subject of discussion and one that we think requires not just a decision that deals with the VA but deals with the total Executive Department as well as with private commerce because it is interrelated in finance and other issues.

As I have indicated in my testimony, we have implemented many of the provisions of the various bills. VA is strongly committed to providing all available protections to the safety and security of personal information of veterans and their beneficiaries.

As we continue to work on improvements in our systems and procedures, we will be pleased to work with your Committee in fostering methods to achieve a level of information security that is responsible and necessary.

The Secretary has determined that the VA will move forward with data breach analysis service to protect veterans, and we should be finished with that RFP soon.

That concludes my testimony. I would be glad to answer your questions, sir.

THE CHAIRMAN. Would you wish to submit it for the record?

MR. MANSFIELD. Yes, please.

MR. WILLIAMS. Yes.

THE CHAIRMAN. Both answer in the affirmative. Hearing no objection, so ordered.

Mr. Williams, you are recognized.

[The statement of Gordon Mansfield appears on p. 93]

STATEMENT OF JAMES A. WILLIAMS

MR. WILLIAMS. Thank you. Good afternoon, Chairman Buyer, Ranking Member Filner, and members of the Committee. I am Jim Williams, Commissioner of the Federal Acquisition Service of the General Services Administration, GSA.

I am pleased to have this opportunity to appear before you today to discuss the program that we have put in place to assist agencies in being able to respond to data protection and credit protection scenarios.

GSA helps Federal agencies better serve the public by offering the best value, superior workplaces, expert solutions, acquisition services, and management policies. One of the most important ways that we do this is through the multiple award MAS Program.

Through the MAS Program, GSA establishes contracts with firms large and small to provide commercial products and services to the government at competitive prices. The schedules can be used by all Federal agencies as a streamlined convenient, money-saving, and time-saving tool for obtaining the commercial goods and services they need. When combined with E-Buy, GSA's electronic request for quote system, the process is also transparent.

One of the key features of the MAS Program allows agencies to establish blanket purchase agreements. These BPAs are used to fill recurring needs for supplies or services while taking advantage of quantity discounts, saving administrative time, and reducing paperwork.

One MAS Program Schedule which is particularly appropriate to discuss in light of the reasons we are here today is the Financial and Business Services Schedule. This is a schedule of approximately 425 contracts representing expertise in financial areas. This schedule also includes 21 contractors with expertise in credit reporting and at least three firms with expertise in credit monitoring.

As this hearing and the Committee's draft legislation signify, identify theft is a serious issue. When an agency experiences a data loss, there can be serious problems for our employees and the citizens of this nation. The Federal government must be in a position to respond to situations quickly and effectively.

With GSA's BPA for credit monitoring in place, an affected agency

has quick and ready access to the industry experts it needs. This way, all agencies facing a data breach will have a fast and cost-effective remedy available.

On July 10th, 2006, GSA invited 21 contractors under the Financial and Business Services Schedule to compete for multiple blanket purchase agreements. Under this competition, these 21 firms have been asked to propose three different levels of remedy based on the extent of the risk of exposure.

The firms have been asked to quote different levels of credit monitoring services ranging from basic or single monitoring to comprehensive coverage, reports called three- in-one, which cover all three of the major credit bureaus.

A key feature will be that based on the degree of vulnerability, risk and protection, ordering agencies will be able to select the most appropriate level of credit monitoring services.

Responses to this BPA request are due on Monday, July 24, 2006. GSA will then evaluate the responses to be sure we award the companies demonstrating the knowledge, understanding, and technical capability required to perform the credit monitoring services. We plan to make those awards in August and expect several Federal agencies to begin placing orders the same month.

In conclusion, I would like to state that this situation is a good example of the important mission that GSA plays in helping our government stop identity theft and protect the privacy of individuals. We are mobilizing and providing a shared services solution so that we can leverage the government's buying power, drive down prices, drive up service delivery, and provide a fast and agile response to security breaches.

I am very proud of the hard work that the GSA team has already put into this effort, and look forward to a highly successful award of several BPAs next month. We join the Committee in its commitment to better protect sensitive personal information of our veterans.

I look forward to any questions you might have. Thank you.

MR. BILBRAY. [Presiding] Thank you, Mr. Williams.

[The statement of James A. Williams appears on p. 99]

MR. BILBRAY. Why don't we defer it over to the Ranking Member at this time. Mr. Filner.

MR. FILNER. Thank you.

I just have to say, Mr. Mansfield, I have great respect for you. I know your history. But I am really disappointed in your testimony today.

You could have come here and said we are doing the following at VA to atone for this mistake and change our culture. You could have said we have taken the following personnel actions because we had some violations of what we considered to be good practice and several

employees let us down. You could have said, you know, we have made the following decisions in regard to policies that we did not have before. You could have said that we are offering even more assurance to our veterans. And you just came and said, "well, the laptop has been found, eight bills are irrelevant. I do not have any comment on your bill, the hell with you."

Should I interpret what you did in any other way?

MR. MANSFIELD. I think that you should recognize that I have sat at this table many times in many guises and not one time did I come down here without fully respecting what this Committee is, who it is, and what their job is, and try and fulfill the role that I am supposed to fulfill as a Deputy Secretary.

MR. FILNER. This is a hearing on a draft bill to deal with a major disaster in your department and you have nothing to say? That is my question.

MR. MANSFIELD. Sir, that draft bill was given to us a short while ago. In fact, I think you are still working on parts of it. As you know—

MR. FILNER. You said you have been informed about it.

MR. MANSFIELD. You know I am not here as a free agent. I have to fulfill the role that I am given and that involves executive agency coordination.

MR. FILNER. You could have just said we are not participating because we do not have anything yet.

MR. MANSFIELD. Sir, I would be more than happy to tell you the steps that we have been taking. The Secretary has been down here. His last testimony indicated that.

We are going forward with a reorganization that involves the transfer of 4,610 people to the centralized order of the IT. The Secretary has directed, as the Chairman indicated, a new authority to make sure that the CIO has the ability to enforce that.

We have gone forward with the direction that in addition a CFO should be hired in that office so that the IT can follow the finances of the IT budget that Congress has given us. In addition to that, we have got a training officer in line, and we are going forward with many, many changes.

MR. FILNER. Have you made a decision on the recommendations of the IG report?

MR. MANSFIELD. The IG report has been delivered to the Secretary. He has responded. And the Secretary has indicated in his response that actions are going forward. Some of those involve changes, as I have indicated, in the IT organization. Some of them are personnel actions that I am not at liberty to discuss in public.

MR. FILNER. Your testimony shows how important it is to have the time lines in this legislation and to have you respond to us within X number of days because if it was up to you, you would never respond.

I yield back, Mr. Chairman.

MR. BILBRAY. Mr. Mansfield, look. I will say this as someone who knows the Ranking Member quite personally. If you were not here today, he would be the first one to raise holy cane for you not being present.

So in all fairness, even though he may not like your testimony, I am sure on second thought, he would much prefer to have you here to be able to address personally rather than you not being present at all.

I would ask, Secretary, that over the past several weeks, we have listened to many experts from government, academia, and the industry to learn more about the challenges of effective information management and information security.

From all of this, we have come to a common theme of effectively address the challenges of information security, we have to centralize IT governance. We have to consolidate IT expertise. We have to assess the classified data so that we know what is sensitive and what is not, and who is authorized to access it. We need to develop a well-defined security policy and use technology to ensure compliance of the policy.

Given the data breaches that occurred eight weeks ago, what has VA done on those four issues? This is your chance to be able to answer his questions.

MR. MANSFIELD. Well, sir, as I mentioned, in the area of reorganization, we continue with a planned reorganization that dates back to a year ago, last July. And just last week, we signed a contract with IBM to help us move forward on a plan that actually then Assistant Secretary McFarland put forward to have us reorganize the Department over the period of the next six to eighteen to twenty-four months.

I think there was some question here about whether we should do it immediately or we should do it in a measured way without outside expertise that will be provided by IBM to make sure that we do it right and we do it so it takes hold. So that is one action that has taken place.

The Secretary, as I indicated, has issued a directive that the CIO, the Acting or the Assistant Secretary for IT will have complete authority throughout the Department to enforce the FISMA and other security regulations, and that document has been delivered and is in effect. That is one change.

The other issue is that going back to last April before the event, there was a direction that the IT be given an augmentation that would allow him to have a CFO office so that he could supervise the dollars that are now under his control both for the maintenance and operation domain and for the development domain. And those are some of the issues that we have taken to attempt to move forward.

In addition to that, the Secretary has directed that we look at the elements that caused the breach, that we make sure that we do ev-

erything possible to ensure that we recognize that we have the trust of these veterans in our hands and we need to make sure that we do the job that should be done to make sure that that is protected.

MR. BILBRAY. So your outreach to the private sector would be through IBM?

MR. MANSFIELD. Sir, in a planned reorganization, in a reorganization that was planned starting a year ago, we have moved forward. And the last element in that is that we hired a major contractor to come in and oversee the reorganization, as I said, basically planned by former Assistant Secretary McFarland to move this Department into a situation where you have a centralized operation and maintenance domain. That is the 4,610 individuals plus approximately 560 unfilled slots that will be moved under the direct authorization and control of the Assistant Secretary for IT.

At the same time, we are moving the development program for the Veterans Health Administration into a centralized situation under VHA's direction, and that is about 806 individuals.

And then in the area of Veterans Benefits Administration, we are moving about 253 individuals into a centralized domain for their development program.

And that is the process that we are using to move forward. IBM will come in and under the process of the RFP that we put out help us make sure that we get this total reorganization of the Department started moving forward, in place and working.

And, sir, I would make the point that while Admiral Gauss can talk about collateral damage, when I hear the words collateral damage, I think about our veterans' hospital system and the fact that I cannot afford any collateral damage in developing a program that deals with hospitals and doctors and people going through that situation. That is not a place where you can afford collateral damage. So we have to make sure we recognize that as we move forward.

MR. BILBRAY. Well, Mr. Secretary, I have been involved with government data files since I was 25 years old and supervised the operation of different government agencies with the data files. And one thing I have learned is that all of us in government, I do not care if it is city, county, state, or Feds, are so far behind what the private sector is doing. So I have a major concern.

IBM is your private sector source for cutting-edge approach to this problem?

MR. MANSFIELD. Yes, sir. That is true. They are the ones that were picked in a process again that we have to live under because it is the Federal procurement process and the contracting process. And it has taken the time that it has taken to make sure that we do it right and have them in place.

But I would also make the point that not necessarily as a part of their selection process, but IBM itself went through this process for

their whole total corporate effort not too long ago.

MR. BILBRAY. The question, though, is that IBM is for the reorganization of the structure, not necessarily for the security of the data?

Mr. Mansfield. Sir, we are making sure that in addition to IBM, there are other corporate entities. Some of those have already been involved. I do not have the total picture here with me, but—

MR. BILBRAY. Okay. Let me ask you a question.

MR. MANSFIELD. —we do have people coming in to deal strictly with the security issue or will have.

MR. BILBRAY. One of the things that we looked at when we did the telecommunication bill a few years ago— seems like decades now and, you know, Congressman Stearns was right on top of it—was this issue of biometric confirmation for accessing the data.

You know, with everything that we did last year with Real ID and telling state agencies that they have to start tooling up and using biometric confirmation, are you looking at any system requiring biometric confirmation before access?

MR. MANSFIELD. Sir, I would have to go back and get the experts to come here and talk to you about that.

MR. BILBRAY. Okay. My concern is—

MR. MANSFIELD. I know we are looking across the board, though, but I would make sure that I got the answers. So I will bring the answer back to you. I will talk to the experts.

MR. BILBRAY. Okay. It does not take brain surgery to do fingerprint reading with a computer, you know. I mean, they have been doing that since 1978 out on the west coast.

MR. MANSFIELD. Right. I do know that it has been a subject of discussion with the acting IT and some of his senior staff and other members in the Department. I cannot tell you that we have somebody specifically implementing that in a specific time frame.

MR. BILBRAY. Okay. And it is not just you. I mean, I will tell you I am concerned when I go in the Pentagon. It's still using the same access system that it had on 9/11. I know they are talking about changing it, but it still scares me to death that the access system has not been modified over there either, so it is not just your operation. It is inherent to a government bureaucracy of not wanting to go to cutting-edge.

You know, given the VA's current function functioning with an acting CAO and that the Director of the Office of Cyber Security recently resigned, what executives do you have in charge in the effort right now today?

MR. MANSFIELD. I have to be careful about the terminology. So we have Major General Bob Howard down in IT in an acting capacity.

MR. BILBRAY. Is he operating day to day?

MR. MANSFIELD. Pardon me, sir?

MR. BILBRAY. Is he in charge of the day-to-day operation?

MR. MANSFIELD. Yes, sir. He is supervising the day-to-day operations. And, again, he is going forward on a confirmation on the other side of the Hill, and we have to recognize the protocol that needs to be in place as far as what definitions—

MR. BILBRAY. Now, could I assume that he is looking at the securing of the veterans' data day to day?

MR. MANSFIELD. Yes, he is. And we have individuals in an acting capacity. Mr. Sullivan is in place in OCIS and he has been seconded by a Mr. Gephardt to replace the folks that have just recently left us.

MR. BILBRAY. I think the big question my veterans would ask, Mr. Secretary, is the VA less vulnerable today than they were on May 3rd?

MR. MANSFIELD. Less vulnerable in a sense of it would be harder for this to happen, yes, sir, I believe it is. The Secretary put in place a whole week of cyber-security - awareness activities. We moved up the date for all the personnel to go through the training on cyber security and privacy.

The reports that came in to me showed that 99.2 percent or something of the workforce has done that. Those folks that are called to active duty because they have a National Guard or reserve capacity are exempted from it and people that are home sick or on sick leave are exempted. So I think we have got most people covered with that.

And part of the process that the Secretary has directed and the IT is starting to put in place is an additional officer down there to deal with education and training to make sure that we can carry this effort out not just one week of the year but every day and every week and every month throughout the year to make sure that the people remember each and every day what the importance of this issue is and that they pay attention to the rules and that they follow them.

MR. BILBRAY. What is the status of the directive 6500?

MR. MANSFIELD. It is still in process, sir, and I will have it.

MR. BILBRAY. How long has it been in process?

MR. MANSFIELD. Sir, I am going to have to go back, and I promise you I will report back to your senior staff today.

MR. BILBRAY. Okay. The rumor is three years.

MR. MANSFIELD. Pardon me?

MR. BILBRAY. The rumor is that we have been working on this for three years.

MR. MANSFIELD. Yes, sir.

MR. BILBRAY. Sure would be nice if we had it done before the next Administration—

MR. MANSFIELD. I think the Secretary's directive on authority is a part of that, but I will double check for you.

MR. BILBRAY. Okay. And not to pick on you.

Mr. Williams, have you received any requests from the VA on any breach analysis contracts?

MR. WILLIAMS. Congressman, we are talking to the VA even as late as last night about a potential contract for data breach analysis. We are also working with OMB on that.

MR. BILBRAY. Okay. The Committee wants to be able to better monitor and assist the Department in making progress on the sensitive data files for veterans.

What actions and milestones is the Department able to commit today for securing these veterans' sensitive data?

MR. MANSFIELD. Mr. Chairman, there are two or three actions that are in process based on directions that the Secretary gave and that were given to the administrations and staff offices.

One is to go through a follow-up to a current directive that we have on the books that allows us to take each and every work description, job description and go through that to figure out what the access level for that person should be to sensitive data and then define from that access level what type of clearance we need to have for that person. And that process is under the direction of Human Resources and is moving forward with IT obviously giving some information as to what the access levels should be.

We already have had in place in the Veterans Health Administration an activity that takes all but the last part of this, and the Veterans Benefit Administration was starting it. So we have a process in place that we are using to add on the access for sensitive information and then from there define what the clearance level is.

In addition to that, as we have indicated, we have gone out for a data call to find out exactly how many laptops we have, how many laptops are owned by the VA, and bring those in so that we can, when the lawsuits allow us to and General Counsel may have to talk to that, to be able to clean those down.

And then also the question that came up here earlier about whether VA doctors should have VA owned laptops is one that the Secretary has made a decision that they shall, but we need to figure out what the number is and then the decision is how do we go forward and purchase the equipment that is needed and make sure that the training that is required to use this takes place and we go forward with what is required in our new order and our new ability to protect information.

The problem we have right now and the reason I granted waivers is we have got doctors that may have operated on a patient at ten o'clock in the morning and a nurse or an attending physician may be calling them at home at ten o'clock at night and that doctor wants to be able to access the information that is available throughout the day in that file so he can get a sense of what orders he should be giving to that nurse or attending physician.

And that is one of these issues where again collateral damage is an issue that we need to take into account and recognize that we have a hospital system we are running here and the effort is to make sure that we can get those doctors identified and the appropriate equipment in their hands as soon as possible. And that is underway.

MR. BILBRAY. The current policy basically says the General Counsel's Office is responsible for its own data security. And there has been no standard operating procedure on the policy on the Regional Counsel's Offices.

Why was there no policy on the data security of the Regional Counsel's Offices?

MR. MANSFIELD. Sir, I make the point that under the reorganization, the GC's IT folks are responsible to the Office of Information Technology. There is no doubt that we have some catching up to do as we bring all these people all over the country, approximately, I think, 420 some, into the fold, make sure that they are all following the same directions and orders and make sure that they all understand what they have to do.

This is the first time that we have pulled these folks together as an IT workforce. And we have also direct in October there will be the first national conference, national training conference for all these IT folks so that we can help them understand what the processes are and what the needs are and have them move forward.

Mr. Bilbray. What are the barriers that are preventing the Department from moving forward to implementing the Goldman-Sachs and CitiGroup's recommendations on centralization and consolidation of IT infrastructure?

MR. MANSFIELD. Well, you have heard some of the prior discussion here. It has been about some of the issues that we have to deal with. And I would make the point that, as I said, we are in the middle—

MR. BILBRAY. I just want to make sure that when we come down the pike so that you can identify right now where your problems are that we may be able to help. But where is the barriers of executing those recommendations?

MR. MANSFIELD. Well, as I said, part of it is we are required and we are following the Federal rules for acquisition to make sure that, you know, the correct RFPs are put together and that we go through the process for selecting these folks so that we do not wind up in court over that.

You have heard some discussion here about personnel issues. And I can make the point that a year ago, it took us 145 to 165 days to hire an SES person on board, you know, a regular schedule, not a political.

Today with efforts going forward under Human Resources, we are down to 94 days to hire SES from the time of the announcement to the closure. Part of that time is when the files are in OPM for their

final approval as they have an SES position.

In an effort to help move forward the IT arena, I have directed the Director of Human Resources, the Assistant Secretary to put together a special group that will concentrate on IT and will be devoted to IT in an effort to fill their high-level, mid-level, and low-level positions across the board.

In addition to that, as we look at how we need to reorganize in addition to what we had originally planned, one of the things that we know, for example, to fulfill the FISMA requirements is the ability not only for enforcement by the Information Security Officers but also ability at least on a regional basis to have folks that can go out and do checkups on what is going on in the area. And those people also will have authority to ensure that the facility Director follows the instructions that are given if we come in to do an audit on IT capabilities.

So there are many changes going into place, and we are dealing with the normal issues of fulfilling the general service requirements and the procurement requirements and the contracting requirements, et cetera, et cetera.

MR. BILBRAY. Well, thank you. I want to thank the gentle lady from the great State of South Dakota for her patience. I will recognize her at this time.

MS. HERSETH. Thank you, Mr. Chairman.

Understanding the time it takes to get some of the positions through and the coordination, since we are marking this bill up on Thursday, we will still, you know, await the views on the bill, not the draft bill.

And do you anticipate and can you give us some sort of time table in which we might be able to see the views on the bill after it is marked up on Thursday? Would it maybe be sometime next week before the August recess or do you know if it is going to be August?

MR. MANSFIELD. Madam Congresswoman, part of the process here requires that I have a final product in my hand that I can then have my General Counsel look at. And then the process also requires that there be some intergovernmental, you know, review of this. And that is done by OMB. So that means OMB gets the final product. Until I have a final product, I cannot pass it on to them. I cannot come here and release the information on behalf of the Executive Department until I get that clearance.

MS. HERSETH. Okay. So you will have a final product obviously Thursday when we mark it up. In terms of just getting some views, I am hoping—

MR. MANSFIELD. Let me—

MS. HERSETH. Let me just interrupt. I understand the situation you are in. I do not take necessarily the same perspective on it that Mr. Filner does. I understand that this is going to take some time.

However, in light of the previous testimony, in light of the article today, with all these other agencies having these problems, in light

of the need to move, in light of the fact that you and the Secretary have been responsive to the IG report—your response to the recommendations are in here—I am just hopeful that we will see a desire on your and Secretary's end to expedite the process of making all that coordination happen so that we can get the views of the Executive Branch on the provision of creating the Office of the Under Secretary of Information Security, that we can get the Administration's views on what will be in the bill as it relates to, you know, what we owe to the veterans in the case of a breach.

And perhaps you cannot respond to these questions, but I feel that what the Secretary brought in a couple of weeks ago in giving the authority, including enforcement, that we were seeking, that we thought would have helped, that that is essentially de facto what we are trying to do in creating the Office of the Under Secretary so we do not have this problem with a different political appointee at some time in the future, that serving as Secretary of the VA, that we have to then wait for the same kind of memo and the same kind of sign-off, and that we also have some explanation given the hard work that has already been done in the agency in responding to the IG report and recommendations of how what has already happened, what the planned actions are, how that fits in with what we hope to achieve if we get the full House and the Senate to agree that the bill that we mark up on Thursday is going in the right direction to achieve the kind of expedited manner of going forward that can be of assistance to other Federal agencies.

MR. MANSFIELD. I will get it as soon as I can, and I promise you I will go back and make one more concerted effort to see what we can get. I think we now have a product in hand that will allow us to work on it.

I want to make the point that this is an issue that is of the first priority in this Department and we are doing everything we can to attempt to move forward and solve this and hopefully start the process of getting back in a favorable position with the veterans whom we let down when this happened.

And as an aside, I would make the point that I have dealt with Mr. Filner again on both sides of this table for a long time, and I have no problem with listening to or answering his questions.

MS. HERSETH. I appreciate that. I think it is always helpful when members of the Committee, you know, pose a fair a question as possible for our witnesses to answer. And I am not suggesting that other members of this Committee do not always make a good-faith effort to do that. I just think we all have different approaches. And we have to work together.

I mean, part of the problem here is that there has been this obstruction that people discuss within some departments of the VA. And it is important to me that rather than taking these constantly adversarial

positions of the Committee versus those at the departments that are trying to make this happen, that at this point, we set that aside to the extent that we have had disagreements there, that we recognize we are really in a bind not only at the VA but with other Federal agencies and how far behind we are of getting a grasp of this problem, and that we do everything possible to recognize that I think we are on the same page of wanting to move forward here, but that just as the VA may have its institutional barriers of breaking through and making this happen, this institution and both chambers and how we interact, you know, need to move quickly here as well.

And my hope is that because we are marking up on Thursday that if we can get you all to coordinate in an expedited way with those views that that gives us then a chance to move quickly in September in the full House sending a clear message to the Senate that you have had your opportunity to give your views, that we have made whatever changes we think need to be made on the House floor through amendments, and that Congress can move quickly here, too, in working in coordination with the recommendations of the IG, the actions that you have already taken, and that we keep this one outside of any politics that can be anticipated prior to November so that we do not have to wait until after November to actually make the type of progress and moving with the type of speed that I think you want to move, that I want to move, that the Chairman wants to move, the Committee staff wants to move, that your staff wants to move.

So that is the reason I bring it up, because I am hoping that we have that to guide us then in early September to move quickly the way that—Congress should move as quickly as we want you to be moving within the agency.

Thank you, Mr. Chairman. I yield back.

MR. BILBRAY. Thank you.

Mr. Secretary, I appreciate your time. I just hope you understand that though media may not be talking about this like the issue of armoring the Humvees when our soldiers were being hit by roadside bombs, the veterans out there feel like they are at risk just as much and that the security of data files that can be tapped in for huge financial benefits to anybody who wants to do it or can get into it needs to be given a very high priority, that the veterans not only deserve to have their armor for their sensitive information in place protecting them, but please understand that there are people out there who recognize that data mining information, financial access has huge potential to not only do damage to the individuals who take it but also to financially benefit those who could crack in.

And I think we are all learning that the criminal elements that would love to have access to this are not just people that we would perceive as the traditional mob mentality, but also are organized, not organized crime, but organized terrorists would love to be able to

generate the kind of revenue that information sharing illegally could generate.

So I hope that you recognize that even though the media is not talking about it, the degree of urgency should reflect the same kind of degree of urgency to protect the veterans' files as we were hearing about protecting the active-duty Humvees.

And I just remember the Chairman of Armed Services literally making phone calls flying back from Iraq trying to get that out there. I would sure love to see that kind of urgency when it comes to protection of our veterans' critical information.

MR. MANSFIELD. Sir, the Secretary has stated at this table, and I will repeat it, that this is the highest urgency for us. We understand that we have to do the job of protecting veterans' information, and we are doing everything we can and we are working as cooperatively as we can and as fast as we can with this Committee because we know that in this area that we are in lockstep, we have the same interests at heart here.

MR. BILBRAY. I just want you to remember that the same barriers to getting the job done apply to the armoring project, exactly the same barriers, that there are procedures that they have to go through. Just understand that that kind of urgency needs to be there because we do not want to have another story and have the media on top of you after another breach has happened. We would rather that that pressure be put on now and avoid that problem in the future.

I thank you very much, all of you gentlemen, for being here today and testifying.

MR. MANSFIELD. Thank you, Mr. Chairman.

MR. BILBRAY. Thank you.

MR. WILLIAMS. Thank you.

MR. BILBRAY. We have the next panel.

THE CHAIRMAN. Our final panel is comprised of several veterans service organizations and military service organizations with an interest in this legislation.

First we will hear from Mr. Peter Gaytan, the Director of Veterans Affairs Rehabilitation for the American Legion.

Next we will hear from Colonel Bob Norton, the National Commander for the Military Officers Association of America.

We will then hear from Louis Irvin, the Acting Deputy Executive Director for PVA.

And, finally, Mr. Larry Madison, the Deputy Legislative Director for the Retired Enlisted Association.

Gentlemen, thank you.

And, Mr. Gaytan, you are now recognized.

STATEMENTS OF PETER S. GAYTAN, DIRECTOR, VETERANS AFFAIRS AND REHABILITATION COMMISSION,

AMERICAN LEGION; COL. ROBERT F. NORTON, USA (RET.), DEPUTY DIRECTOR, GOVERNMENT RELATIONS, MILITARY OFFICERS ASSOCIATION OF AMERICA; LOUIS IRVIN, ACTING DEPUTY EXECUTIVE DIRECTOR, PARALYZED VETERANS OF AMERICA; AND MSGT. LARRY MADISON, USAF (RET.), DEPUTY LEGISLATIVE DIRECTOR, THE RETIRED ENLISTED ASSOCIATION

STATEMENT OF PETER GAYTAN

MR. GAYTAN. Thank you, Mr. Chairman.

The American Legion is encouraged that Congress and the Administration are carefully reviewing the lapse in procedure that led to the largest information security breach in the history of VA.

However, VA must now do everything possible to ensure that the personal information of America's veterans, active duty, Guard, and reserve personnel is never stored, packaged, or transferred in a method that will allow such an enormous loss to result from the laps in judgment of a single VA employee.

This loss of more than 26 million veterans' records to include spouses, active duty, Guard, and reserve members is an inexcusable betrayal of trust, and VA must now implement new policies, procedures, and processes needed to ensure proper IT security.

And the American Legion appreciates the opportunity to comment on the proposed legislation being considered here today.

THE CHAIRMAN. Do all of you have written testimony? All of you answer in the affirmative.

Would you like it submitted for the record? All answer in the affirmative.

Hearing no objection, so ordered.

MR. GAYTAN. Thank you, sir.

The American Legion is supportive of this proposed legislation and the attitude of Secretary Nicholson which are in agreement with the VA OIG report recommendations, specifically taking whatever administrative action deemed appropriate concerning the individuals involved, establishing one clear, concise VA policy on safeguarding protected information, modifying mandatory cyber security and privacy awareness training, ensuring that all position descriptions are evaluated and have proper sensitivity level designations, and that required background investigations are completed in a timely manner, also establishing VA-wide policy for contracts that ensures contractors are held to the same standards as VA employees, establishing VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information.

Regarding specific recommendations of this proposed legislation,

the American Legion supports including spouses on the list of individuals protected in this legislation if personal information is compromised.

Also, regarding the provision of credit protection services and fraud resolution services, the American Legion supports language that will ensure monetary reimbursement for any negative financial impact resulting from compromised personal information.

Also, the American Legion supports a protection plan that can be implemented even after the one-year time limit proposed in this legislation.

Finally, the American Legion wants legislative assurances made to veterans that if their information is compromised by VA, unless is it undeniably the result of some other cause, the VA or Federal government will assume the responsibility of any loss incurred by the veteran or relevant family members. We want to avoid the need for veterans to ever have to prove it was the fault of VA that their information was compromised.

The data theft that occurred in May has served as a monumental wake-up call to the nation. VA can no longer ignore the needs to improve its IT security directives.

Mr. Chairman, I think you brought that issue up several years ago and you have been fighting for IT issues within VA to be upgraded at the least, and now we know that there is a need not only for upgrading that IT, but also ensuring that security provisions exist in the VA's directives. And we applaud you for that, sir.

Also, the American Legion wants solid assurance that funding for the IT overhaul within VA will not be paid for with money from other VA programs.

In my remaining time, Mr. Chairman, if you will, I want to mention the importance of the information that was gathered in the OIG report. And I urge you as Chairman of this Committee and any other member on the Committee if you have not reviewed the information in that OIG report, if you have the time, do it yourself. If not, get your staff to do it. If you do not have time, call the American Legion. We will give you a brief synopsis of some of the other issues within the Department of Veterans Affairs that were brought to light as a result of that IG report.

The issues in the agency go a lot deeper than what happened with the theft of one computer. The reasons behind not only the theft of that computer but the lax in control of information, the assumption that taking that information home was permitted and also the huge delay in reporting time from the theft of that information up the chain of command within VA can be attributed to personnel issues that need to be addressed within the Department of Veterans Affairs.

And I urge you and your staff and the members of this Committee

to review that important information in that IG report.

Mr. Chairman, I thank you again for the opportunity for the American Legion to present our opinions on this terrible breach of security within the Department of Veterans Affairs. And I am here to answer any questions if needed.

THE CHAIRMAN. Thank you very much for your testimony.

Colonel Norton, you are recognized.

[The statement of Peter Gaytan appears on p. 106]

STATEMENT OF ROBERT F. NORTON

COLONEL NORTON. Thank you, Mr. Chairman.

On behalf of the 360,000 members of the Military Officers Association of America, I am honored to have this opportunity to present our association's views on the Veterans Identity and Protection Act of 2006.

Mr. Chairman, I would like to offer four points for the Committee's consideration on the legislation at hand and then I would be happy to take your questions.

First, MOAA supports the establishment of the position of Under Secretary for Information Services in the VA. We believe the CIO position offers potential for advancing the goal of seamlessly transferring data and information securely from the Armed Forces to the VA.

MOAA recommends that the Committee consider specifying in the bill language regarding the role of the VA CIO in the context of the joint VA/DoD Executive Council. That body, as the Committee knows, provides oversight on cooperative activities between DoD and VA. Until we get the seamless transition goal right, we believe that the military and veterans' communities will not be well served in terms of their healthcare and benefits.

No doubt DoD has lost confidence in the VA to protect sensitive information. The VA CIO must work to restore a strong partnership with the Defense Department.

Second, if adopted by Congress, the Under Secretary of Information Security should make as a priority action informing and educating veterans about the credit protection and fraud resolution services identified in the bill.

We appreciate the fact that the Committee intends to authorize these services at no cost to veterans and survivors in the event of a data breach of personal information.

Third, we believe all government agencies that use the Social Security account number as a record identifier should begin now to develop alternative identifiers that pose less risk of security theft.

We understand, Mr. Chairman, of course, that such an effort as discussed earlier today poses enormous challenges. But if other large

bureaucracies such as the State of Virginia can develop alternative ID numbers for State residents to place on their driver's licenses, Federal agencies should strive to offer at least the same level of protection.

Finally, in our view, a key measure of effectiveness for the CIO position will be its integration into the complex VA bureaucracy. As you know, this will be—and this was discussed at length in earlier panels—this will be no easy task. Veterans know that navigating the three line operations of the VA, health, benefits, and memorial affairs, is difficult at best. Adding another bureaucratic layer into this system is fraught with many challenges and even risk. But we believe that a single manager is needed to ensure the security of veterans' personal information and to advance the effective business integration of the VA.

This concludes my testimony, Mr. Chairman, and I appreciate the opportunity to appear before you today. I look forward to your questions.

THE CHAIRMAN. Mr. Irvin, you are recognized.

[The statement of Robert F. Norton appears on p. 110]

STATEMENT OF LOUIS IRVIN

MR. IRVIN. Thank you, Mr. Chairman and members of the Committee.

I would like to take the opportunity to thank you for the availability to speak here today. We appreciate the extensive amount of work that has gone into review of VA's IT process along with the recent data theft and occurrence.

It is incumbent upon the VA and Congress to ensure that this does not happen again and to ensure that the interests of the veterans are protected. PVA recognizes that the need to reform the VA information management services is paramount.

We do support the idea of strengthening the authority of the Chief Information Officer. However, we do not believe the importance of this individual should rise to the level equivalent of the Under Secretaries for Health, Benefits, and the National Cemetery Administration.

Information services functions as a support service to these entities. Information technology is not a mission- level program within the Department.

The responsibility of the CIO are much like those of an Assistant Secretary for Operations, Security, and Preparedness. The Assistant Secretary ensures that the life and property of both veterans and VA employees is protected. Personal information is clearly as important.

We do believe all the functions and responsibilities of the CIO

should be consolidated as outlined in the legislation. We support centralizing the creation and implementation of policies and procedures including information security within the CIO's program.

We think it is important that control of activities and systems that support information services should be retained within VHA, VBA, and NCA. Furthermore, the management of all mission applications, information resources, personnel, and infrastructure should be retained at that level as well.

Although the CIO would manage the information systems policy of the entire VA, he would not necessarily know what systems and applications work best to actually provide healthcare or benefits information. Information technology is not the mission of the VA. It is the tool that individuals responsible for the mission should have the authority to manage their tools the best way they see fit.

PVA fully supports the data breach reporting requirements established by this legislation. We also recognize the need to put in place credit protection services as outlined in the legislation. It is important that if veterans' personal data is stolen in the future that their credit be protected from criminal behavior.

However, it is important to emphasize that the VA must notify veterans immediately if a data breach occurs. It should be done within days, not weeks. The three weeks it took to notify the public with the most recent data theft is wholly unacceptable.

PVA does not believe it is necessary to move forward with credit monitoring and other protections if it is clearly determined that none of their personal information has been compromised.

The VA has been fortunate to recover the stolen hardware on which the data was stored. We do strongly caution, however, that any data breach in the future be immediately viewed as if it has been compromised. At such time, veterans are given the opportunity to access a credit monitoring process supplied by the VA. This is imperative in reestablishing the trust that has been lost through this ordeal.

We must also emphasize that if VA is to provide these services due to a data breach in the future that separate funding must be appropriated to provide these services.

Finally, we believe that as this legislation moves forward, the Committee should ensure that this legislation offers the same types of protections to those men and women who are currently serving.

PVA would like to thank you for the opportunity to testify today. We would be happy to answer any questions that you may have.

THE CHAIRMAN. At the end of a long hearing, it is only proper that the Master Sergeant fill in all the details. You are recognized, Larry.

[The statement of Louis Irvin appears on p. 114]

STATEMENT OF LARRY MADISON

MR. MADISON. Thank you, Mr. Chairman, members of the Committee, for this opportunity to provide testimony for the record to the House Committee on Veterans' Affairs.

All of us were shocked and alarmed in early May when it was announced that a laptop computer containing the personal data of nearly 29 million veterans, active-duty, Guard, and reserve personnel was stolen. And although we are pleased that the laptop has been recovered and it appears that the data was not accessed, the problems regarding data security at the Department of Veterans Affairs still need to be corrected. That is why we are pleased with the draft legislation that is the focus of this hearing today.

We want to thank you, Mr. Chairman, and all of the members of the Committee for the collective nonpartisan way in which you have sought to handle this crisis. It was sincerely gratifying to watch the Committee work together in seeking to learn the details of the situation and then coming up with the proposed legislation.

Like many others, we were amazed to learn during the hearings held by this Committee about the warnings from the GAO and the VA's own Inspector General and Assistant Inspector General going back as far as 1997 concerning the weaknesses in the VA's information security systems.

That is why we have no doubt that the legislation under discussion today is necessary to ensure the corrections needed at the VA are accomplished and to help restore the faith of America's veterans in the security of their personal information that is kept by the Department.

In particular, we believe the creation of the position of Under Secretary for Information Services is vital if the task of increasing personal data security in the Department is to succeed.

During the testimony given by officials from the Department of Veterans Affairs before this Committee, it was painfully apparent that there was not a single individual who was in charge and responsible for data security. The change envisioned in this legislation is a positive one that we believe is urgently needed.

In addition, we applaud and strongly support the reporting requirements outlined in the legislation. We believe the annual compliance report to Congress and the monthly reports to the Secretary are urgently needed, and they send a signal to the Department about the seriousness with which this Committee and the Congress take this issue.

We note that the legislation provides for credit protection services for any individual whose personal data held by the VA was breached at no expense to the individual if the individual requests one of the

credit protection services contained in the bill. We believe this is a reasonable way to handle this issue and we support the provision.

We are pleased that the legislation directs the Secretary to enter into an agreement with one or more credit reporting agencies and this agreement will be in place so that any breaches in the future that place the personal data of veterans in jeopardy can be quickly and efficiently monitored by that agency if individual veterans request such service.

The last item we want to mention is the use of Social Security numbers for identification. As you know, the draft legislation prohibits the use of the Social Security number of any individual to identify that individual unless the use thereof is required by law or the Secretary determines that such use is necessary for the identification of an individual.

It is our hope that this is the beginning of a process within the Federal government of getting away from using an individual's Social Security number as a person's one and only ID. Although we recognize the efficiency of using one number as the all-purpose identifier, it is obvious that doing so also increases the efficiency with which a stolen Social Security number can be used to commit identity fraud or other criminal behavior.

We hope this section of the draft legislation will be as carefully monitored as the other aspects of the bill because we can foresee a less than enthusiastic response for this provision from the IT persons within the Department.

Once again, TREA wants to thank the members of the Committee for your commitment to serving our veterans. Based on what we have learned, we believe this draft legislation will result in the personal data security that is needed for our veterans and is something which every member of this Committee can proudly point to when questioned about this issue by veterans in your districts.

This concludes my statement, and I will be happy to answer any questions you may have.

[The statement of Larry Madison appears on p. 119]

THE CHAIRMAN. Gentlemen, thank you very much for your testimony. And I did not get your testimony last night. To let you know, in the future, the reason we ask for testimony, not only the staff want to see it, but they put together a briefing book for me and they give it to me the night before and I am able to read all of the testimony. And we can get it out to members. And when we do not get it in time, it makes it challenging.

So we are just hearing it for the first time. And what I am going to have to do is—I have made notes here—because we have a product and we have asked for your view on it. You have given some detailed recommendations, we will have to swing back through another wick-

et. Okay?

So after this afternoon and then tomorrow, prior to this being introduced, we will examine your recommendations. Whether or not we incorporate them or not, it is worth another wicket. And that is what we are going to do.

Gentlemen, you were here when Admiral Gauss and Mr. McFarland testified with regard to a recommendation about an implementation requirement and time line.

Would all of you concur with that testimony? You can do it in the affirmative or the negative. All right. All agree.

With regard to Secretary Mansfield's testimony that an additional six-month review from the IG would be unnecessary because the IG, quote, regularly issues reports about data security practices within the VA and FISMA audits and consolidated financial statement audits performed annually, I ask for your thoughts.

Given the Department's track record in implementing recommendations from the Inspector General and GAO, would this be a prudent requirement?

Mr. Gaytan. If I can, sir, for the American Legion, I mentioned a little bit about the information that is in the IG report, and the information that is in that report definitely requires another IG report in six months.

And they need to look further and they need to ask some new questions and ask the individual who did take the information home why they thought that they could take it home. And the admission of the individual that took it home to the IG was that they had been taking the information home since 2003.

THE CHAIRMAN. So what I take from this then, from the question and your input, and I know I am preempting—I apologize—but that an implementation audit would be a prudent performance measure given the VA's track record?

MR. GAYTAN. Yes, sir.

THE CHAIRMAN. All of you would agree with that?

Now, I believe we had some differences on the testimony with regard to the promotion to an Under Secretary. So I want to make sure I get this. The opinions on elevating the Assistant Secretary for Information Technology to the Chief Information Officer to an Under Secretary level, agree or disagree?

Mr. Gaytan?

MR. GAYTAN. We agree.

THE CHAIRMAN. Mr. Norton?

COLONEL NORTON. We agree.

THE CHAIRMAN. Mr. Irvin?

MR. IRVIN. We disagree.

MR. MADISON. We agree.

THE CHAIRMAN. Okay. All right. Ms. Herseth, you are recognized.

MS. HERSETH. Thank you, Mr. Chairman. I was going to probe a little bit more on that whole issue of elevating the CIO to an Under Secretary position.

Thank you, Mr. Gaytan. I missed that part of your testimony since you were the first there. So I was jotting down everyone's position.

Now, just to probe a little bit further, Mr. Madison, you think that it is essential, I mean, it is vital according to you and the Association to elevate the CIO to an Under Secretary position, correct?

MR. MADISON. Yes, ma'am. And I think the testimony from the two gentlemen in the second panel, I believe, underscored that.

MS. HERSETH. And, Mr. Norton, I think you stated that you support elevating the CIO to an Under Secretary position, but you did express some concern about yet another bureaucratic layer in light of some of the other issues you have dealt with in some of the other departments, correct? But at the end of the day, you still support the elevation of the position?

COLONEL NORTON. Yes. We definitely support the elevation of the position.

MS. HERSETH. And, Mr. Gaytan, could you elaborate just a little bit on why American Legion believes it is important to elevate the CIO to an Under Secretary?

MR. GAYTAN. Yes, ma'am. The American Legion feels that the current VA IT security directives, there are dozens of them that exist within the Department of Veterans Affairs. And the personnel in the Department of Veterans Affairs are not sure which directives to follow, which ones that they should apply to their own information that they use in their jobs.

And the existing position of the IT Chief right now within the Department of Veterans Affairs has been unable to put their arms around that information and provide a clear and direct guidance to VA personnel on how they can handle personal information of those veterans that they have when doing their job.

So increasing the position that would have oversight over IT within the Department of Veterans Affairs cannot be detrimental. We cannot be any worse than what we are currently working with right now.

I will refer back to the IG report and the information in there. The individual who took the information home said that they were never told that they could not take it home. So that response alone is a direct need for VA to provide a clear description of their IT security issues regarding their personnel and what their personnel can and cannot do.

So increasing this position cannot be any worse than what we are dealing with right now. So we do not see it as detrimental to what our objective here is and that is securing the information that VA personnel utilize in relationship to veterans' personal information.

MS. HERSETH. Okay. Thank you for that, the elaboration on the position.

So let me come back to you, Mr. Irvin. And just to better understand PVA's position, because I think you support the enhanced authority.

MR. IRVIN. Absolutely.

MS. HERSETH. But do you have a concern, and this is what I was trying to get at a little bit earlier with Mr. Mansfield. I feel that the Secretary's memo sets out to achieve de facto what we are trying to secure in the future by elevating that position. So do you have any concern that we will run up against the same maybe bureaucratic obstacles with each new appointment of a new Secretary if there is a delay in reissuing that memo and having those enhanced authorities available to the CIO?

MR. IRVIN. Well, yes, I do. I think, you know, as you look at the structure within the Department, the Under Secretary positions are held at mission-level structure. Information technologies is a support of those business lines. And I think if you create a structure where the support is at the same level as the mission, then the mission can sometimes evolve around the support.

And so I would think that, you know, the amount of emphasis placed on information technologies and security is due to the amount of attention that the Secretary, the Deputy Secretary, and the Under Secretaries will place on that. That is why I think positioning at an Assistant Secretary level is the key.

I think the Deputy Secretary already indicated a lot of changes going on with VA. I do not think that those changes would be enhanced by creating an Under Secretary position. So the authority can be put in place for the CIO without elevating to a mission-level program.

MS. HERSETH. I respect your concerns there. I maybe would harken back to the previous testimony from the second panel, though, as well. And, again respecting your concerns in terms of the distinction between mission versus support.

But at the same time, I feel almost like this support function, if it is within that category, is so core not only to advancing the mission but also to addressing these problems that really are putting veterans at risk in different ways in light of advances in technology, that by at least having your CIO at the table, on the board that can work with the other Under Secretaries as they make the best case for any recommendations coming from the CIO that would seem to trump support over mission, I just feel it is important to have that person at the table, on the board. But if we do not have them on the board—

MR. IRVIN. I think that could happen. I think the Secretary could have that ability to do that with a person at the table.

MS. HERSETH. But we would have to ensure that each Secretary—

MR. IRVIN. But I do not think creating an Under Secretary—I mean,

there are people that sit at that table that are not Under Secretaries. Am I incorrect in that? Maybe I am missing the structure. But I think there are people that sit at that table that are not necessarily Under Secretaries.

MS. HERSETH. Well, that may be the case. Maybe that is something that we can pursue with staff. But I do think that we still run into the problem that I expressed at the outset which is even if that is the case, that it is at the discretion of each Secretary, and we are just looking for some guarantee in the organizational structure that the Committee does not have to with each new appointment, whether that is two years, four years, six years, however long it is, with the particular testimony of the past number of weeks of the culture and obstacles and more—well, that they are just great obstacles it seems within this particular agency than perhaps some other Federal agencies, that even CIOs that have worked in different agencies have testified about that it may be important to make this organizational change.

But I recognize and respect the fact that you have offered the Committee your thoughts, the PVA's thoughts on how we could approach this a little bit differently, although it has been met with skepticism at least from me and perhaps some of your colleagues within the veterans service organization community.

But thank you for your testimony, and if there is any final point you would like to make.

MR. IRVIN. I would just like to say something. I think as the information technologies does evolve and you take a look at, for example, in the last 24 months with VHA's implementation of the electronic health record, which has really moved VA forward in a lot of ways in providing better healthcare, this is going to continue. I mean, the information technology structure, I should say support will not be stagnant by any means in the future.

So as this continues to evolve, I think it is important that as the Committee looks at this in addressing this issue that it is clearly identified that this is a support for the mission of the Department. That is where we come from. That is what we would like to stress here today.

Thank you.

MS. HERSETH. Thank you, Mr. Chairman. I yield back.

THE CHAIRMAN. Therein lies our challenge. Therein lies my challenge. And Lord knows patience is a virtue, and I have just run out at the end of seven years. I have. Too many hearings, too much testimony, too many, you know, IG reports, too many GAO reports.

Sometimes it takes an external factor in life to require change even in our personal lives. And we have an incident that finally gets some attention to something and we can perfect some change from it.

I will be a good listener and I do not lock into status quos. There

are other departments and agencies that even will take support services and elevate them depending upon the size. I mean, the only thing I will just ask is not to get locked in to, well, this is a substantive lane, that is a substantive lane, therefore, support functions have to be under them. You know, sometimes we get our military thoughts and go in chain of commands.

The whole idea of empowerment of someone that can be the enabler and be the partner of enabling those three Under Secretaries to get their jobs done, if they subordinate instead of embrace, I do not know how I can achieve the results for which we all seek.

I am just being very candid with you and very honest on where I am. And it is easy to come in and say, well, I think it should be this and here is why too. I am just letting you know personally where I am coming from. And I respect your opinion on it. I just wanted you to know that from me.

Mr. Mansfield, thank you for sticking around and listening to the testimony of the VSOs. And I apologize. I was not in the room during your testimony. I want to ask this panel and then I am going to ask you, Mr. Secretary, what your thoughts are.

We are going to also work on this idea of creating a scholarship for cyber security Ph.D. You know, here we have a country not just the VA in the challenge. You know, Gordon, congratulations. You are the one that just got the attention of everybody. It could have been the Department of Ag. It could have been somebody else. But it was you. But CitiGroup, name the company, others have had these challenges. And as a country, if we are producing such low number of cyber security experts for our country, we are not meeting a need.

I cannot change a country in this legislation, but we can take a step to get our own house in order and then I can introduce legislation and go to the Ed and Labor Committee and see what I can do to open this up to help a country. But with regard to our own house, I will ask for your input on an idea to create a scholarship program for cyber security for the VA.

Mr. Gaytan. I think there is a definite need for it and I think it is a great idea to offer anybody the opportunity to improve their education in this country. But I like what you also prefaced your statement with by putting our own house in order first.

I would hate to see the desire to provide an educational opportunity in cyber security override our focus on the problems that exist in securing the IT and personal information of America's veterans that are handled by VA.

Colonel Norton. I like the idea, Mr. Chairman. I draw the analogy with the tremendous advances in VA healthcare delivery winning all kinds of quality and safety awards in recent years. I think the VA could be an engine of change for the Federal government and, to some extent, even for the private sector if there were an investment

in these kinds of people who have the extraordinary capability to help improve the security of sensitive information. The VA could lead in this way and then be sort of a seed bed for the rest of the Federal government.

THE CHAIRMAN. Mr. Irvin.

MR. IRVIN. Thank you, Mr. Chairman.

I, too, support the idea. I think as information technologies evolve, having the top people available to support that is a good thing. I think it offers a lot of opportunities within the Department to provide better services and efficiencies, and having better qualified staff and educative staff is definitely key to that mission.

Thank you.

THE CHAIRMAN. Mr. Madison.

MR. MADISON. I support the idea, Mr. Chairman. I think it makes a lot of sense. The implementation of it would be interesting to see and see if there is anything comparable to it that exists right now, I am not sure, but I like the idea.

THE CHAIRMAN. You are right. Minority council and I have just spoken—and we will look at the scholarship programs that we do within VHA with regard to medical specialties. We can look at that.

But in order to bring them on line so that they can assist the Department, I think in the first five years perhaps doing a loan forgiveness so we can try to immediately tap an expertise now and bring them in as we get the program on line. So you are right about the implementation. We will put our thinking caps on here and try to get to there.

Mr. Secretary, what are your thoughts?

MR. MANSFIELD. I wholeheartedly agree with the idea. I think it is a follow-up to what we are doing with VHA programs.

I am also sitting here thinking about some of the soldiers at Walter Reed, Bethesda that could be brought into our IT program as interns. I met one of them yesterday. He is visiting. He is going to summer school. He is going back to college. That is the kind of individual that hopefully we could also bring into this program through not just the VA program but also through VBA.

THE CHAIRMAN. We will put a veterans' preference in this. I think that would be very good.

What?

MS. HERSETH. Well, if I might take a point of personal privilege—

THE CHAIRMAN. Sure.

MS. HERSETH. —in light of your question and the responses. I would wholeheartedly endorse not just the scholarship but the idea of loan forgiveness. We have a number of undergraduate and an increasing number of graduate programs at Dakota State University involving cyber security.

I received a demonstration there recently where you cannot even—

if you have a laptop and you type in your user name and password, the computer can recognize the manner in which you type it in. You cannot even log onto the computer because it is keyboard recognition that they have integrated.

So I do think that in terms of that generation of students being very far advanced in what we can do as it relates to some of the testimony we got here earlier about laptops and how we make sure they have either got the encryption software and all of these other things that are available to us that we bring in these young people and give them these opportunities to address these problems quickly with a loan forgiveness type of program.

If I could pursue one other quick line of questioning before we go to vote.

THE CHAIRMAN. Hold your thought. Is it on a different issue?

MS. HERSETH. Yes.

THE CHAIRMAN. Mr. Secretary, if you could, over the next 24 hours give an assignment to someone to think about that and be in touch with the Committee.

MR. MANSFIELD. And report back?

THE CHAIRMAN. Yes. Be in touch. Sure. Report back. I mean, we just want to work with you rather than just say here is what you are going to do. Give us your idea and we will come up with something. All right.

Please.

MS. HERSETH. Thank you, Mr. Chairman.

Just in the essence of time here, I just wanted to quickly pursue an area where there was also another difference in the testimony from the Under Secretary position, but also something you referenced earlier which was my last line of questioning in an earlier hearing about going forward with offering certain services even though it did not look like the information had been compromised in this letter to the speaker from Mr. Portman at OMB withdrawing the request for the resources necessary to offer those services to the 26 and half a million veterans.

Mr. Irvin, I believe you had mentioned in your written testimony that you said you did not think it was necessary to move forward with the credit monitoring and other protections for veterans if it is clearly determined that none of their personal information was compromised by this latest incident.

But, Mr. Gaytan, I think in your written testimony you said that the VA must follow through with its promise to provide one year of free credit monitoring to veterans.

Mr. Norton, Mr. Madison, do you have positions on that issue, and, Mr. Irvin, perhaps you could explain why PVA is not pushing for the free credit monitoring like the American Legion is or perhaps there is a difference of opinion you would like to explain for me?

MR. IRVIN. I guess being the disagreer here, I will step forward first. I think what I would like to make very clear is that what we have been provided, this data was not compromised. As I further stated, though, I do have a concern in future data breach issues. But, you know, I do not know the scientific clarity of that. I am not a data analyst, so I cannot do that.

But if it is clear that this data has not been compromised and all the data and all the hardware has been recovered, then I think that I do not see how it can be necessary to go forward with credit monitoring for that specific instance.

But I do caution that in the future that the Department is not given 90 days to look to see if the data has been compromised. I think that if there is a breach in the future that it is important to automatically assume that the data has been compromised and, therefore, things should go forward to provide credit monitoring for veterans.

MS. HERSETH. Which is what I think the draft bill seeks to do.

So, Mr. Gaytan.

MR. GAYTAN. Yes. If I can explain the American Legion's support for credit checks for those individuals who were reported on this list of stolen data, it was also reported, we had initially heard, too, that the data was not accessed. But then if you read the IG report, you also see that after the laptop was recovered, access to that information did not require a password. They easily pulled up all the information on the veterans.

So we are erring on the side of the veterans in protecting them and ensuring that if any veteran feels they have been compromised as a result of this stolen information that they have the opportunity to seek, to choose assistance.

The Chairman. Mr. Gaytan, as I understand, further forensics has been done.

MR. GAYTAN. After that?

THE CHAIRMAN. Yes. So I want you to know that you are commenting right now on something that is stale and much has been done since then. So you are formulating an opinion based on something that was already here. And what is unfortunate is that this mile marker is not open to public disclosure right now.

MR. GAYTAN. Yes, sir.

THE CHAIRMAN. I just want you to know that. So there is a reason and a rationale as to why the Director of OMB came back to us and then said it is unnecessary for the $160 million.

MR. GAYTAN. Okay.

THE CHAIRMAN. I just wanted you to know that only because I want to protect the integrity of the Legion. I want you to be able to give an opinion based on present information.

MR. GAYTAN. Yes, sir.

THE CHAIRMAN. And it is not there at the moment.

MR. GAYTAN. That information did not reach the American Legion. Well, I appreciate that. But also the American Legion supports the offering of credit checks and credit protection for any veteran who may have been compromised.

And, again, we agree with PVA in any future instances where a veteran needs to do that, we support the legislative language in this piece of legislation that would protect veterans and allow them that security.

MS. HERSETH. Well, I appreciate your response. And my final comment is that I think that your testimony, appreciating what the Chairman just explained in terms of what is for public consumption, what is not, and the additional forensics, is that because of what we know of other incidents, which is sort of what I was getting at the other day, and knowing from the second panel that we are going in the right direction based on your commitment to look at the ID IQ contracting process, that because of these other incidents that may be out there that we are still gathering information on, that we do have a system in place that for any veterans in that subset, that if they request a credit check, that that is there.

So we appreciate your patience with how I have probed on that particular issue too.

Thank you, Mr. Chairman.

THE CHAIRMAN. Very good. Thank you very much for your testimony. The hearing is now concluded.

[Whereupon, at 1:43 p.m., the Committee was adjourned.]

APPENDIX

Committee on Veterans' Affairs
Congressman Steve Buyer
Veterans Identity and Credit Protection Legislation
July 18, 2006
10:30 a.m.

Good morning ladies and gentlemen.

Before we begin, I would like to welcome our newest committee member, Mr. Brian Bilbray. Mr. Bilbray returned to Congress following a June 6 special election in the 50th district in California.

A native San Diegan, he brings to his constituency a unique level of experience, having served the people of San Diego County as a mayor, county supervisor and congressman.

His two decades of business and local government service were instrumental in developing San Diego County's progressive initiatives regarding environmental protection, pollution control and economic development.

Mr. Bilbray has been at the forefront of the battle to protect the Mt. Soledad Veterans War Memorial and has cosponsored legislation with Congressman Duncan Hunter to make Mt. Soledad a National War Memorial, allowing it to remain for San Diegans to enjoy for generations to come. I believe it is on the floor tomorrow. Welcome, sir.

This morning we will review draft legislation prepared in response to the theft in May of personal data belonging to as many as 26.5 million veterans, 2.2 million servicemembers as well as family members. The stolen computer's recovery and the FBI's determination that the files were not accessed, does not reduce the importance of improving information security and management at VA. We have been warned.

We also have the Minneapolis and Indianapolis breaches and others. We have challenges requiring ongoing stewardship as we work with VA on securing its information management systems.

I want to commend the members of this committee and our staff. To get here, we conducted within three weeks a series of five committee and two subcommittee hearings that, layer by layer, these last five weeks have allowed us to build our knowledge and equipped us to examine this issue in its totality, so we may have a greater understanding of the problems.

We brought 18 witnesses and senior VA officials – including former VA chiefs of information – who answered questions on the data loss itself, the current and potential structure of VA's IT system or lack thereof. We have learned from experts how the best firms in industry manage their information and data security, and we have heard from academia as well. This work is under-girded by six years of hearings conducted by this committee since 2006. I expect that when we introduce legislation, its quality will reflect this approach.

Eight legislative proposals have been introduced and referred to this committee since the May 3rd data theft. Proposals have included requirements that VA notify veterans of data loss and provide free credit monitoring. Additionally, at first I envisioned a claims process, but the Secretary talked to me about insurance. Mr. Bilbray has legislation to address this issue, which calls for credit insurance as well as monitoring.

At least one bill requires VA to implement Government Accountability Office data security recommendations (one wishes it needn't take a law to prompt such sensible behavior). We have reviewed proposed legislation to limit the use of social security numbers and to create personal identification numbers for veterans, and we have received a proposal to create a new office of identity protection within VA.

There is much here worthy of our consideration.

Today we will review draft legislation that draws on many of these ideas. The draft bill and a summary are before the Members.

First, the bill adds government wide requirements to FISMA for agency procedures in the event of data breaches, and for notice to individuals whose personal information has been compromised. Further, the bill would also make it clear that under FISMA, agency CIO's have enforcement authority for information security policy. For the FISMA provisions of the bill, I want to thank Chairman Davis and Ranking Member Waxman of the Government Reform Committee, as well as their staffs. They attended our hearings; were good listeners, recognized the challenge in all departments and agencies, and have worked with us in a cooperative spirit to move FISMA improvements to the floor without delay.

Our goal must be to determine how best we can make whole any person harmed by data compromise at VA. As important, we must address and ensure that the department's polices and organizational structure work to efficiently manage and safeguard information.

For without a good organization guided by sound policy, we will be revisiting the tragedy of compromised personal data all too often.

I look forward to our discussion today. I wish to commend Mr. Filner and members of the Committee for your perseverance and hard work on a difficult issue. I now recognize Mr. Filner for an opening statement.

Our first panel is comprised of Members who have introduced various legislation following the announcement of the May 3rd data loss. Two of these members come from our own committee.

Our first witness is Ms. Darlene Hooley from the 5th District of Oregon. Ms. Hooley is also a member of this Committee, with two VA facilities in her district.

Next we will hear from Ms. Marsha Blackburn, who represents the 7th District of Tennessee. The bill introduced by Ms. Blackburn, H.R. 5464, shows her experience from serving on the Energy and Commerce Committee has provided some guidance in the draft bill before us.

The next witness is Mr. John Salazar, who represents the 3rd District of Colorado. The only veteran in the Colorado delegation, Mr. Salazar has been a member of this committee since February of this year.

Our final witness on the first panel is Mrs. Shelley Moore Capito representing the 2nd District of West Virginia. Mrs. Capito has traveled twice to Afghanistan and once to Iraq where she was able to meet with U.S. troops fighting the War on Terror and review rebuilding efforts in both countries.

Our second panel had also appeared at our June 28 hearing with the Chief Information Officers. We have brought them back to receive their input on the draft legislation the Committee is reviewing.

An Army veteran, Robert McFarland was nominated by President George W. Bush to serve as Assistant Secretary for Information and Technology in the Department of Veterans Affairs (VA) on October 15, 2003, and was confirmed by the Senate on January 22, 2004. Prior to his appointment, he served as vice president of government relations for Dell Computer Corporation. Mr. McFarland left the Department of Veterans Affairs on May 18, 2006.

Dr. John Gauss was nominated by the President, confirmed by the Senate, and served as the Assistant Secretary for Information and Technology, and Chief Information Officer, for the Department of Veterans Affairs from August 2001 through June 2003. In January 2005, RADM (Ret) Gauss founded Gauss Consulting Services, Inc. and in February 2006, he joined FGM, Inc. as the company's President.

Our third panel represents the views of the Administration. We have before us the Deputy Secretary for the Department of Veterans Affairs, Mr. Gordon Mansfield. From the General Services Administration, we have Mr. James A. Williams, the Associate Administrator for the Federal Acquisition Service who will discuss what offerings they are providing under their contract.

Our final panel is comprised of several veterans service organizations and military service organizations with an interest in this legislation. First we will hear from Mr. Peter Gaytan, the Director for Veterans Affairs and Rehabilitation from the American Legion. Next will be Col. Bob Norton, the National Commander for the Military Officers Association of America. We will then hear from Mr. Louis Irvin, the Acting Deputy Executive Director for the Paralyzed Veterans of America. Finally, Mr. Larry Madison, the Deputy Legislative Director of The Retired Enlisted Association will testify. Gentlemen, welcome.

Thank you all for being here today. This hearing has proved to be very informative. I believe we are in a position to introduce a bi-partisan bill tomorrow. I am going to ask staff to finalize a bill for introduction and send it out with a summary to all committee members later today.

Members will have an opportunity to review it, and become original cosponsors before it is introduced midday tomorrow. Any Member interested in cosponsoring the legislation, should contact Deb Collier at the Full Committee.

Without objection, all members will have 5 legislative days in which to submit opening statements or statements for the record. So ordered.

With no further business, this hearing is now adjourned.

Rep. Corrine Brown
HOUSE COMMITTEE ON VETERANS' AFFAIRS
Legislative Hearing on Veterans Identity and Credit Protection Legislation
Tuesday, July 18, 2006, 10:30 a.m.
334 Cannon House Office Building

Thank you, Chairman Buyer, Ranking Member Evans and Acting Ranking Member Filner for holding this hearing on Veterans Identity and Credit Protection Legislation.

I appreciate the hard work you have put into developing this legislation since we first received word of the data theft at the end of May.

Through the many hearings, the bipartisan nature of this Committee really came through.

I know this legislation is still a work in progress. It is important that what happened, or should I say did not happen, to the 26.5 million veterans and dependents and 2.2 million active duty servicemembers should never happen again.

It was indefensible what happened. Only by the grace of God was none of the data compromised.

The VA got a "Get Out of Jail Free" card.

Now is the time to work to make sure it does not happen again.

I look forward to hearing the testimony of today's experts on the proposed legislation.

Opening Statement of the Honorable Cliff Stearns

Full Committee on Veterans Affairs

July 18, 2006 – 463 Words

Mr. Chairman, thank you for holding this Full Committee hearing to examine legislative responses to potential privacy breach of personal data within the Department of Veterans' Affairs. 26.5 million veterans, and 2.2 million Guards, Reservists, and active duty servicemembers, were at risk. Fortunately, we have since recovered the stolen laptop and forensic analysis revealed the data was uncompromised. But we must learn from this incident what steps we must take to A) change the organizational structure and requirements at the VA, and B) design a meaningful package of action items we will deliver for veterans should a breach ever occur again.

Over the past nearly two months we have heard from everyone from the Secretary, each Under Secretary, General Counsel, and the IG and GAO; from industry and academic data security experts; and from veterans themselves. Today, I look forward to hearing testimony on

some specific proposals by my colleagues, as well as the Chairman's draft. I have worked with some of the Members testifying on no less than data privacy itself: Representative Blackburn on my Subcommittee of Commerce, Trade, & Consumer Protection of the Energy & Commerce Committee. And Representative Hooley and I a couple of years ago created kind of an informal RFID (radio frequency ID) working group.

As the Chairman of the CTCP, for years I have led in the issue of consumer data protection and privacy. Unfortunately, data breaches like this highlight the need for legislation that I have authored: H.R. 4127, the Data Accountability and Trust Act (DATA). This bill, which the Energy & Commerce Committee approved March 29, and reaffirmed in a markup May 24, goes to the heart of this problem of the critical need to protect consumers' personal information.

Mr. Chairman, because of my experience with this issue, and my bill, I have a special interest in the area of notification. Because of the very threat that a breach of personally identifiable information poses to one's financial security, not to mention peace of mind, time is of the

essence in alerting an affected consumer or veteran. Therefore, I think that while we are instructing the VA when they must notify veterans, let's not limit ourselves to notification by "snail mail". The standard of business practice is – if a consumer or veteran in this case prefers – to communicate in writing by e-mail, because it is immediate and portable. What if a veteran My DATA Act makes explicit that this is an acceptable alternative means of notification if the consumer opts for it, and I hope that we will consider this in this Committee's bill, too. Secondary to providing better service to the veteran, this would save tremendous money to the VA: didn't the May notification mailing cost $7 million?

Through both of my Committee seats, I will continue to take an active role in ensuring that veterans, and all consumers, feel confident and secure about their financial and personal information.

Statement of Congresswoman Stephanie Herseth
Full Veterans' Affairs Committee Oversight Hearing
Veterans Identity and Credit Protection Act

July 17, 2006

Thank you Mr. Chairman for holding today's hearing on the Veterans Identity and Credit Protection Act. I appreciate your leadership on this issue and efforts to work swiftly to draft legislation that will improve information management within the Department of Veterans Affairs.

While many unanswered questions remain regarding the VA employee who took personal veterans information home and whether or not he had permission to do so, it is obvious that blatant problems exist within the VA's information management infrastructure that must be promptly addressed.

It is apparent that the VA's Chief Information Officer (CIO) has not had the enforcement powers needed to properly implement and execute the information security policies and plans of the Department. The Veterans Identity and Credit Protection Act will resolve this problem by bestowing the CIO with the power to better enforce information security requirements.

I am pleased the bill also outlines important credit protection services and fraud resolution services in the event of another data breach. If veterans' personal data is compromised they must be notified immediately and protected from criminal behavior.

I hope that today's hearing will shed further light on the need to make changes within the VA's information management infrastructure and lead to better safeguarding information security systems at the VA. We must work to ensure that the personal information of our nation's veterans is protected, and I believe the Veterans Identity and Credit Protection Act is an important step in the right direction.

Thank you again Mr. Chairman. I look forward to hearing from today's witnesses.

Honorable John Boozman

of Arkansas

Remarks for Full Committee Hearing on Cyber Security Bill

July 18, 2006

Thank you, Mr. Chairman.

I am so pleased that we have been able to put a bill together in such a quick turn around. I am glad to see that you were able to put additional tools into the bill to give the Secretary and the CIO more authority to give remediation to any veteran whose identity may have been compromised.

I am interested in the report regarding the feasibility of using personal identification numbers instead of social security numbers. So often when a veteran calls or writes my office they easily give over their social security numbers to gain assistance. In these uncertain times of identity theft it is important to protect veterans' information in any way we can.

Finally, I want to thank the Chairman, Ranking Member, and the staff of the Committee for all of their hard work in the past few months as we have dealt with the security breach.

Thank you, Mr. Chairman; I reserve the balance of my time.

Congressman Tom Udall (NM-3)
House Veterans Affairs Committee
Full Committee on Cyber Security Legislation
July 18, 2006

Mr. Chairman,

Thank you for holding today's hearing, and thank you to the many witnesses who will be testifying. While law enforcement has recovered the VA's stolen laptop and hard drive which contained the personal information on millions of veterans, and apparently there appears to be no evidence that the information on the laptop or hard drive was accessed, there continues to be a great need for comprehensive legislation that will overhaul the definition and authority of the Chief Information Officer at the VA, as well as more clearly outlined protection for veterans that will ensure their information is kept in the strictest confidentiality possible.

The legislation being forged today by this committee goes a long way to ensure that such protection is in place. From defining exactly what is meant by "data breach" and "identity theft" to demanding that any future incidents are more clearly and quickly reported by the VA, this legislation will make the needed changes to data security policy. Perhaps most importantly, this legislation provides the CIO with the authority to ensure compliance with FISMA, an important aspect that has been mission from the CIO position. As we heard during our numerous hearings on this issue, many former VA CIO's became frustrated with the difficulty of ensuring compliance with FISMA when they had no real authority. This legislation changes that and gives the CIO he or she needs.

I look forward to the testimony of our witnesses to hear if additional changes to the legislation are necessary. Mr. Chairman, thank you again for holding these hearings. I am pleased to see a good piece of legislation stemming from the several oversight hearings we have had on this issue. Again, thank you to all of today's witnesses for their testimony.

Thank you, Mr. Chairman.

U.S. Congresswoman
Ginny Brown-Waite
Representing Citrus, Hernando, Lake, Levy, Marion, Pasco, Polk, and Sumter Counties

Statement of Congresswoman Ginny Brown-Waite
Committee on Veterans' Affairs Legislative Hearing on Cyber Security Bill
7/18/2006
10:30 AM

Thank you Mr. Chairman,

It is more than apparent that the Information Technology system at the Department of Veterans Affairs is in dire need of reform. In the past, the Veterans' Affairs Committee has issued cyber security recommendations to the VA. Unfortunately, it appears as though the VA either did not listen or did not feel the need to act. This approach by the VA is unacceptable. Our veterans deserve better than the current system.

I am pleased that the House Committee on Veterans Affairs has put together legislation that will address some of the problems over at the VA. As Members of Congress, we have an obligation to exercise our oversight authority to ensure that a similar security breach does not happen again.

I want to thank Chairman Buyer, as well as the Committee staff for their efforts on this issue. I look forward to continuing to work with my colleagues to ensure that our nation's veterans receive the care and support they deserve.

July 18, 2006

Testimony of Congresswoman Darlene Hooley (OR-5)

Before the House Committee on Veterans Affairs

Legislative Hearing on Veterans Identity and Credit Protection Legislation

Good morning and thank you, Chairman Buyer and Ranking Member Filner for the opportunity to appear before the Committee. As one of millions of former credit card fraud victims and as a member of the House Financial Services Committee I have long had a strong interest in protecting consumers from potential ID theft threats and financial crimes.

Identity theft represents a fundamental threat to e-commerce, to our overall economy and to our Homeland Security. No longer are we facing just hobbyist hackers looking to create a nuisance. Increasingly these attacks are driven by skilled criminals and ID theft has become big business.

For the past six years, I've worked in the Financial Services Committee to protect consumers from the threat of ID theft. We've made significant progress in the recent past, including the signing into law of the Fair and Accurate Credit Transactions Act, or the FACT Act, in 2003. That bill, which I was proud to co-author with Congressman LaTourette, provided consumers with landmark new protections, including the right to free annual credit reports and the right to place a "red flag" fraud alert on their credit reports.

Last February, after data security breaches at data brokers Choice Point and Lexis Nexis, I began working on legislation to prevent future data breaches, to provide meaningful notification when consumers are placed at risk of harm by a security breach, and to provide consumers with additional protections when they are placed at risk of ID theft.

The need for such legislation was made crystal clear by the massive data security breach suffered by the VA in May. The details of that breach, which have been highlighted many times before this Committee, underscore the glaring weaknesses in data security policies and procedures at not only the VA, but throughout government agencies and the private sector.

Any data security bill passed by Congress must include a number of key ingredients to be effective.

First, it must mandate data security safeguards and require all businesses and government entities that handle sensitive personal financial information to have robust data security policies and procedures in place. Currently, many businesses and most government agencies are not required to employ such protections, leaving consumers at risk. Mandating protection of sensitive information is the first step in protecting consumers.

Second, legislation must mandate that all businesses and government entities immediately conduct an investigation upon learning that a breach of security might have occurred. That investigation should determine the information involved, whether or not the information is useable, and determine the likelihood that the information has been or will be misused.

Third, legislation should require that upon discovering a breach, the business or government entity notify the Secret Service, their functional regulator, each of the credit reporting agencies, and any third party who must take steps to protect consumers from resulting fraud or identity theft.

Fourth, legislation should include system restoration requirements that require any business or government entity to repair any breach and restore the security and confidentiality of the sensitive financial personal information and to make improvements to its data security policies and procedures.

Finally, legislation should require a meaningful consumer notice anytime a consumer is at risk of account fraud or identity theft. That notice should contain vital information to aid the consumer in protecting themselves from any harm that might result. In addition that notice should provide consumers who are put at risk of ID theft with opportunity to sign up for free of charge credit monitoring services.

Legislation I've coauthored, H.R. 3997, the Financial Data Protection Act, would accomplish exactly that.

However, the breach suffered by the VA, highlighted a few shortcomings of that legislation as it was passed out of the Financial Services Committee. In order to address those shortcomings, I introduced legislation shortly after the massive VA breach that would supplement H.R. 3997.

In the event of a data breach, H.R. 5487, the Veterans' ID Theft Protection Act of 2006, would:

- Authorize funding as necessary to the Secretary of Veterans Affairs to provide credit monitoring as required; and
- Make certain the VA has all necessary negotiating powers to secure the best possible price for the credit monitoring services.

In conclusion, Chairman Buyer and Ranking Member Filner, I would simply state that now is the time to act. The need for federal action on data security is clear and we should not wait for the next catastrophic breach to prod us to action.

Again, I thank you for the opportunity to testify before the Committee today and look forward to working with each of it's members in passing common-sense data security legislation.

MARSHA BLACKBURN
7TH DISTRICT, TENNESSEE
ASSISTANT MAJORITY WHIP

COMMITTEE ON
ENERGY AND COMMERCE

Congress of the United States
House of Representatives
Washington, DC 20515–4207

WASHINGTON OFFICE:
509 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225-2811

DISTRICT OFFICES:
7975 STAGE HILLS BOULEVARD
SUITE 1
MEMPHIS, TN 38133
TELEPHONE: (901) 382-5811

CITY HALL
109 3RD AVENUE SOUTH
SUITE 117
FRANKLIN, TN 37064
TELEPHONE: (615) 591-5161

1850 MEMORIAL DRIVE
CLARKSVILLE, TN 37043
TELEPHONE: (931) 503-0391

House Committee on Veterans Affairs

Hearing: "Cyber Security bill"

July 18, 2006
Testimony Submitted by Congressman Marsha Blackburn

Mr. Chairman, I want to thank you for holding these hearings and for inviting me to testify today regarding legislation I introduced with Representative Rob Simmons.

We drafted our Veterans Identity Protection Act this May in the days after Congress learned that the personal information of millions of the nation's veterans had been stolen from a Department of Veterans Affairs employee.

As Representative to a large military Post and a district with tens of thousands of veterans, this issue has clearly been a source of concern. I know that Representative Simmons who is a veteran himself has also heard the same thing from his constituents.

The idea that your identity could be stolen, your credit ruined, and your life impacted in such a negative way is absolutely unsettling and it's our responsibility to bring as much reassurance and assistance as possible to those veterans who have been touched by this theft.

The situation is very similar to the information breaches that have occurred with data brokers over the past year. Those instances led to Energy and Commerce Committee hearings that exposed just how easy it is to steal a person's identity by acquiring their financial information.

After the data breaches occurred, brokers addressed the situation by sending a notice to affected customers informing them that they could request a free credit report and free credit monitoring. Approximately, 10% of the affected people chose this option.

The bill Representative Simmons and I introduced follows a similar course of action. Instead of mandating a costly 100% coverage of free monitoring and reports, veterans would be provided a notice from which they could opt for these items. This keeps the cost down to millions, instead of billions of taxpayer dollars.

This legislation would also allow the VA to contract with credit agencies for reports and monitoring, which further keeps costs down. It would provide a free credit report every three months for the next year.

It has been reported the stolen laptop containing these veterans' information was not accessed or compromised. While that may be so, now is the time for the VA to coordinate with credit agencies for future data thefts -- which we hope will not occur, but as we have seen are increasingly a fact of life.

A recent report by VA's inspector general shows many shortcomings with the department and its security practices and vulnerabilities. We would be wise to remain concerned about the ability of the VA to secure the personal information of our veterans and it's my hope every step will be taken to prevent future thefts, and prepare contingency plans should a breach occur.

I will end by requesting that the committee consider including a provision to tie salaries and expenses at the department to the implementation of the IG recommendations.

I believe these steps are necessary to focus the department on this critical concern and ensure the appropriate steps are taken to protect veterans' personal information.

Mr. Chairman, this concludes my statement, and I am available to answer questions from the committee.

Statement of
Congressman John T. Salazar
Representing the Third Congressional District
Of Colorado
Before the Veterans' Affairs Committee
United States House of Representatives
Washington, DC
July 18, 2006

Chairman Buyer, Acting Ranking Member Filner, I thank you for the opportunity to come before the House Committee on Veterans' Affairs to testify with regard to certain provisions of the Veterans Identity and Credit Protection Act of 2006. I wish there was no need for this bill, but the simple fact is that on May 3 of this year, personal computer equipment containing the personal information of some 26.5 million veterans and 2.2 million active duty and reserve component service members and their spouses was stolen from the home of a VA employee.

This theft, while alarming on its own merit, brought to light a deep and more troubling tragedy regarding cyber security and communications at the Department of Veterans' Affairs. In the two months since the theft of this computer equipment, this committee has held five oversight hearings in which we heard from current and former VA employees, private sector experts on IT security, academics, and the Secretary himself. These hearings opened the Committee's eyes to numerous problems that have already been discussed.

The purpose of my testimony is to discuss provisions of the bill related to new notification requirements for the Secretary. I, like many of my colleagues in this committee, was outraged when I learned that there was a 19 day gap between the date of the theft and the day Congress and the public was notified. In response to the theft of this

data and the revelation that such delays in notification occurred, I introduced HR 5588. This comprehensive bill, much of which is adopted in the bill before the Committee today, addresses the notification structure and requirements within the Department should another data breach occur.

There are several subtle differences between this bill and HR 5588 so I will address the similarities of the two bills.

Both HR 5588 and the Veterans Identity and Credit Protection Act of 2006 codify in federal statute the manner in which the Secretary of Veterans' Affairs is to notify both Congress and affected individuals involved in a data breach. By outlining the manner, content and timeframe under which the notification of a data breach takes place, it is my hope we can prevent a repeat of the 19 day delay we witnessed in May.

Under the provisions of both bills, this committee and our counterparts in the Senate are to receive notice of any breach "without unreasonable delay following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system." More importantly, however, HR 5588 proscribes the way in which the Secretary is to notify affected individuals. Each individual is whose information has been compromised shall be notified in writing without unreasonable delay and that notification will include the following:

- A description of the personal information that was acquired during the breach;
- A telephone number the individual may use at no cost to make inquiries about the breach;

- Toll free contact numbers for the major credit reporting agencies;
- Toll free telephone number and website address for the Federal Trade Commission; and
- Information regarding the right of an individual to place a fraud alert, obtain a security freeze, and receive credit monitoring where applicable.

There are relatively few differences between HR 5588 and the Veterans Identity and Credit Protection Act in this section of the bill. Mr. Chairman, I hope to work with you in the next two days to address some of these minor differences and come to agreement on any amendments that may need to be made.

Mr. Chairman, I would like to conclude by thanking you and Acting Ranking Member Filner for holding this hearing today as well as the previous five oversight hearings. I feel this committee can work in a bipartisan manner to pass a finely crafted, comprehensive piece of legislation that I think will serve our veterans well. The bill makes much needed changes to the VA culture of indifference which we heard so much about during our oversight hearings. By ensuring that VA officials have both resources and authority to implement IT security, it is my hope we can prevent future breaches of data especially those on the magnitude of the one we saw this year. In addition to those changes, I am happy that this bill affords veterans whose identities may be compromised the opportunity to seek appropriate remedies to protect their identity including the use of fraud alerts and credit freezes.

Mr. Chairman, I thank you for inviting me to testify before the committee today. Your work and dedication to fixing the bureaucratic inefficiencies and problems within VA as well as your commitment to protecting veterans is very much appreciated.

Testimony of Rep. Shelley Moore Capito
Veterans Identity Protection Legislation
July 18, 2006

Chairman Buyer, Ranking Member Evans, and Members of the Committee:

I want to thank you for holding this important hearing today and for giving me the opportunity to testify on the important issue of protecting the personal data of our nation's veterans. My state of West Virginia has long had one of the highest per capita rates of military service, making veterans issues and the protection of personal data an issue with direct implications for tens of thousands of our state's residents.

The loss of the personal data of over 26 million veterans and service personnel last month has highlighted the need for legislation to protect the credit of those who have bravely served our nation.

Identity theft can have extremely negative consequences for those impacted. Because the government handles large amounts of personal data, it is vital that we have policies to protect information from theft and help victims cope.

Later this week we will celebrate the 75th anniversary of the Department of Veterans Affairs. As the department carries out its mission of caring for our veterans, we must ensure the Department is adequately protecting veterans from identity theft.

First, I commend the Department for offering free credit reports to those veterans whose personal information was exposed. It is important that government take responsibility for its mistakes.

The legislation I introduced would establish an Office of Veterans Identity Protection within the Department to prevent the loss of personal data, and to work with credit reporting agencies, law enforcement agencies, and veterans to mitigate the impact if data is lost.

I commend the committee's draft bill for its creation of a new Under Secretary for Information Services who would serve as a "Chief Information Officer" for the Department. Advances in technology open up exciting possibilities for using information, but the complexities involved in technology often make it that much easier for those who want to access data for illegal purposes. It is important that the Department of Veterans Affairs, and other government agencies, have a proper management structure in place to protect personal information.

It is important and appropriate that a mandate to properly report information losses to law enforcement entities, the Federal Trade Commission, this Congress, and the public be included in any legislation we pass. In the recent security breach, the VA initially attempted to resolve the situation internally. Clearly, the best chance we have to

prevent lost or stolen data from being used by criminals is to get law enforcement involved as quickly as possible so they can begin recovery efforts.

Veterans themselves should be notified as quickly as possible so that they can immediately begin to monitor their bank accounts and credit activity. Congressional committees should be notified so that proper oversight can be exercised and if necessary, legislation to provide additional protection or help prevent future data losses can be considered promptly.

We must also remember that in the recent security breach, the personal data of up to 1.1 million active duty military personnel, 430,000 National Guard members, and 645,000 Reserve personnel were also compromised. My legislation would require that the Department of Veterans Affairs work closely with the Department of Defense to ensure that these active duty personnel have access to credit reporting services.

Our nation's military forces, particularly those deployed in combat operations in Iraq, Afghanistan, and elsewhere around the globe already bear a heavy burden as they bravely defend our nation. The last thing they need to worry about is whether someone is illegally accessing their credit.

I believe strongly that anyone removing personal data without authorization should be punished. My bill contains a provision that would allow for criminal penalties for anyone who removes personal data without proper authorization. We can and should establish a structure within the Department to protect personal data, but these policies will not do much good if they are ignored. My bill would make it a felony, punishable by fines or up to two years in prison for removing personal data without proper authorization. I believe stiff penalties are important as a deterrent to violating data security procedures.

I agree with provisions of the Committee's discussion draft that would prohibit the release of personal data by any Department contractor and require contracts to include penalties for data breaches that would pay for credit protection services. It is crucial that any contractor with access to personal data be a strong partner in protecting the identities of veterans.

Mr. Chairman, I want to thank you for your willingness to tackle this important issue to our nation's veterans and look forward to working with you and other members of the committee to pass legislation to provide these vital identity protections.

Opening Statement of
John A. Gauss
Former Assistant Secretary for Information and Technology
And Chief Information Officer
At the Department of Veterans Affairs

Before the
Committee on Veterans' Affairs
U. S. House of Representatives

July 18, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here today to discuss some of the important issues related to the draft legislation to enact the "Veterans Identity and Credit Protection Act of 2006".

My comments today are focused on those elements of the draft legislation relating to the management of the Department of Veterans' Affairs (VA) Information Technology and Information Security programs.

As a private citizen interested in the welfare of our nation's veterans and the efficient operation of government, I would like to commend the Chairman and this Committee for exercising such bold leadership by moving forward with this groundbreaking piece of legislation. By elevating the positions of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at the VA to Under Secretary and Deputy Under Secretary positions respectively, you are blazing a trail for the rest of the executive branch of government to follow. Based on 34 years of government service in the Department of Defense and at the VA, it has become clear to me that until the position of CIO is elevated to an Under Secretary position within all Departments of the Executive Branch of government, the authors of the Information Technology Management Reform Act of 1996 will remain disappointed. As an Under Secretary, the CIO will have a "seat at the table" where the real decisions are made with respect to the operation of the Department and he or she will not be relegated to subordinate "working groups" that can only recommend and not decide.

I know the Committee is struggling to determine the appropriate level of legislative direction to enact into law. Too little direction will allow the advocates of the status quo to find loopholes in the law or legal interpretations to preserve "business as usual". Conversely, too much detail becomes legislative micromanagement which I know is not the intent of this Committee. With that said, although some of the recommendations I will put forth below are aimed at proposing changes to the draft legislation, other recommendations should be considered for direction to be placed in appropriations bills, policy to be implemented by the Office of Management and Budget, and/or discussion points that could be used during future Senate confirmation hearings.

With respect to the draft legislation, I would respectfully request that the Committee consider the following:

(1) Section 2 of the draft legislation provides for strengthening the CIO's ability to enforce information security requirements to achieve compliance with the Federal Information Security Management Act of 2002 (FISMA). Since FISMA applies to all Departments and Agencies of the federal government, I can appreciate the difficulty in legislating enforcement authority for all Departments and Agencies. However, given that enforcement has been a key issue with the VA at previous hearings, I recommend the Senate Veterans' Affairs Committee consider asking future VA Secretary nominees about their views regarding Section 2 of this legislation with respect to, and I quote, "to the extent determined necessary by the head of the agency, to enforce", during future confirmation hearings.

(2) Section 3 of the draft legislation establishes the position of Under Secretary for Information Services, elevating the CIO position from an Assistant Secretary. Section 3(c) of the draft legislation is titled "Conforming Amendment". It addresses a change to the existing statute regarding the responsibilities of Assistant Secretaries and Deputy Assistant Secretaries at the VA by removing the responsibilities for Information management functions. Since the draft legislation elevates the CIO from the position of an Assistant Secretary to the position of an Under Secretary, the Committee may want to consider decrementing the number of Assistant Secretaries defined in Section 308(a) of the same statute from seven to six as a part of this "Conforming Amendment" of the draft legislation.

(3) In Section 4 of the draft legislation, a new Section to Title 38, United States Code defines three Deputy Under Secretary positions that would report to the new Under Secretary for Information Services. At a recent House Veterans' Affairs Committee hearing, the representative from the Gartner Group, my colleague on this panel and I testified that, in our expert opinion, the VA should centralize the management of all systems development activities under the Office of the CIO. Although this legislation does not specifically mandate this degree of centralization for the VA, I believe there are program management oversight and Enterprise Architecture responsibilities that must be carried out by the CIO independent of the centralization issue. Lack of an effective Enterprise Architecture and inadequate executive oversight of ongoing development programs have been long standing issues identified by the GAO. Both my colleague and I addressed these issues during our tenures as VA CIO. In order not to loose sight of these important functions, I am recommending to the Committee that a fourth Deputy Under Secretary position be established as part of the draft legislation – Deputy Under Secretary for Enterprise Architecture and IT Program Management Oversight.

(4) In Section 4 of the draft legislation, several new Sections to Title 38, United States Code relate to contracting activities associated with the handling of sensitive personal information. In my review of the draft legislation, I was unable to find any prohibitions for offshore storage of, or access to, this sensitive information from

companies that might operate outside the United States. I recommend the Committee consider adding such prohibitions to the draft legislation.

(5) A CIO must be more than just the "IT person" for a Department or Agency. To be effective as a CIO, I believe the CIO also must be the "change agent" of the organization from a business perspective. The CIO, working with the Administrations and Department's offices, must lead the cross functional integration of business processes in order to improve mission effectiveness and gain efficiency. A single 1-800 number for a Veteran to call to obtain service and one integrated registration process are but two examples of improvements that should be pursued. The CIO must establish plans and have the authority to implement those plans to control the growth of Information Technology spending. The CIO must understand that data is a strategic capital asset. He or she must understand how best to store the information and make it available only to those who must use the data to service our nations' veterans in a secure and protected manner. Mr. Chairman and Members of the Committee, I most strongly recommend that future nominees for the newly established position of Under Secretary for Information Services be required to have these skills and demonstrate during the confirmation process how they will apply these skills at the VA.

(6) The qualifications for the Deputy Under Secretary for Security are equally as important as the qualifications for the CIO. I believe this person must be a Certified Information Systems Security Professional (CISSP) and demonstrate a comprehensive understanding of cyber security in general, information security, details of FISMA and be thoroughly versed in physical and personnel security related issues as they pertain to electronic and information security. Security is all about risk management. The only secure computer is one you never turn on. The only secure building is one that no one can ever enter. The Deputy Under Secretary for Security must demonstrate that he or she knows how to evaluate risk and take steps to mitigate that risk. I most strongly recommend that future candidates for the newly established position of Deputy Under Secretary for Security be required to have these skills and demonstrate during the hiring process how they will apply these skills at the VA.

(7) In executing the duties of the Under Secretary for Information Services, the CIO must not forget the times that we live in where Continuity of Government, Continuity of Operations and the VA's fourth mission in support of emergency preparedness are missions critical to servicing our veterans and the nation. The CIO must be intimately involved in using Information Technology to further these objectives.

(8) With respect to accessing sensitive and critical information, I believe it is imperative that the CIO be responsible for electronic identity management at VA and that electronic identity management be implemented with a sense of urgency to comply with Homeland Security Presidential Directive 12 (HSPD 12). Electronic identify management will not only strengthen access controls for electronically stored data, it can also be used to strengthen physical access controls throughout the VA.

(9) Policies need to be implemented and funding must be provided to encrypt data while in motion or at rest. The implementation of data encryption must be closely coupled with the electronic identity management process just discussed.

(10) Finally, I once had the privilege to meet Mr. Louis Gerstner when he was the Chief Executive Officer of IBM. He shared with me the actions he took to transform IBM's business processes and information technology from a collection of stovepipes to a highly integrated machine. He reorganized the management of all of IBM's Information Technology by centralizing the authority with the Corporate CIO in less than 90 days. Over the next two years and on a global basis, IBM transitioned its IT stovepipe infrastructure to a modern, integrated corporate wide infrastructure. During the same two year period, he led the modernization of IBM's business processes focusing on eliminating duplication, improving productivity, increasing efficiency and effectiveness, and reducing IT cost. Mr. Gerstner emphasized the need for speed. He believed that the absence of speed would allow the inertia of the status quo to prevail. Since this legislation is clearly focused on effecting real change at the VA, this change must be implemented with lightning speed to be effective. Therefore, I recommend the committee consider including two additional items in this legislation to enable a high velocity change at VA.

(a) First, the VA should be given 90 to 180 days to fully implement this legislation. The advocates of the status quo will argue that speed will create too much risk and that deliberate thought and study is necessary to avoid creating problems. Given the current situation at the VA, isn't the risk associated with the status quo significantly greater than whatever damage might be caused by moving forward with lightning speed?

(b) Second, the VA should be given the same hiring authority to support the implementation of this legislation that was given to the Department of Homeland Security in the legislation that formed that Department. If VA uses the "business as usual" hiring processes, it will take months or even years to properly staff the offices established by this legislation.

I hope the information I have provided in this opening statement will help the Committee in its deliberations and thank you for this opportunity to discuss this landmark legislation. I will be happy to answer any questions you might have.

Statement of the Honorable
Gordon H. Mansfield
Deputy Secretary
Department of Veterans Affairs
Before the Committee on Veterans' Affairs
U.S. House of Representatives
July 18, 2006

Mr. Chairman and Members of the Committee,

I am pleased to provide the Department's views on eight bills, all intended to protect the personal privacy of veterans and others affected by the May 3, 2006 theft of computer equipment containing veterans' personal data. While you had also invited our views on a draft bill your staff shared last week, I regret that time has not permitted us have cleared positions on its many provisions. We will supply those for the record once the necessary executive-branch coordination is completed.

Initially, I wish to point out that the eight bills covered in my testimony were introduced before the stolen computer hardware was recovered. As you know, the FBI has concluded with a high degree of confidence that, based upon its forensic examination and other evidence developed during its investigation, the veterans data were not accessed or compromised prior to their recovery. That development has eliminated the need for much of what is proposed in the legislation, and while we understand the concerns that engendered these eight bills we do not support their enactment.

H.R. 5455

H. R. 5455, the "Veterans Identity Protection Act of 2006," would require the Department of Veterans Affairs to: (1) provide notification to each individual whose personal information was included in the recent data breach; (2) provide to any of these individuals a free one-year credit monitoring service; (3) provide a copy of that individual's credit report once annually during the two year period following the termination of the credit monitoring services; and (4) certify in writing to Congress that any individual whose personal information has been compromised due to data security lapses at the Department has been appropriately notified in writing

The Secretary has already taken proactive and aggressive steps to notify all individuals whose personal information was potentially at risk as a result of the May 3 data theft. Also, the recovery of the data, apparently uncompromised, eliminates the need to offer credit monitoring or additional free credit reports at this time.

In addition, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*, requires each of the three major credit bureaus to provide, upon request, a free copy of an individual's credit report once every twelve months and upon the individual's placement of an initial fraud alert on his or her credit file. Therefore, an individual who places an initial fraud alert could make a request to each of the three credit bureaus and receive up to six free credit reports annually. The Department's website at http://www.va.gov. documents the actions taken by the Secretary in this regard and advises veterans how to place a fraud alert with, and obtain free credit reports from, the credit bureaus. For these reasons, H.R. 5455 is unnecessary.

H.R. 5464

H. R. 5464, the "Veterans Identity Protection Act," would require VA to: (1) provide detailed notification to each veteran whose personal information was included in the data breach; and (2) include a form for the veteran to elect to receive a free credit report once every three months for the year following notification and free credit monitoring for that year also. The bill also would limit the funds available to Office of the Secretary to 90 percent of the funds otherwise available if the 16 information security recommendations of VA's Inspector General are not fully implemented by January 1, 2007. The bill would limit the funds otherwise available to the Office of the Secretary by 10 percent in subsequent fiscal years, after January 1, 2007, for any information security recommendation not fully implemented.

VA supports the underlying intent of H.R. 5464, but cannot support the bill. In addition to the actions already discussed, VA is taking steps to implement the 16 information security recommendations. The Secretary has established an Information Security Task Force composed of senior officials and has hired a Special Advisor on Information Security. Working together with the Chief Information Officer of the Department, these individuals will implement the recommendations. For these reasons, we believe that H.R. 5464 too is unnecessary.

H.R. 5467

H. R. 5467, the "Veterans Identity Security Act of 2006," would establish criminal penalties for knowingly disclosing without authorization records containing personal information about veterans. The bill would amend title 38, United States Code, by adding a new section 5706 applicable to officers, employees, contractors, and volunteers of the Department who disclose personal information without lawful authorization. The bill defines personal information as "name, date of birth, address, phone number, Social Security number, and (if applicable) disability rating." Penalties range from fines to imprisonment for up ten years when there is intent to sell, transfer, or use the personal information for commercial advantage, personal gain or malicious harm.

VA has no objection to the intent of H.R. 5467 but has several technical suggestions for improving its drafting and coverage. We would be happy to discuss these with Committee staff at its convenience.

H.R. 5487

H. R. 5487, the "Veterans' ID Theft Protection Act of 2006," would also require VA to notify any person affected by the breach, but also to notify consumer reporting agencies and appropriate third parties who may be required to act in a manner to further protect affected persons from fraud or identity theft. The notice specifications must include details of the breach, current safeguards of personal information, contact information for the Department, information provided by the Federal Trade Commission (FTC) regarding identity theft, information on obtaining a copy of a consumer's credit report free of charge and other information regarding placing a fraud alert on one's file and contact information for the FTC. The bill also would require the Department to offer affected persons free credit monitoring service, at their request, for not less than six months, and to take prompt and reasonable measures to repair the data breach that would improve the data security policies and procedures.

For reasons already discussed, H.R. 5487 is unnecessary.

H.R. 5490

H. R. 5490, the "Veterans Identification Protection Act," would require the Department of Veterans Affairs to: (1) provide a four-digit personal identification number (PIN) for each veteran who receives or applies for VA benefits, and (2) take steps to provide that any entity entering into a commercial transaction with a veteran that "includes the extension to the veteran of credit, a loan, or any other thing of value" shall verify the veteran's identity through the PIN established. Any entity that is required to so verify a veteran's identity, but fails to, would be liable to that individual for all attorney fees and injuries incurred by that individual resulting from that failure.

VA does not support H.R. 5490. VA understands that the current level of security as recommended by the National Institute of Standards and Technology and other security experts requires a PIN number with more than four digits. However, even if the bill were amended in this regard, VA would be opposed to the requirement that the Secretary provide, assign, monitor, or validate any universal PIN number exclusively for the use of veterans in commercial enterprises. The bill is unclear about the commercial enterprises to be covered. For example, there is no distinction made between commercial activities with a VA involvement (such as a home loan guarantee) and other commercial activities a veteran may be involved with that have no VA connection.

H.R. 5577

H. R. 5577, the "Veterans Identity Protection Act of 2006," is intended to enhance the protection from disclosure of VA records containing personal identifying information that is required by law to be confidential and privileged.

It would require the Department to establish an Office of Identity Protection, administered by a Director who shall be appointed by the Secretary. The Office would notify each individual whose personal information has been lost or compromised, provide him or her with one credit report every six months for three years at no charge, offer a 24-hour toll-free telephone number and a web site to provide information regarding credit reporting services, ensure that active-duty military personnel have access to credit reporting services, make information available on possible fraudulent consumer credit or reporting services that may be targeted at affected veterans and service members and notify the Department of Justice and the FTC immediately when personal data in VA records may have been compromised. Furthermore, the Act would require the VA Inspector General (IG) to conduct a study of the data-security practices at VA and submit a report not later than six months after the date of the law's enactment to the Senate and House Committees on Veterans' Affairs. Finally the Act would impose criminal penalties of a fine or imprisonment on any VA employee who removes records from VA custody without proper authorization.

VA supports the underlying purposes of H.R. 5577, but cannot support the bill. In addition to the ameliorative actions already discussed, VA has provided a toll-free telephone number and a section on the Department's web site with information for those individuals seeking assistance, and established an Information Security Task Force to improve data security. While the Information Security Task Force will consider administrative alignments to enhance data security protections, there does not appear to be a need for a separate administrative Office of Identity Protection at this time. And, as already noted, FCRA already provides up to three free credit reports annually, and up to another three annually when an initial fraud alert is placed. For these reasons, we do not believe that these provisions are necessary.

The requirement for the VA IG to report on the Department's progress in implementing data security improvements within six months after the law's enactment would not allow sufficient time for the Department to address corrective actions before the report must be submitted. Furthermore, the VA Inspector General regularly issues reports about data security practices within VA in Federal Information Security Management Act (FISMA) audits and consolidated financial statement audits performed annually. There does not appear to be a need for additional reports in this area.

In addition, the criminal penalty provision is not sufficiently specific for enforcement purposes. In particular, the bill does not specify whether "remove from the custody of VA," refers to removal from the "custody of a VA employee" or any removal from a "VA worksite." H.R. 5577 also does not consider the reality that files leave the worksite every day for legitimate purposes, nor does it identify the specific part of title 18 that would provide for the fines imposed for such action. We could support enactment of the additional criminal penalties in H.R. 5467 if those provisions were amended as discussed above.

H.R. 5588

H. R. 5588, the "Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006," would require the Secretary of Veterans Affairs to: (1) issue policies and procedures to safeguard sensitive personal information before the end of the 90-day period beginning on the date of the enactment of the Act; (2) notify the Secret Service, VA IG, Senate and House Committees on Veterans' Affairs, the FTC, and the affected individual of any breach: (3) place fraud alerts or security freezes in the credit file of affected individuals; (4) provide affected individuals with credit monitoring services; and (5) establish the position of an Ombudsman for Data Security within the Department to provide information and assistance to such individuals.

In light of the ameliorative actions outlined above, VA does not believe that H.R. 5588 is necessary and does not support enactment.

H.R. 5636

H. R. 5636, the "Social Security Numbers Privacy and Protection Act," would require: (1) the alteration of selective service reminder mailback cards; and (2), the elimination and prohibition of social security account numbers from Medicare, Medicaid, and SCHIP- and VA-issued health care identification cards by the end of the two-year period after the enactment of the Act

VA supports alternative methods for the identification of veterans for the purpose of providing health care or other benefits available under Title 38. To that end, VA has already removed the social security numbers from the Veterans Identification Cards known as VIC cards and is therefore already in compliance with the bill. With respect to Medicare, Medicaid, and SCHIP programs, the Department of Health and Human Services advises us that instituting a new number for use on the identity cards used for these programs would entail substantial expense and require a substantially longer time than allowed by the bill. They are continuing to work on these efforts. Therefore, we believe that enactment of H.R. 5636 would not be productive.

Conclusion

As I have indicated, VA already has implemented many of the provisions of the various bills that provide, among other things, stronger safeguards to protect against data breaches within the Department. VA is strongly committed to providing all available protections to the safety and security of personal information of all veterans' and their beneficiaries. As we continue to work on improvements in our systems and procedures, we will be pleased to work with your Committee in fostering methods to achieve a level of information security that is responsible and necessary.

STATEMENT OF

JAMES A. WILLIAMS
COMMISSIONER

FEDERAL ACQUISITION SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

COMMITTEE ON VETERANS AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

JULY 18, 2006

Good Morning Chairman Buyer, Ranking Member Evans and Members of the Committee, I am Jim Williams, Commissioner for the Federal Acquisition Service of the General Services Administration (GSA). I am pleased to have this opportunity to appear before you to discuss the programs we have put in place to assist agencies in being able to respond to data protection/credit protection scenarios.

GSA helps Federal agencies better serve the public by offering the best value, superior workplaces, expert solutions, acquisition services, and management policies. One of the most important ways that we do this is through the Multiple Award Schedules (MAS, pronounced "M-A-S") program.

Through the MAS program, GSA establishes contracts with firms, large and small, to provide commercial products and services to the Government at competitive prices.

GSA's MAS program is one of the most powerful business tools available to Federal Government agencies. The schedules can be used by ***all*** Federal agencies as a streamlined, convenient, money-saving, and time-saving tool for obtaining the commercial goods and services they need. To obtain the commercial services offered under the MAS program, agencies need only develop a request outlining the work to be performed, invite schedule contractors to respond, and award task orders. The MAS program mirrors commercial buying practices more than any other procurement process in the Federal Government; Federal agencies receive fast, direct access to the commercial products and services of all businesses of all sizes and classifications, including numerous small businesses. When combined with E-Buy, GSA's electronic request for quote system, the process is also transparent.

The MAS program consists of 43 separate groupings of like products and services, called schedules, and covers everything from office products, furniture, tools and appliances to scientific products, information technology, training, business consulting, security related products, and financial services, to name just a few. Overall, the MAS program includes over 17,000 thousand contractors providing over 11 million different products and services. Streamlined ordering procedures, robust e-tools, and efficient processes merge transparency, speed, and efficiency in the Government's premiere acquisition program. Agencies will spend over $35 billion through the MAS program this year to meet their needs.

One of the key features of the MAS program allows agencies to establish Blanket Purchase Agreements (BPAs). BPAs are used to fill recurring needs for supplies or services, while taking advantage of quantity discounts, saving administrative time, and reducing paperwork.

BPA's eliminate continual contracting solicitation costs for recurring needs. BPA's also—

- Provide an opportunity to negotiate improved discounts;
- Reduce administrative efforts by eliminating repetitive individual orders and payments;
- Let customers obtain better value by leveraging buying power through volume purchasing;
- Enable an ordering agency to use streamlined ordering procedures;
- Allow for quicker turnarounds on orders; and
- Permit an ordering agency to incorporate additional terms and conditions which do not conflict with the underlying schedule contract.

A BPA may be set up for all the field offices of an agency across the nation, allowing them to reap additional discounts. GSA is also able to establish a multi-agency BPA further leveraging the Government's buying power.

One MAS program schedule which is particularly appropriate to discuss in light of the reasons we're here today, is the Financial and Business Services Schedule. This is a schedule of approximately 425 contracts representing expertise in financial areas such as accounting, auditing, budgeting, financial management, loan servicing, debt collection, asset management, asset sales, and business

reporting. In 2005, sales under this schedule totaled approximately $745 million and it continues to rapidly grow. This schedule also includes 21 contractors with expertise in credit ***reporting*** and at least three firms with expertise in credit ***monitoring***.

Over the years, GSA has worked very closely with the Office of Management and Budget (OMB) and the Federal Credit lending agencies in designing and continually improving the Financial and Business Services Schedule. In past years, the Small Business Administration and the Department of Treasury have used this schedule to sell loans and other assets, the Department of Education has used it for loan servicing and collection of delinquent student loans, and most recently the Internal Revenue Service has awarded a set of contracts for collection of delinquent tax debt.

Based on GSA's strong track record in this area, I am pleased that GSA was offered the opportunity to lead the procurement of credit monitoring services on behalf of several Government agencies.

As this hearing and the Committee's draft legislation signify, identity theft is a serious issue. When an agency experiences a data loss, there can be serious problems for our employees and the citizens of this Nation. The Federal Government must be in a position to respond to situations quickly and effectively. Federal agencies do not have the luxury of time to embark upon a prolonged procurement process on their own.

With GSA's BPA for credit monitoring in place, an affected agency has quick and ready access to the industry experts it needs. In recent months, numerous agencies, including the Department of Veterans Affairs, the Department of Agriculture, the Federal Trade Commission, the Department of Energy, and the Department of the Navy have all faced situations where sensitive personnel information such as employee names, addresses, and social security numbers were potentially compromised.

When VA decided that it would offer free credit monitoring to any veteran whose personal information was potentially compromised, it turned to GSA for help in providing services to complete this task.

GSA identified the Financial and Business Services schedule as the best way that GSA could help VA. GSA employees immediately went to work and have continued to work closely with VA to create and develop a performance based Statement of Work for commercial credit monitoring services.

Because this is a Governmentwide problem, we also worked closely with OMB to offer GSA's help in providing a Governmentwide solution. This way, all agencies facing a data breach will have a fast and cost effective remedy available.

The requirement for credit monitoring services is a very real requirement across the Government, and I am delighted to report that GSA and VA have continued to work closely to establish a Governmentwide solution to provide protection in the event of future security breaches.

On July 10, 2006, GSA invited 21 contractors under the Financial and Business Services Schedule to compete for Multiple Blanket Purchase Agreements. Under this competition, these 21 firms have been asked to propose three different levels of remedy, based on the extent of the risk of exposure. The firms have been asked to quote different levels of credit monitoring services, ranging from basic (single monitoring) to comprehensive coverage (reports called three-in-one which cover all three of the major credit bureaus). A key feature will be that, based on the degree of vulnerability, risk and protection, ordering agencies will be able to select the most appropriate level of credit monitoring services.

Some of the other features we are looking for in credit monitoring include the following:

- Providing credit reporting services,
- Implementing solutions to detect early signs of fraudulent activity and identity theft,
- Reporting lost or stolen Social Security numbers to the three national credit bureaus and requesting fraud alerts and statements on all credit files,
- Contacting the victims' creditors and law enforcement agencies,
- Making dedicated fraud resolution representatives available for victims of identity theft,
- Placing extended alerts on credit reports,
- Reviewing credit files every 30 days,
- Providing credit alerts within 24 hours of fraudulent activity,
- Providing updated credit scores with data compiled from all three national credit agencies,
- Providing important contact information and addresses to affected individuals for use in resolving identity theft issues,
- Identify theft insurance, and
- Outlining various levels of credit monitoring services based on the degree of vulnerability, risk and protection with an explanation for the degree of monitoring selected.

Contractors will be held to high standards, including compliance with the Privacy Act of 1974, to guarantee strict confidentiality of the information provided by the Government during the performance of the task order. We are also requiring rigorous restrictions on the contractors' authorization to disclose information.

Responses to the BPA request are due on Monday, July 24, 2006. GSA will then evaluate the responses to be sure that we award to companies demonstrating the knowledge, understanding and technical capability required to perform the credit monitoring services. We plan to make awards in August and expect several Federal agencies to begin placing orders the same month.

In conclusion, I would like to state that this situation is a good example of the important mission that GSA plays in helping our Government stop identity theft and protect the privacy of individuals. We are bringing together the best talents of the private sector to recognize and remedy a problem. We

are mobilizing and providing a shared services solution, so that we can leverage the Government's buying power, drive down prices, drive up service delivery, and provide a fast and agile response to security breaches.

I am very proud of the hard work that the GSA team has already put into this effort and look forward to a highly successful award of several BPAs next month. We join the Committee in its commitment to better protect the sensitive personal information of veterans. While GSA is still studying the impact of the draft legislation, we look forward to working with this Committee to ensure that any legislation and our current procurement efforts are properly coordinated and mutually supportive of our common goal of protecting sensitive government data and obtaining needed credit protection services. I look forward to answering any questions you might have.

STATEMENT OF
PETER S. GAYTAN, DIRECTOR
VETERANS AFFAIRS AND REHABILITATION COMMISSION
THE AMERICAN LEGION

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

ON

DRAFT LEGISLATION TO BETTER PROTECT THE SENSITIVE PERSONAL INFORMATION OF VETERANS

JULY 18, 2006

STATEMENT OF
PETER S. GAYTAN, DIRECTOR,
VETERANS AFFAIRS AND REHABILITATION COMMISSION
THE AMERICAN LEGION
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
ON THE
DRAFT LEGISLATION TO BETTER PROTECT THE SENSITIVE PERSONAL INFORMATION OF VETERANS

JULY 18, 2006

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to present The American Legion's views on this proposed legislation. On May 3, 2006, the home of a Department of Veterans Affairs (VA) employee was burglarized. The burglary was reported to the local police. It is reported that the employee discovered that computer equipment, which contained personal information on approximately 26 million veterans and military personnel, was among the items stolen, he immediately notified VA management in the Office of Policy, Planning, and Preparedness, including Security and Law Enforcement personnel. The employee reportedly advised all of them that the stolen personal computer equipment contained VA data. However, the VA Secretary was not informed of the incident until May 16, 2006, almost 2 weeks after the data was stolen. The Congress and veterans were not notified until May 22, 2006. VA's failure of leadership in establishing Information Technology (IT) reform over the past three years has undeniably led to the current crisis we are now addressing.

While the stolen laptop and external hard drive have been recovered and reports from the F.B.I. stated that the information on the equipment was not accessed, The American Legion's position is that legislation still needs to be enacted to protect all effected veterans and servicemen from any possible future unauthorized release of their personal information. Even a high likelihood that the information was not accessed is not a guarantee that it was not. According to the July 11, 2006 report of the Office of Inspector General (OIG) there was no, "encrypting or password protecting the data." Originally, VA tried to mitigate the risk involved saying that most of the critical data was stored in files protected by a statistical software program, making it difficult to access. The OIG reported that, "This, however, was not the case because we were able to display and print portions of the formatted data without using the software program."

Equally disturbing is the more recent news of other security breaches that have only come to light because of the spotlight that is now on the VA. It wasn't until a follow up hearing on the data breach on June 29, 2006 that 10 pages of security breaches were presented to this Committee to include an incident in Minnesota that occurred in 2005. The August 1, 2005 cut off date in the proposed legislation puts veterans who may have had their information compromised before that time at risk of having no help from VA in the future. Because we may

never know the extent of the lapses in VA IT security, it is The American Legion's position that VA be appropriated the necessary funding to monitor all veterans' credit who are victims of identity theft as a result of security breaches regardless of when these breaches may have occurred. On June 21, 2006, Secretary Nicholson announced that the VA would provide one year of free credit monitoring to people whose sensitive personal information might have been stolen in the latest incident. This promise should not be broken. The Secretary stated, "Free credit monitoring will help safeguard those who may be affected, and will provide them with the peace of mind they deserve." The American Legion agrees with the Secretary's statement.

The American Legion is supportive of the proposed legislation and the attitude of Secretary James Nicholson which are in agreement with what the VA OIG report recommended, namely: (1) take whatever administrative action deemed appropriate concerning the individuals involved; (2) establish one clear, concise VA policy on safeguarding protected information when stored or not stored on VA automated systems; (3) modify mandatory Cyber Security and Privacy Awareness training; (4) ensure that all position descriptions are evaluated and have proper sensitivity level designations, and that required background investigations are completed in a timely manner; (5) establish VA-wide policy for contracts that ensures contractors are held to the same standards as VA employees and that protected information used on non-VA automated systems is safeguarded; and (6) establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems.

The American Legion also offers the following recommendations related to the draft legislation:

Section 4. Department of Veterans Affairs Information Security: Under **section 5721. Definitions,** subparagraph (7), which identifies what sensitive personal information is, should include any information with regard to family members as well.

Under section 5725. Provision of credit protection services and fraud resolution services: This section does not address the issues of whether or not the victim will be liable for any fiscal loss due to VA's mistake; to what extent the VA will make the victim whole; how are multiple occurrences of identification theft handled?

Under subparagraph **(g) (2) Fraud Alerts,** what happens if identity theft occurs after the one-year monitoring period? What if stolen data is held for longer than one year before it is used?

Finally, The American Legion wants legislative assurances made to veterans that if their information is compromised by VA, unless it is undeniably the result of some other cause, the VA or federal government will assume the responsibility of any loss incurred by the veteran or relevant family members. Veterans should never be required to have to prove it was the fault of VA that they were the victims of identity theft if VA has already put them at risk.

The American Legion urges patience in allowing the Federal government to continue working toward a fair and expeditious resolution to this matter. It is the position of The American Legion that to bring the judicial branch into this by filing a lawsuit will only impede the process. Filing a lawsuit against the VA will not act as a catalyst for reform; in fact, it will slow down the

process. Neither will it expedite the passing of legislation that would compensate veterans for the cost of monitoring and protecting their current credit ratings and personal accounts or for those who may become victims of identity theft.

The American Legion stresses the importance of a swift resolution to this issue by avoiding the inevitable delays and unfair rulings that often result from class action suits. The outcome of the Agent Orange class action settlement should serve as a reminder that judicial oversight isn't always the best remedy. This historic case did not equate to fair compensation for veterans exposed to Agent Orange. Out of about 105,000 claims received, 52,000 totally disabled veterans or their survivors received payments averaging approximately $3,800. This certainly didn't cover the health care for these severely disabled veterans. However, the lawyers who split the $9.2 million granted by in attorney fees weren't complaining.

The data theft that occurred in May has served as a monumental "wake up call" to the nation. VA is no longer ignoring IT security. The American Legion is hopeful that this legislation along with the steps VA takes to enhance and enforce its IT security will renew the confidence and trust of veterans who depend on VA for the benefits they have earned. We reiterate the point that funding for the IT overhaul should not be paid for with money from other VA programs. This would in essence make veterans pay for VA's mistakes. The American Legion urges that VA and Congress will not attempt to fix this problem on the backs of America's veterans.
In addition to a fair and expeditious resolution to this breach of security at VA, there should be a complete review of IT security government-wide. VA isn't the only agency within the government that needs to overhaul its IT security protocol. The American Legion urges the President and Congress to review each Federal agency to ensure that the personal information of all Americans is secure.

Mr. Chairman, The American Legion appreciates this opportunity to express its views on this legislation and the issues surrounding it. We look forward to working with you and the members of the committee to make sure comprehensive changes take place in the VA regarding the security of sensitive personal information to the benefit of veterans, active-duty service members, Reservists and their families.

This concludes my testimony.

STATEMENT

of the

MILITARY OFFICERS ASSOCIATION OF AMERICA

on

"THE VETERANS' IDENTITY
AND CREDIT PROTECTION ACT OF 2006" (draft legislation)

before the

HOUSE VETERANS' AFFAIRS COMMITTEE

July 18, 2006

Presented by

Colonel Robert F. Norton, USA (Ret.)
Deputy Director, Government Relations

Mr. CHAIRMAN AND DISTINGUISHED MEMBERS OF THE COMMITTEE, on behalf of the 360,000 members of the Military Officers Association of America (MOAA), I am honored to have this opportunity to present the Association's views on the "Veterans' Identity and Credit Protection Act of 2006" (draft legislation).

MOAA does not receive any grants or contracts from the federal government.

OVERVIEW

MOAA believes the draft "Veterans Identify and Credit Protection Act of 2006" offers positive steps that will serve the interests of our nation's veterans as well as those of the government. We applaud the Committee members for working in a bi-partisan manner to fashion a bill that serves the interests of our nation's veterans.

MOAA supports the establishment of the position of Undersecretary for Information Services in the Department of Veterans Affairs, for two main reasons:

First, it will focus individual responsibility for centralizing and enforcing data security requirements. Second, we hope that establishing this organizational priority will also help advance the objective for the VA and the Department of Defense (DoD) to develop real and timely solutions to long-standing problems of data-sharing between those two departments.

SPECIFIC COMMENTS and RECOMMENDATIONS

Seamless Transition and Servicemember / Veteran Data Security

Entry into military service triggers the collection of personal information on our military men and women that is transmitted at various points of time to the VA. We know from the recent theft of a VA laptop that data on tens of thousands of records of currently serving military personnel were at risk. The establishment of an Under Secretary for Information Security / Chief Information Officer position should include overall responsibility within the VA for the coordination of personnel information reporting between the DoD and the VA.

Despite many years of prodding, consultation, and reports, VA and DoD information management systems still don't really talk to each other. The Report of the President's Task Force on Health Care Collaboration between the DoD and VA (2003) recommended as a priority the development of a single separation physical and bi-directional medical records between the two departments. There have been some improvements that allow viewing between the two departments of certain elements of each others' data, but we're little closer to having a bi-directional electronic medical record or an electronic DD-214 than we were twenty years ago. These "seamless transition" goals must be accomplished in a secure way to protect our veterans' personal information.

The legislation does not address the responsibilities of the new CIO position in regard to coordination of information sharing and reporting between the DoD and the VA. And, clearly, the confidence of the DoD in the VA's information security capability has been damaged.

Presently, the DoD – VA Joint Executive Council includes a Health Executive Council (HEC) and a Benefits Executive Council (BEC) to oversee policy coordination and collaboration between the Departments. ***MOAA recommends the Committee consider incorporating language in the bill that defines the role of the new Under Secretary of Information Security position in the DoD – VA Executive Council.***

Provision of Credit Protection Services and Fraud Resolution Services (Section 5725)

MOAA appreciates the inclusion of specific language in Section 5725, Subsections (g), (h), (i) and (j) that would provide credit reporting and fraud resolution services at the request of a veteran in the event of a data breach "at no cost to the individual."

Education and outreach to veterans and survivors will be extremely important to the successful implementation of Section 5725 of the draft bill.

MOAA recommends that the bill language include a requirement for the VA to develop and promulgate through its Veterans Integrated Service Networks (VISNs) and print / electronic media an explanation of the services that would be provided in the event of a data breach as set forth in the bill.

We also support the provision that would authorize the VA to enter into pre-positioned contracts to protect the interests of current and future veterans who may be subject to financial or other risk through breaches of their personal information.

MOAA would, however, recommend a word change in Section 5725(e) to ensure that veterans would not be charged for receiving services under agreements between the VA and credit reporting agencies: "Any such agreement shall [vice 'may'] include provisions for the Secretary to pay the expenses of such a credit reporting agency for the provision of such services."

Social Security Account Number (SSAN) Access. MOAA supports the Committee's objective to curtail routine use of and access to veterans' SSANs. We believe all government agencies that use the SSAN as a record identifier should begin now to develop alternative identifiers that pose less risk of identity theft. We understand that such an effort may well pose significant challenges. But, if other large bureaucracies such as the state of Virginia can develop alternate identification numbers for state residents to place on their drivers' licenses, federal agencies should strive to offer at least the same level of protection.

Coordination and Integration of the CIO Position within the VA. In MOAA's view it will be extremely important for the Secretary of Veterans' Affairs to ensure that the new CIO position is fully integrated with the VA Health, Benefits, and Memorial Affairs Administrations. The CIO role in some major corporations is to support line operations. However, in today's management environment, the security of data must be a paramount concern of government and private organizations alike. Veterans must have confidence in the ability of the VA to protect their personal information. Building a culture that demands security over personal information will be a key measure of merit for the new CIO.

Conclusion

The Military Officers Association of America greatly appreciates the opportunity to present its views on the Veterans' Identity and Credit Protection Act of 2006.

STATEMENT OF LOUIS IRVIN,

ACTING DEPUTY EXECUTIVE DIRECTOR,

PARALYZED VETERANS OF AMERICA

BEFORE THE HOUSE COMMITTEE ON VETERANS' AFFAIRS

CONCERNING

DRAFT LEGISLATION RELATING TO DATA PROTECTION

AND THE RIGHTS OF VETERANS TO RECEIVE

CREDIT PROTECTION SERVICES

JULY 18, 2006

On behalf of Paralyzed Veterans of America (PVA) I would like to thank you for the opportunity to testify today on the need for data protection and the rights of veterans to receive credit protection services in the event of a data breach containing sensitive personal information from the Department of Veterans Affairs (VA). We are greatly concerned about this major breach of trust that veterans have experienced as a result of the recent theft of their personal data. It is incumbent upon the VA and Congress to ensure that this does not happen again, and to ensure that the interests of veterans are protected.

Chartered by the Congress of the United States
801 Eighteenth Street, NW ★ Washington, DC 20006-3517
phone:(202) 872-1300 ★ tdd:(202) 416-7622 ★ fax:(202) 785-4452 ★ www.pva.org

In light of the events surrounding the theft of 26.5 million veterans' personal information, PVA recognizes the need for reform in the VA information management structure. Although we support many of the principles and provisions contained in the "Veterans Identity and Credit Protection Act," we also have concerns about aspects of the legislation which I will address individually.

PVA generally supports the idea of strengthening the authority that a Chief Information Officer (CIO) would have in the VA. However, we do not believe that the importance of this individual should rise to a level equivalent to the Under Secretaries for Health, Benefits, and the National Cemetery Administration. We would point out that the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA), carry out the mission of the VA by providing health care and benefits to "him who shall have borne the battle and for his widow and his orphan." Information services and systems merely function as a support service to these entities. Information technology is not a mission level program within the Department.

The responsibilities of the CIO are much like those of the Assistant Secretary for Operations, Security, and Preparedness. The Assistant Secretary ensures through his or her department that the life and property of both veterans and VA employees is protected. Personal information is certainly equally important, but it does not necessarily supersede these concerns.

PVA understands the need to centralize certain functions and responsibilities with the CIO; however, we do not believe all of the functions and responsibilities should be consolidated as

outlined in the legislation. We support centralizing the development, approval, and implementation of policies and procedures, including information security, with the CIO. However, we believe that control of the activities and systems that support information services should be retained within VHA, VBA, and NCA. Furthermore, the management of all mission applications, information resources, personnel, and infrastructure should be retained at that level as well. Although the CIO can adequately drive the information systems policy for the entire VA, he or she does not necessarily know what systems and applications work best to actually provide health care or benefits. Information technology is not the mission, it is the tool, and the individuals responsible for the mission should have the authority to manage their tools the best way they see fit.

PVA fully supports the data breach reporting requirements established by this legislation. Rapid disclosure of similar occurrences should help the VA avoid similar embarrassments and allow Congress to take necessary actions to fix this situation, if appropriate.

PVA recognizes the need to put in place credit protection services as outlined in the legislation. It is important that if veterans' personal data is stolen in **the future**, that their credit be protected from criminal behavior. To this end, allowing veterans to receive up to four free credit reports for a year, credit-monitoring services, and identity theft insurance should ease some of their worries. However, it is important to emphasize that the VA must notify veterans immediately if a data breach occurs. It should be done within days, not weeks. The three weeks that it took to notify the public about the most recent data theft is wholly unacceptable.

We would like to address a few concerns with the legislation and offer some advice. Specifically, we do not believe that it is necessary to move forward with credit monitoring and other protections for veterans if it is clearly determined that none of their personal information has been compromised. Furthermore, we do not understand the arbitrary date that was chosen as a retroactive starting point to offer these services. At most, the services should not be offered prior to the theft of the laptop from the VA employee's home in May. Otherwise, there would be no shield for the VA from seemingly frivolous requests for credit protection from veterans who may have experienced identity theft in the past year due to their own or others actions.

We must also emphasize that if the VA is forced to provide these services due to some data breach in the future, that separate funding must be appropriated to provide these services. The VA should not be forced to compromise veterans' health care and benefits by transferring funding away from those accounts to provide credit protection services. In fact, the VA should develop a separate line item in its budget request to support these programs year after year.

PVA also supports the creation of a new unique identification system for veterans who have claims files with the VA. Nearly 20 years ago, the VA assigned veterans file numbers, principally because many veterans did not have a social security number. However, in the late 1980's, the VA began using service members social security numbers as their claims file numbers. We believe that now is the right time to move away from the practice once again. Maintaining veterans' social security numbers for record keeping purposes is just one more threat that could lead to future data theft. If the VA does return to a unique identification system,

it must ensure that those veterans who have claims numbers with the old identification system, prior to the use of social security numbers, receive an entirely new number altogether.

Finally, PVA is concerned that although this legislation would provide protection in the future for veterans and their families affected by data breaches, there are no specific protections provided for active duty service members, National Guardsmen, or Reservists. We should not forget that all of our men and women currently serving in uniform were also affected by this most recent breach. We believe that as this legislation moves forward, the Committee should explore ways to offer the same types of protections to those men and women who are currently serving.

PVA would like to thank you again for the opportunity to testify. We would be happy to answer any questions that you might have.

Statement Of

Larry Madison, Master Sergeant, USAF, (Ret)

Deputy Legislative Director

The Retired Enlisted Association

Before The

House Committee On Veterans' Affairs

July 18, 2006

MR. CHAIRMAN, RANKING MEMBER FILNER, and MEMBERS OF THE COMMITTEE, thank you for this opportunity to provide testimony for the record to the House Committee on Veterans Affairs. This testimony is provided by Larry Madison on behalf of the members of The Retired Enlisted Association.

The Retired Enlisted Association is a Veterans' Service Organization founded 42 years ago to represent the needs and points of view of enlisted men and women who have dedicated their careers to serving in all the branches of the United States Armed Services Active Duty, National Guard and Reserves, as well as the members who are doing so today.

All of us were shocked and alarmed in early May when it was announced that a laptop computer containing the personal data of nearly 29 million Veterans, Active Duty, and Guard and Reserve personnel was stolen. And although we are pleased that the laptop has been recovered and it appears that the data was not accessed, the problems regarding data security at the Department of Veterans Affairs still needs to be corrected.

That's why we are so pleased with the draft legislation to better protect the sensitive personal information of Veterans, Active Duty, and Guard and Reserve personnel that is the focus of the hearing today.

I want to thank Chairman Buyer and all of the Members of the Committee for the collective, non-partisan way in which you have sought to handle this crisis. It was sincerely gratifying to watch the Committee work together in seeking to learn the details of the situation and then coming up with the legislation we are discussing today which will, hopefully, result in greatly increased security for the personal data of millions of veterans that is kept by the Department of Veterans Affairs.

Like many others, we were amazed to learn during the hearings held by this Committee about the warnings from the GAO and the VA's own inspector general and assistant inspector general going back as far as 1997 concerning the weaknesses in the VA's information security systems.

And although we hope this has given the leadership in the department a wake-up call that will result in a serious effort to fix their data security system, we believe the legislation under discussion today is necessary to insure the corrections needed at the VA are accomplished and to help restore the faith of America's veterans in the security of their personal information that is kept by the department.

Under Secretary for Information Services

In particular, we believe the creation of the position of Under Secretary for Information Services

is vital if the task of increasing personal data security in the Department is to succeed. During the testimony given by officials from the Department of Veterans Affairs before this committee it was painfully apparent that there was not a single individual who was in charge and responsible for data security. The change envisioned in this legislation is a positive one that we believe is urgently needed.

Congressional Reporting

In addition, we applaud and strongly support the reporting requirements outlined in the legislation. We believe the annual compliance report to Congress and the monthly reports to the Secretary are urgently needed and they send a signal to the Department about the seriousness with which this Committee and the Congress take this issue.

Provision of Credit Protection Services

We note that the legislation provides for credit protection services for any individual whose personal data held by the VA was breached, at no expense to the individual, if the individual requests one of the credit protection services contained in the bill. We believe this is reasonable way to handle this issue and we support this provision.

Contract with Credit Reporting Agency

We are pleased that the legislation directs the Secretary to enter into an agreement with one or more credit reporting agencies and that this agreement will be in place so that any breaches in the future that place the personal data of Veterans in jeopardy can be quickly and efficiently monitored by that agency if individual veterans request such service.

Use of Social Security Numbers for Identification

The last item we want to mention is the use of Social Security numbers for identification.

As you know, the draft legislation prohibits the use of Social Security numbers on any individual to identify that individual, unless the use of the Social Security number is required by law or the Secretary determiñes that such use is necessary for the identification of an individual.

It is our hope that this is the beginning of process within the federal government of getting away from using an individual's Social Security number as a person's one and only ID. Although we recognize the efficiency of using one number – the Social Security number – as the all-purpose identifier, it is obvious that doing so also increases the efficiency with which a stolen Social Security number can be used to commit identity fraud or other criminal behavior.

Frankly, we are alarmed at the pervasive use of the Social Security number for identification purposes and we believe all Americans would be better off if the use of the Social Security number were severely circumscribed.

We hope this section of the draft legislation will be as carefully monitored as the other aspects of the bill because we can foresee a less than enthusiastic response for this provision from the IT persons within the Department.

While the use of separate ID numbers may be less efficient, we believe veterans will be better served in the long-run because their Social Security numbers will less widely circulated than is the case presently.

Once again, TREA wants to thank the Members of the Committee for the way you have joined together to investigate this most serious situation and for the draft legislation you are proposing. Based on what we have learned, we believe this draft legislation will result in the personal data security that is needed for our veterans.

This concludes my statement and I will be happy to answer any questions you may have.

DRAFT BILL SUMMARY
July 18, 2006

The Veterans Identity and Credit Protection Act of 2006 would:

1. Establishes federal agency data breach notification requirements including provision of enforcement authority to the Chief Information Officer of the Department by amending section 3544(a)(3) of title 44, United States Code (the Federal Information Security Management Act of 2002).
2. Amend title 38, United States Code, to create a new Under Secretary of Information Services for the Department of Veterans Affairs who would also serve as the Chief Information Office for the Department of Veterans Affairs.
3. Create the office of the Under Secretary for Information Security, which would contain three Deputy Under Secretaries:
    a. Deputy Under Secretary for Security, who would also serve as the Senior Information Security Officer of the Department,
    b. Deputy Under Secretary for Operations and Management, and
    c. Deputy Under Secretary for Policy and Planning.
4. Define the responsibilities of the Secretary of Veterans Affairs and the Under Secretary for Information Services under FISMA, which include regular reporting of compliance or noncompliance with FISMA to the Secretary and Congress.
5. Provide Congressional reporting and notification guidelines in the event of a data security breach.
6. Require an independent risk analysis of data breaches following any data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach, and provide notification to affected individuals which would include:
    a. the availability of fraud alerts at the request of the individual, and
    b. the availability of a credit security freeze at the request of the individual.
7. Permit the Secretary to have final determination with respect to the reasonable risk for the potential misuse of sensitive information involved in a data breach based on the risk analysis performed in item 6.
8. In the event of a determination by the Secretary that a reasonable risk exists for the potential misuse of the breached data, allow remediation of identity theft for a veteran or other individual, whose sensitive personal information was compromised due to a data security breach at the Department, through the availability of credit protection services and fraud resolution services upon the request of that individual, which includes;
    a. a definition of the covered individual
    b. notification in writing that the individual's sensitive personal information was part of a security breach,
    c. the availability of services through other government entities
    d. contracting with credit reporting agencies
    e. the availability of a data breach analysis, and
    f. credit monitoring services and identity theft insurance.

9. Require as a condition of contracting with the Department for the processing or maintenance of sensitive personal information, that a contractor not disclose such information to any other person, unless the disclosure is lawful and is expressly permitted under the contract. Should a breach occur by either the contractor or the subcontractor, liquidated damages would be incurred by the contractor. Monies collected from contractors as liquidated damages would be used to provide credit protection services to covered individuals affected by the data breach for which the penalty is paid.
10. Provide for an appropriation of such funds as may be necessary for each fiscal year.
11. Provide conforming technical amendments.
12. Require a report on the feasibility of using personal identification numbers instead of social security numbers for the purpose of identifying individuals whose sensitive personal information is processed or maintained by the Secretary. The report is to be submitted to Congress no later than 180 days after the date of enactment.

[DISCUSSION DRAFT]

109TH CONGRESS
2D SESSION

H. R. _____

To amend title 38, United States Code, to improve information management within the Department of Veterans Affairs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 38, United States Code, to improve information management within the Department of Veterans Affairs, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 **SECTION 1. SHORT TITLE.**
4 This Act may be cited as the "Veterans Identity and
5 Credit Protection Act of 2006".

1 **SEC. 2. FEDERAL AGENCY DATA BREACH NOTIFICATION**
2 **REQUIREMENTS.**
3 (a) AUTHORITY OF DIRECTOR OF OFFICE OF MAN-
4 AGEMENT AND BUDGET TO ESTABLISH DATA BREACH
5 POLICIES.—Section 3543(a) of title 44, United States
6 Code, is amended—
7 (1) by striking "and" at the end of paragraph
8 (7);
9 (2) by striking the period and inserting "; and"
10 at the end of paragraph (8); and
11 (3) by adding at the end the following:
12 "(9) establishing policies, procedures, and
13 standards for agencies to follow in the event of a
14 breach of data security involving the disclosure of
15 sensitive personal information in violation of section
16 552a of title 5, including a requirement for timely
17 notice to be given to those individuals whose sen-
18 sitive personal information could be compromised as
19 a result of such breach, except no notice shall be re-
20 quired if no reasonable risk of identity theft, fraud,
21 or other unlawful conduct exists regarding such indi-
22 vidual.".
23 (b) AUTHORITY OF CHIEF INFORMATION OFFICER
24 TO ENFORCE DATA BREACH POLICIES.—Section
25 3544(a)(3) of title 44, United States Code, is amended
26 by inserting after "authority to ensure compliance with"

1 the following: "and, to the extent determined necessary
2 and explicitly authorized by the head of the agency, to en-
3 force".

4 (c) INCLUSION OF DATA BREACH NOTIFICATION IN
5 AGENCY INFORMATION SECURITY PROGRAMS.—Section
6 3544(b) of title 44, United States Code, is amended—

7 (1) by striking "and" at the end of paragraph
8 (7);

9 (2) by striking the period and inserting "; and"
10 at the end of paragraph (8); and

11 (3) by adding at the end the following:

12 "(9) procedures for notifying individuals whose
13 sensitive personal information is compromised con-
14 sistent with policies, procedures, and standards es-
15 tablished under section 3543(a)(9) of this title.".

16 (d) SENSITIVE PERSONAL INFORMATION DEFINI-
17 TION.—Section 3542(b) of title 44, United States Code,
18 is amended by adding at the end the following new para-
19 graph:

20 "(4) The term 'sensitive personal information'
21 means any information contained in a record, as de-
22 fined in section 552a(4) of title 5.".

1 **SEC. 3. UNDER SECRETARY FOR INFORMATION SERVICES.**

2 (a) UNDER SECRETARY.—Chapter 3 of title 38,
3 United States Code, is amended by inserting after section
4 307 the following new section:

5 **"§ 307A. Under Secretary for Information Services**

6 "(a) UNDER SECRETARY.—There is in the Depart-
7 ment an Under Secretary for Information Services, who
8 is appointed by the President, by and with the advice and
9 consent of the Senate. The Under Secretary shall be the
10 head of the Office of Information Services and shall per-
11 form such functions as the Secretary shall prescribe.

12 "(b) SERVICE AS CHIEF INFORMATION OFFICER.—
13 Notwithstanding any other provision of law, the Under
14 Secretary for Information Services shall serve as the Chief
15 Information Officer of the Department under section 310
16 of this title.".

17 (b) CLERICAL AMENDMENT.—The table of sections
18 at the beginning of such chapter is amended by inserting
19 after the item relating to section 307 the following new
20 item:

"307A. Under Secretary for Information Services.".

21 (c) CONFORMING AMENDMENT.—Section 308(b) of
22 such title is amended by striking paragraph (5) and redes-
23 ignating paragraphs (6) through (11) as paragraphs (5)
24 through (10) respectively.

1 **SEC. 4. DEPARTMENT OF VETERANS AFFAIRS INFORMA-**
2 **TION SECURITY.**
3 (a) INFORMATION SECURITY.—Chapter 57 of title
4 38, United States Code, is amended by adding at the end
5 the following new subchapter:
6 "SUBCHAPTER III—INFORMATION SECURITY
7 **"§ 5721. Definitions**
8 "For the purposes of this subchapter:
9 "(1) The term 'data breach' means the loss,
10 theft, or other unauthorized access to data con-
11 taining sensitive personal information, in electronic
12 or printed form, that results in the potential com-
13 promise of the confidentiality or integrity of the
14 data.
15 "(2) The term 'data breach analysis' means the
16 identification of any misuse of breached sensitive
17 personal information.
18 "(3) The term 'fraud resolution services' means
19 services to assist an individual in the process of re-
20 covering and rehabilitating the credit of the indi-
21 vidual after the individual experiences identity theft.
22 "(4) The term 'identity theft' has the meaning
23 given such term under section 603 of the Consumer
24 Credit Protection Act (15 U.S.C. 1681a).
25 "(5) The term 'identity theft insurance' means
26 any insurance policy that pays benefits for costs, in-

1 cluding travel costs, notary fees, and postage costs,
2 lost wages, and legal fees and expenses associated
3 with the identity theft of the insured individual.
4 "(6) The term 'principal credit reporting agen-
5 cy' means a consumer reporting agency as described
6 in section 603(p) of the Fair Credit Reporting Act.
7 "(7) The term 'sensitive personal information'
8 means the name, address, or telephone number of an
9 individual, in combination with any of the following:
10 "(A) The Social Security number of the in-
11 dividual.
12 "(B) The date of birth of the individual.
13 "(C) Any information not available as part
14 of the public record regarding the individual's
15 military service or health.
16 "(D) Any financial account or other finan-
17 cial information relating to the individual.
18 "(E) The driver's license number of the in-
19 dividual.
20 **"§ 5722. Office of the Under Secretary for Information**
21 **Services**
22 "(a) DEPUTY UNDER SECRETARIES.—The Office of
23 the Under Secretary for Information Services shall consist
24 of the following:

1 "(1) The Deputy Under Secretary for Informa-
2 tion Services for Security, who shall serve as the
3 Senior Information Security Officer of the Depart-
4 ment.
5 "(2) The Deputy Under Secretary for Informa-
6 tion Services for Operations and Management.
7 "(3) The Deputy Under Secretary for Informa-
8 tion Services for Policy and Planning.
9 "(b) APPOINTMENTS.—Appointments under sub-
10 section (a) shall be made by the Secretary.
11 **"§ 5723. Information security management**
12 "(a) RESPONSIBILITIES OF CHIEF INFORMATION OF-
13 FICER.—To support the economical, efficient, and effec-
14 tive execution of subtitle III of chapter 35 of title 44, and
15 policies and plans of the Department, the Secretary shall
16 ensure that the Chief Information Officer of the Depart-
17 ment has the authority and control necessary to develop,
18 approve, implement, integrate, and oversee the policies,
19 procedures, processes, activities, and systems of the De-
20 partment relating to that subtitle, including the manage-
21 ment of all related mission applications, information re-
22 sources, personnel, and infrastructure.
23 "(b) ANNUAL COMPLIANCE REPORT.—Not later than
24 March 1 of each year, the Secretary shall submit to the
25 Committees on Veterans' Affairs of the Senate and House

1 of Representatives, the Committee on Government Reform
2 of the House of Representatives, and the Committee on
3 Homeland Security and Governmental Affairs of the Sen-
4 ate, an annual report on the Department's compliance
5 with subtitle III of chapter 35 of title 44. The information
6 in such report shall be shown for each Administration, of-
7 fice, and facility of the Department.

8 "(c) REPORTS TO SECRETARY.—(1) At least once
9 every month, the Chief Information Officer shall report
10 to the Secretary any deficiency in the compliance with sub-
11 title III of chapter 35 of title 44 of the Department or
12 any Administration, office, or facility of the Department.

13 "(2) The Chief Information Officer shall immediately
14 report to the Secretary any significant deficiency in such
15 compliance.

16 "(d) DATA BREACHES.—(1) The Chief Information
17 Officer shall immediately provide notice of any data
18 breach to the Secretary.

19 "(2) Immediately after receiving notice of a data
20 breach under paragraph (1), the Secretary shall provide
21 notice of such breach to the Director of the Office of Man-
22 agement and Budget, the Inspector General of the Depart-
23 ment, and, if appropriate, the Federal Trade Commission
24 and the United States Secret Service.

1 "(e) BUDGETARY MATTERS.—When the budget for
2 any fiscal year is submitted by the President to Congress
3 under section 1105 of title 31, the Secretary shall submit
4 to Congress a report that identifies amounts requested for
5 Department implementation and remediation of and com-
6 pliance with this subchapter and subtitle III of chapter
7 35 of title 44. The report shall set forth those amounts
8 both for each Administration within the Department and
9 for the Department in the aggregate and shall identify,
10 for each such amount, how that amount is aligned with
11 and supports such implementation and compliance.

12 **"§ 5724. Congressional reporting and notification of**
13 **data breaches**

14 "(a) QUARTERLY REPORTS.—(1) Not later than 30
15 days after the last day of a fiscal quarter, the Secretary
16 shall submit to the Committees on Veterans' Affairs of
17 the Senate and House of Representatives a report on any
18 data breach with respect to sensitive personal information
19 processed or maintained by the Department that occurred
20 during that quarter.

21 "(2) Each report submitted under paragraph (1)
22 shall identify, for each data breach covered by the report,
23 the Administration and facility of the Department where
24 the data breach occurred.

1 "(b) NOTIFICATION OF SIGNIFICANT DATA
2 BREACHES.—(1) In the event of a data breach with re-
3 spect to sensitive personal information processed or main-
4 tained by the Secretary that the Secretary determines is
5 significant, the Secretary shall provide notice of such
6 breach to the Committees on Veterans' Affairs of the Sen-
7 ate and House of Representatives.

8 "(2) Notice under paragraph (1) shall be provided as
9 promptly as possible and without unreasonable delay fol-
10 lowing the discovery of such a data breach and the imple-
11 mentation of any measures necessary to determine the
12 scope of the breach, prevent any further breach or unau-
13 thorized disclosures, and reasonably restore the integrity
14 of the data system.

15 **"§ 5725. Data breaches**

16 "(a) INDEPENDENT RISK ANALYSIS.—(1) In the
17 event of a data breach with respect to sensitive personal
18 information that is processed or maintained by the Sec-
19 retary, the Secretary shall ensure that, as soon as possible
20 after the data breach, a non-Department entity conducts
21 an independent risk analysis of the data breach to deter-
22 mine the level of risk associated with the data breach for
23 the potential misuse of any sensitive personal information
24 involved in the data breach.

1 "(2) If the Secretary determines, based on the find-
2 ings of a risk analysis conducted under paragraph (1),
3 that a reasonable risk exists for the potential misuse of
4 sensitive information involved in a data breach, the Sec-
5 retary shall provide credit protection services in accord-
6 ance with section 5726 of this title.

7 "(b) NOTIFICATION.—(1) In the event of a data
8 breach, the Secretary of Veterans Affairs shall provide to
9 an individual whose sensitive personal information is in-
10 volved in that breach notice in writing that—

11 "(A) describes the circumstances of the data
12 breach and the risk that the breach could lead to
13 misuse, including identity theft, involving the sen-
14 sitive personal information of the individual;

15 "(B) describes the specific types of sensitive
16 personal information that was compromised as a
17 part of the data breach;

18 "(C) describes the actions the Department is
19 taking to remedy the data breach;

20 "(D) the individual may request fraud alerts
21 and credit security freezes under this section;

22 "(E) clearly explains the advantages and dis-
23 advantages to the individual of receiving fraud alerts
24 and credit security freezes under this section; and

1 "(F) includes such other information as the
2 Secretary determines is appropriate.
3 "(2) The notice required under paragraph (1) shall
4 be made as promptly as possible and without unreasonable
5 delay following the discovery of a data breach and the im-
6 plementation of any measures necessary to determine the
7 scope of the breach, prevent any further breach or unau-
8 thorized disclosures, and reasonably restore the integrity
9 of the data system.
10 "(c) REPORT.—For each data breach with respect to
11 sensitive personal information processed or maintained by
12 the Secretary, the Secretary shall promptly submit to the
13 Committees on Veterans' Affairs of the Senate and House
14 of Representatives a report containing the findings of any
15 independent risk analysis conducted under subsection
16 (a)(1), any determination of the Secretary under sub-
17 section (a)(2), and a description of any credit protection
18 services provided under section 5726 of this title.
19 "(d) FINAL DETERMINATION.—Notwithstanding sec-
20 tions 511 and 7104(a) of title 38, United States Code,
21 any determination of the Secretary under subsection
22 (a)(2) with respect to the reasonable risk for the potential
23 misuse of sensitive information involved in a data breach
24 is final and conclusive and may not be reviewed by any

1 other official, administrative body, or court, whether by
2 an action in the nature of mandamus or otherwise.
3 "(e) FRAUD ALERTS.—(1) In the event of a data
4 breach with respect to sensitive personal information that
5 is processed or maintained by the Secretary, the Secretary
6 shall arrange, upon the request of an individual whose sen-
7 sitive personal information is involved in the breach to a
8 principal credit reporting agency with which the Secretary
9 has entered into a contract under section 5726(d) and at
10 no cost to the individual, for the principal credit reporting
11 agency to provide fraud alert services for that individual
12 for a period of not less than one year, beginning on the
13 date of such request, unless the individual requests that
14 such fraud alert be removed before the end of such period,
15 and the agency receives appropriate proof of the identity
16 of the individual for such purpose.
17 "(2) The Secretary shall arrange for each principal
18 credit reporting agency referred to in paragraph (1) to
19 provide any alert requested under such subsection in the
20 file of the individual along with any credit score generated
21 in using that file, for a period of not less than one year,
22 beginning on the date of such request, unless the indi-
23 vidual requests that such fraud alert be removed before
24 the end of such period, and the agency receives appro-

1 priate proof of the identity of the individual for such pur-
2 pose.
3 "(f) CREDIT SECURITY FREEZE.— (1) In the event
4 of a data breach with respect to sensitive personal infor-
5 mation that is processed or maintained by the Secretary,
6 the Secretary shall arrange, upon the request of an indi-
7 vidual whose sensitive personal information is involved in
8 the breach and at no cost to the individual, for each prin-
9 cipal credit reporting agency to apply a security freeze to
10 the file of that individual for a period of not less than
11 one year, beginning on the date of such request, unless
12 the individual requests that such security freeze be re-
13 moved before the end of such period, and the agency re-
14 ceives appropriate proof of the identity of the individual
15 for such purpose.
16 "(2) The Secretary shall arrange for a principal cred-
17 it reporting agency applying a security freeze under para-
18 graph (1)—
19 "(A) to send a written confirmation of the security
20 freeze to the individual within five business days of apply-
21 ing the freeze;
22 "(B) to refer the information regarding the security
23 freeze to other consumer reporting agencies;
24 "(C) to shall provide the individual with a unique per-
25 sonal identification number or password to be used by the

1 individual when providing authorization for the release of
2 the individual's credit for a specific party or period of
3 time; and
4 "(D) upon the request of the individual, to tempo-
5 rarily lift the freeze for a period of time specified by the
6 individual, beginning not later than three business days
7 after the date on which the agency receives the request.
8 **"§ 5726. Provision of credit protection services**
9 "(a) COVERED INDIVIDUAL.—For purposes of this
10 section, a covered individual is an individual whose sen-
11 sitive personal information that is processed or maintained
12 by the Department (or any third-party entity acting on
13 behalf of the Department) is involved, on or after August
14 1, 2005, in a data breach for which the Secretary deter-
15 mines a reasonable risk exists for the potential misuse of
16 sensitive personal information under section 5725(a)(2) of
17 this title.
18 "(b) NOTIFICATION.—(1) In addition to any notice
19 required under subsection 5725(b) of this title, the Sec-
20 retary shall provide to a covered individual notice in writ-
21 ing that—
22 "(A) the individual may request credit protec-
23 tion services under this section;

1 "(B) clearly explains the advantages and dis-
2 advantages to the individual of receiving credit pro-
3 tection services under this section;
4 "(E) includes a notice of which principal credit
5 reporting agency the Secretary has entered into a
6 contract with under subsection (d), and information
7 about requesting services through that agency;
8 "(C) describes actions the individual can or
9 should take to reduce the risk of identity theft; and
10 "(D) includes such other information as the
11 Secretary determines is appropriate.
12 "(2) The notice required under paragraph (1) shall
13 be made as promptly as possible and without unreasonable
14 delay following the discovery of a data breach for which
15 the Secretary determines a reasonable risk exists for the
16 potential misuse of sensitive personal information under
17 section 5725(a)(2) of this title and the implementation of
18 any measures necessary to determine the scope of the
19 breach, prevent any further breach or unauthorized disclo-
20 sures, and reasonably restore the integrity of the data sys-
21 tem.
22 "(3) The Secretary shall ensure that each notification
23 under paragraph (1) includes a form or other means for
24 readily requesting the credit protection services under this

1 section. Such form or other means may include a tele-
2 phone number, email address, or Internet website address.
3 "(c) AVAILABILITY OF SERVICES THROUGH OTHER
4 GOVERNMENT AGENCIES.—If a service required to be pro-
5 vided under this section is available to a covered individual
6 through another department or agency of the Government,
7 the Secretary and the head of that department or agency
8 may enter into an agreement under which the head of that
9 department or agency agrees to provide that service to the
10 covered individual.
11 "(d) CONTRACT WITH CREDIT REPORTING AGEN-
12 CY.—Notwithstanding any other provision of law, the Sec-
13 retary shall enter into contracts or other agreements as
14 necessary with one or more principal credit reporting
15 agencies in order to ensure, in advance, the provision of
16 credit protection services under this section. Any such con-
17 tract or agreement may include provisions for the Sec-
18 retary to pay the expenses of such a credit reporting agen-
19 cy for the provision of such services.
20 "(e) DATA BREACH ANALYSIS.—The Secretary shall
21 arrange, upon the request of a covered individual and at
22 no cost to the individual, to provide data breach analysis
23 for the individual for a period of not less than one year,
24 beginning on the date of such request.

1 "(f) PROVISION OF CREDIT MONITORING SERVICES
2 AND IDENTITY THEFT INSURANCE.—During the one-year
3 period beginning on the date on which the Secretary noti-
4 fies a covered individual that the individual's sensitive per-
5 sonal information is involved in a data breach, the Sec-
6 retary shall arrange, upon the request of the individual
7 and without charge to the individual, for the provision of
8 credit monitoring services to the individual. Credit moni-
9 toring services under this subsection shall include each of
10 the following:
11 "(1) One copy of the credit report of the indi-
12 vidual every three months.
13 "(2) Fraud resolution services for the indi-
14 vidual.
15 "(3) Identity theft insurance in a coverage
16 amount that does not exceed $30,000 in aggregate
17 liability for the insured.
18 **"§ 5727. Contracts for data processing or mainte-**
19 **nance**
20 "(a) CONTRACT REQUIREMENTS.—If the Secretary
21 enters into a contract for the performance of any Depart-
22 ment function that requires access to sensitive personal
23 information, the Secretary shall require as a condition of
24 the contract that—

1 "(1) the contractor shall not, directly or
2 through an affiliate of the contractor, disclose such
3 information to any other person unless the disclo-
4 sure is lawful and is expressly permitted under the
5 contract;
6 "(2) the contractor, or any subcontractor for a
7 subcontract of the contract, shall promptly notify the
8 Secretary of any data breach that occurs with re-
9 spect to such information.
10 "(b) LIQUIDATED DAMAGES.—Each contract subject
11 to the requirements of subsection (a) shall provide for liq-
12 uidated damages to be paid by the contractor to the Sec-
13 retary in the event of a data breach with respect to any
14 sensitive personal information processed or maintained by
15 the contractor or any subcontractor under that contract.
16 "(c) PROVISION OF CREDIT PROTECTION SERV-
17 ICES.—Any amount collected by the Secretary under sub-
18 section (b) shall be deposited in or credited to the Depart-
19 ment account from which the contractor was paid and
20 shall remain available for obligation without fiscal year
21 limitation exclusively for the purpose of providing credit
22 protection services in accordance with section 5726 of this
23 title.

1 **"§ 5728. Authorization of appropriations**

2 "There are authorized to be appropriated to carry out
3 this subchapter such sums as may be necessary for each
4 fiscal year.".

5 (b) CLERICAL AMENDMENT.—The table of sections
6 at the beginning of such chapter is amended by adding
7 at the end the following new items:

"SUBCHAPTER III—INFORMATION SECURITY

"5721.Definitions.
"5722.Office of the Under Secretary for Information Services.
"5723.Information security management.
"5724.Congressional reporting and notification of data breaches.
"5725. Data breaches.
"5726.Provision of credit protection services.
"5727.Contracts for data processing or maintenance.
"5728.Authorization of appropriations.

8 (c) DEADLINE FOR REGULATIONS.—Not later than
9 60 days after the date of the enactment of this Act, the
10 Secretary of Veterans Affairs shall publish regulations to
11 carry out subchapter III of chapter 57 of title 38, United
12 States Code, as added by subsection (a).

13 **SEC. 5. REPORT ON FEASIBILITY OF USING PERSONAL**
14 **IDENTIFICATION NUMBERS FOR IDENTIFICA-**
15 **TION.**

16 Not later than 180 days after the date of the enact-
17 ment of this Act, the Secretary of Veterans Affairs shall
18 submit to Congress a report containing the assessment of
19 the Secretary with respect to the feasibility of using per-
20 sonal identification numbers instead of social security

1 numbers for the purpose of identifying individuals whose
2 sensitive personal information (as that term is defined in
3 section 5721 of title 38, United States Code, as added by
4 section 4) is processed or maintained by the Secretary.