ACADEMIC AND LEGAL IMPLICATIONS OF VA'S DATA LOSS

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 22, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109–56

U.S. GOVERNMENT PRINTING OFFICE

28–452 WASHINGTON : 2007

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

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, Indiana, *Chairman*

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

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

JAMES M. LARIVIERE, *Staff Director*

CONTENTS

June 22, 2006

	Page
Academic and Legal Implications of VA's Data Loss	1

OPENING STATEMENTS

Chairman Steve Buyer	1
Prepared statement of Chairman Buyer	50
Hon. Bob Filner, a Representative in Congress from the State of California	3
Hon. Ginny Brown-Waite, a Representative in Congress from the State of Florida, prepared statement of	55
Hon. Corrine Brown, a Representative in Congress from the State of Florida, prepared statement of	57
Hon. Sylvestre Reyes, a Representative in Congress from the State of Texas, prepared statement of	61
Hon. Stephanie Herseth, a Representative in Congress from the State of South Dakota, prepared statement of	63
Hon. Tom Udall, a Representative in Congress from the State of New Mexico, prepared statement of	65

WITNESSES

Brody, Bruce A., Vice President, Information Security, INPUT, Reston, VA, and former Associate Deputy Assistant Secretary for Cyber and Information Security, U.S. Department of Veterans Affairs	7
Prepared statement of Mr. Brody	76
Cook, Mike, Co-Founder, ID Analytics, San Diego, CA	11
Prepared statement of Mr. Cook	85
McClain, Hon. Tim S., General Counsel, U.S. Department of Veterans Affairs	29
Prepared statement of Mr. McClain	92
Spafford, Eugene H., Ph.D., Professor and Executive Director, Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), West Lafayette, IN; Chair, U.S. Public Policy Committee, Association for Computer Machinery (USACM); and Member, Board of Directors, Computing Research Association (CRA)	5
Prepared statement of Dr. Spafford	67

MATERIAL SUBIMTTED FOR THE RECORD

Statements:	
Kappelman, Leon A., Ph.D., Professor of Information Systems, Director Emeritus, Information Systems Research, Fellow, Texas Center for Digital Knowledge; Associate Director, Center for Quality and Productivity, Information Technology and Decision Sciences Department, College of Business Administration, University of North Texas..	110
Post-hearing written Committee questions and the responses:	
Chairman Buyer to U.S. Department of Veterans Affairs	111

Page

Post-hearing written Committee questions and the responses—Continued
Chairman Buyer to Mr. Bruce A. Brody (INPUT) 118
Chairman Buyer to Mr. Mike Cook (ID Analytics) 121

THE ACADEMIC AND LEGAL IMPLICATIONS OF THE VA'S DATA LOSS

THURSDAY, JUNE 22, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS AFFAIRS,
Washington, DC.

The Committee met, pursuant to call, at 10:35 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [Chairman of the Committee] presiding.

Present: Representatives Buyer, Bilirakis, Moran, Brown of South Carolina, Miller, Brown-Waite, Filner, Snyder, Michaud, Herseth, Strickland, Reyes, Berkley, Udall, Salazar.

The CHAIRMAN. The full Committee of the House will come to order, June 22nd, 2006.

Good morning, ladies and gentlemen. We are here today to receive testimony on best practices from experts in the field of information security and data breaches. We will also hear from the Department of Veterans Affairs' General Counsel about the legal implication of the VA's information security breach and data loss.

This hearing is part of a series that will help us determine how to understand the scope of the problems, so we can then proceed to assist in the correction of these concerns of the department. We are systematically examining key aspects of the security breach, and reviewing best practices, and thinking in the realm of information security.

Last week, we heard testimony from the VA inspector general and from the Government Accounting Office, who provided historical context. The context is a sobering. Even as far back as 1997 the GAO had begun to examine these problems, and then in 2002, they recommended the VA centralize its IT security management functions and establish an information security program. The VA's own inspector general has gone on the record with a similar litany of warnings that have been largely if not completely ignored. The VA's assistant inspector general for audit told us the IG has reported VA information security controls as a material weakness in its annual consolidated financial statements, since fiscal year 1997 audit.

VA's IT Information Security Management Act audits have identified significant information security vulnerabilities since fiscal year 2001. A reasonable person might ask what the VA is waiting for. The IG and GAO, our investigations have shown, are not alone in their support for centralized IT management. On June 8th, I held a roundtable discussion with information technology experts

from business, including Goldman Sachs, EMC Corporation, Visa, Citigroup, Tri-West, and American Bankers Association. At my invitation attending also was the chairman of the military quality of life and veterans' appropriations Subcommittee, Jim Walsh.

These experts offered candid appraisals, and emphasized the importance of centralized information security management. None from a good business sense could endorse the VA's approach, the federated model, which still shows a significant degree of decentralization. One of the experts said, quote, "I see the federated approach as an excuse for lack of controls."

As part of our approach, the Subcommittee on disability assistance and memorial affairs held a hearing on Tuesday, on information security at the Veterans' Benefits Administration. Yesterday, the Subcommittee on health examined how the Veterans' Health Administration maintains security and integrity with electronic health records of patients. Both systems face challenges. We are aware of problems with the Benefits Administration. The VA IG has testified at VHA, tens of thousands of VA's health records have been sent by unencrypted e-mail, and were made vulnerable to interception. Problems with uncontrolled access to data, password protection, and even a failure to terminate access for long-departed employees, made the conditions for additional disasters. The more we learn about the awful results of decentralization, in contrast to the bright promises offered by some VA officials, the more we see the system has no departmental standards. And more important, the system, if you call it that, does not identify who is in charge of developing policy, implementing policy, or enforcing policy.

It does not have to be this way. Today, experts from the academic world will also provide insights into the cutting edge information security theories and concepts. The recent passing of management expert, Professor Peter Drucker, reminds us that not all expertise is to be found in the world of practice. We have much to learn from those who earn their pay strictly from the work in their minds.

We will then turn to the department's General Counsel, the Honorable Tim McClain, who will provide testimony regarding the legal implications of VA's data breach. I will also be interested in learning more about the legal review process for VA's information security directive for the past three years. Also, I want to learn more about the adequacy of the VA's legal authority to provide credit counseling and compensation to veterans affected by the loss of their personal information.

Next week, completing a series of hearings, the full Committee will receive testimony from former VA chief information officers. And finally, we will hear from Secretary of Veterans' Affairs Nicholson, and the department's senior leadership, with an update on the progress being made in the department. So please be sure to note these important dates on your schedule.

This weekend, we learned that a laptop stolen from a contractor working for the city of Washington DC, compromised sensitive information on thousands of city employees. While we are now seeing that data security has broad implications across the country and across government, what we would like to see is VA moving from worst disaster to best practice.

We look forward to your testimony. I recognize the Ranking Member for any comments that he might have. Mr. Filner.

[The statement of Chairman Buyer appears on p. 50.]

Mr. FILNER. Thank you, Mr. Chairman, and as we said last week, thank you for embarking on this series of oversight hearings. I don't think it's any accident that the VA announced finally some proactive measures yesterday. I think it's the calendar that you have outlined, reporting will have to be done, that has sparked some activities. I think this is the way that we, Congress, must proceed in terms of oversight, so I thank you so much.

As you have pointed out, we have to figure out what happened, how it happened, how to prevent it, who was responsible, and of course, what can be done in the future. As Chairman Buyer has pointed out, on many occasions, we have heard that long-standing problems in cyber and information security went uncorrected at the VA for unconscionably long times. We have heard testimony before this Committee that the problem lies within the VA's culture of resistance to change, including being impervious to change in, of all arenas, information security. One written statement at a previous hearing offered a rationale for the resistance of VA, a desire to avoid accountability.

Mr. Chairman, last week you and Dr. Snyder both noted apparent problems and conflict with the General Counsel opinions in 2003 and 2004. The net effect of these opinions, and we will hear what the General Counsel says, was to create confusion at VA regarding aspects of enforcement authority for information security. How could this happen if the Federal Information Security Management Act of 2002 was created just to resolve these very problems? And we have seen evidence of the difficulty of implementing change in the IT culture at VA.

For me, as for you, Mr. Buyer, the most illustrative example of that resistance was Secretary Principi's failed directive to centralize control of the IT under the chief information officer. His was the right solution, but it never happened. When the edicts of the Secretary and his team are ignored by the agency, it is time for the Secretary to clean house. In this case, I and a number of my colleagues will be pleased to help move that process along.

All too often, we hear about policy changes at VA that are in the works, or we hear about half solutions and changes that are just around the corner. Problems were raised about the HR links program, but substantive solutions were never implemented. HR links was a good idea, but leadership was needed, and there was none. The result: about a third of a billion-dollar loss to taxpayers.

VETSNET will automate critical functions associated with the compensation and ratings awards, if it is ever fully implemented. But I note that the future tense is always used to address hopeful solutions to VETSNET, for over a decade, now.

The core FLS is another example of a major information technology failure in the multi-hundred million dollars loss range, and the root cause I think is evident: mismanagement at the top.

We must move the entrenched culture inside the agency to conform to what is best for the entire agency and for veterans. That is why we are here. At a minimum, as is often suggested by the

Inspector General, implementation of a robust and standardized policy would be helpful. That has yet to happen.

At our last full Committee hearing, Mr. Michaud referred to a threat by an offshore-based subcontractor to post medical information about 30,000 veterans on the Internet. Yet, when Committee staff asked about the off-shoring of medical transcript and services in previous years, they were told that there was no evidence of such activity. The IG now seems to have found ample evidence in a report released last week.

This indirection and indifference by the Veterans' Administration regarding its protection of sensitive information must halt. We need to have straight shooting with Congress and with the American people.

Finally, Mr. Chairman, the magnitude of the loss of the 26 million records, plus apparently hundreds of thousands of others, is breathtaking. It looks like we are moving in a proactive way, although we have yet to see what contractor will win the contract. I hope we don't give the contract to Halliburton. In fact, one of the companies that is here today has offered the public service of doing it for very little, if any, cost to taxpayers.

So we must assure that any promises we make to fix the problem can actually be kept. We must set expectations for veterans that can be delivered, and have the willpower to keep those promises. Let us keep the faith with our veterans. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Our first panel includes Dr. Eugene Spafford, Ph.D., who is a professor of computer science and is Executive Director for the Center of Education and Research in Information Assurance and Security, at Purdue University. Next, we have Mr. Bruce Brody, Vice President of Information Security for INPUT, and former Associate Deputy Assistant Secretary for Cyber and Information Security with U.S. Department of Veterans Affairs. And finally, we have Mike Cook, Vice President of ID Analytics.

Dr. Spafford, personally I want to thank you for—often, the Federal government has turned to you for your Council. We did in the mid–1990s, with the DOD. You assisted the Department of Air Force, you have helped out with the FBI, we have turned to your expertise in regard to NSA, and once again we are now turning to you, and you don't hesitate. And so there is something inside that says, "Yes, I have knowledge, I have some expertise, and I am willing to help my country." And you have been there, and you have also served on the president/s advisory. I welcome all the members—how many of these do you have, or can you gain access to?

Dr. SPAFFORD. I believe we have about 50 or 70 of them out there.

The CHAIRMAN. You have about 50 or 70 of them out there? You are only here by yourself? You have somebody with you, staff?

Dr. SPAFFORD. There is somebody here, yes.

The CHAIRMAN. Well, somebody go out there and get one of these to Tim McClain for me right now, while he can flip through this. Tim, have you seen this before?

Mr. MCCLAIN. No, sir, I haven't.

The CHAIRMAN. It is very interesting. If you would grab that box, I want to make sure everybody, all of my colleagues have this.

Look how it is titled: "Cyber Security, a Crisis of Prioritization." The president put these experts together.

[The report is being retained in the Committee files and can be found on the internet at: http://www.nitrd.gov/pitac/reports/20050301__cybersecurity/cybersecurity.pdf.]

Dr. Spafford, you are recognized.

STATEMENTS OF EUGENE H. SPAFFORD, PH.D., PROFESSOR AND EXECUTIVE DIRECTOR, CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY, PURDUE UNIVERSITY, WEST LAFAYETTE, IN, CHAIR, U.S. PUBLIC POLICY COMMITTEE, ASSOCIATION FOR COMPUTING MACHINERY, AND MEMBER, BOARD OF DIRECTORS, COMPUTING RESEARCH ASSSOCIATION; MR. BRUCE A. BRODY, VICE PRESIDENT, INFORMATION SECURITY, INPUT, RESTON, VA, AND FORMER ASSOCIATE DEPUTY ASSISTANT SECRETARY FOR CYBER AND INFORMATION SECURITY, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND MR. MIKE COOK, CO-FOUNDER, ID ANALYTICS, SAN DIEGO, CA

STATEMENT OF EUGENE SPAFFORD

Dr. SPAFFORD. Thank you, Chairman Buyer and Members of the Committee. It is my pleasure to be here to attempt to help in this case. We are here because of the significant breach of security and privacy at the Veterans' Administration. That incident has obviously exposed many people to increased risk of identity theft, credit fraud, and other kinds of criminal activities. I would like to point out, however, that it is more than a financial impact that is potentially there. In addition, some of our active-duty personnel and veterans may find themselves denied security clearances, or find their names added to the TSA's no-fly list, because somebody else has misused their identity. And if you have ended up on the no-fly list and tried to get off, you know how difficult that is. And they may also have to criminal warrants or civil actions because others have committed crimes in their name.

This problem is not unique to the Veterans' Administration, however. A recent article in "Computer World" noted that since the start of 2005, there have been nearly 200 similar incidents, resulting in significant disclosure of personal information, with nearly 90 of those incidents occurring since the beginning of this year. The total number of records disclosed by all of these incidents to date is 88 million. What is more, those are only the detected and reported incidents. The actual number is certainly much larger.

For decades, professionals in the field of information security have been warning about the dangers of weak security, careless handling of data, lax enforcement policies, and insufficient funding for both law enforcement and research. This is similar to what you have been hearing from the Inspector General of the Veterans' Administration. Our warnings and cautions have largely been dismissed, however, as unfounded or too expensive to address. Unfortunately, we are now seeing the results of that lack of attention with incidents such as what happened at the VA.

In addition, we have seen new levels of sophisticated computer viruses and spyware emerging, increasing cyber activity by orga-

nized crime around the world, and significant failures of security across a wide variety of public sector entities and government agencies. In the brief time that I have for my verbal remarks, I want to make special note of one particular failure present in this case that you have already identified. There is no centralized position that has all of the three components that are necessary to effectively manage information security: resources, accountability, and authority.

There should be either the CIO or CISO, Chief Information Security Officer, who has adequate funding and trained personnel to carry out a comprehensive security plan. That office, and the management above it, must be held accountable for failures to satisfy necessary standards, and successfully pass audits.

Last of all, that same office must have authority to make changes, shut down systems if necessary, and sanction employees for cause. There are other information security problems at the VA and elsewhere in the government which were not directly involved in the May disclosure incident, but could prove problematic later. It is beyond the scope of this testimony to describe all of them. It is also beyond the scope of this testimony to summarize the magnitude of cyber threats currently facing our information infrastructure, including the Veterans' Administration. There are a number of reports describing these threats, and I can summarize simply by saying the situation is poor, and getting worse. Regrettably, I believe the situation is going to get worse because the problems have been ignored and neglected for too long to be quickly remedied.

As a member of academia, I wanted to say that we can offer few immediate solutions. Although we have several good programs at many colleges and universities across the United States, we are producing too small a number of students to meet the demand. Exacerbating this is a lack of resources. Outside of a few underfunded programs through the National Science Foundation that award competitive grants to faculty, and a few congressionally directed allocations to a few university projects around the country, there is almost no funding for basic research, capacity development, or infrastructure acquisition, for the programs working in information security. As an example, the center I direct at Purdue University, CERIAS, is the nation's leading center in multidisciplinary information security research and education, with over 80 faculty, and we are graduating nearly 25 percent of the nation's Ph.D.'s in information security. CERIAS, in its nine- year lifetime, has never received any government support, although some individual faculty receive funding from agencies such as the NSF for individual research.

As is the case with many of my peer institutions, our ability to make progress in education and research is limited by a severe lack of resources. In February, 2005, as Chairman Buyer noted, the President's Information Technology Advisory Committee issued this report, based on hearings and considerable study by many experts, myself included. That report was entitled "Cyber Security, a Crisis of Prioritization." It described the nature of the problems with cyber security, and some of the trends. It also analyzed the inadequate Federal response to those challenges. It outlined in some detail an agenda to begin to address some of our cyber security prob-

lems. The response to that report was similar to other reports that have been issued over the years. Only one of the four recommendations has been acted upon, and PITAC was disbanded.

I encourage members of the Committee to carefully read the PITAC cyber security crisis report. I participated in the research and writing of that document, and it goes into considerable detail about problems such as those faced at the VA, and issues behind our cyber security deficit, as well as making some concrete suggestions on how those issues might be addressed. I have also included some other recommendations in my written testimony, including a comprehensive list of recommendations for data privacy protection, as developed by the ACM's U.S. public policy Committee.

I welcome your questions and working with you to help address these problems. Thank you.

[The statement of Dr. Spafford appears on p. 67.]

The CHAIRMAN. Thank you very much. Did all the members receive one of these? Everybody has got one? All right, thank you.

Mr. Brody, you are now recognized.

Mr. BRODY. Mr. Chairman, Representative Filner, and members of the Committee, my name is Bruce Brody. As a veteran, I am very grateful for the opportunity to address this distinguished Committee today. With the Chair's permission, I will provide a brief overview, and then submit a longer statement for the record.

The CHAIRMAN. Hearing no objection, so ordered. Dr. Spafford, did you have a written statement that you would like to be submitted for the record?

Dr. SPAFFORD. He has it.

The CHAIRMAN. Mr. Cook, do you have a written statement you would like submitted for the record? All right. Hearing no objection, so ordered. All the statements will be submitted for the record.

STATEMENT OF BRUCE BRODY

Mr. BRODY. I am the Vice President for Information Security at INPUT, a market research firm based in Reston, Virginia. From 2001 to 2004, I was the Associate Deputy Assistant Secretary for Cyber and Information Security at the Department of Veterans Affairs. And from 2004 until January of this year, I was the associate chief information officer for cyber security at the Department of Energy. I believe that I am the only person ever to have served as the chief information security officer at two Cabinet-level departments.

Like the members of this Committee and my fellow veterans, I view the loss of personal information of more than 26 million veterans as willful disregard for responsible behavior, and blatant contempt for established Federal security and privacy requirements by senior VA leadership. I urge this Committee to look very carefully at the following factors, which I believe contributed to the decades of information security and privacy neglect at the VA, that have been documented by the Inspector General and the Government Accountability Office.

First, someone with appropriate substantive expertise must be empowered to set and enforce privacy and cyber security requirements, which will include the physical security requirements for

how such records are maintained, and the personal security requirements for who is allowed access to such records. When I was first introduced to this Committee in April of 2001, I thought that the Secretary had hired me for that purpose. However, the apparent authorities invested in the CIO under the Clinger Cohen Act, and the Paperwork Reduction Act, and both the CIO and the CISO in the Computer Security Act of 1987, the Government Information Security Reform Act of 2000, and finally, in the Federal Information Security Management Act of 2002, were not accepted by VA's leadership. I quickly learned that the department's chief information officer only had authority to advise, encourage, support, and persuade the administrations, insofar as information technology programs were concerned.

In addition, I learned that the CIO had no authority to direct compliance. These points were captured in a memorandum from the assistant General Counsel dated October 6, 2000. Difficulties with this advise, encourage, support, and persuade approach to the CIO's management authority were raised at a March 12th, 2002, oversight Committee hearing by both Chairman Buyer and Ranking Member Carson, questioning the ability of the then-CIO to get the job done without line authority.

Later that year, Secretary Principi took actions to direct the centralization, and enhance line authority of the CIO function, presumably acting on the recommendations of this Committee. But unfortunately, the Secretary's direction met with bureaucratic inertia and cultural resistance, and was never fully implemented.

Subsequent to my arrival at the VA, the Government Information Security Reform Act, followed by the Federal Information Security Management Act, were enacted in 2000 and 2002, respectively. Not being an attorney, I cannot offer legal opinions about what the words of these statutes mean. I can only apply common sense to the purpose of these important pieces of legislation. It seemed to me that after all was said and done, and the opinion of the assistant General Counsel issued in October 2000 was correct, then the Congress went through nonsensical amounts of effort to produce the legislation and provide such detail concerning specific responsibilities. It became all the more apparent that clarification was needed, following the MS Blaster malicious software incident in the second half of 2003.

In advance of what proved to be a serious malicious software attack represented by MS Blaster, my office provided the necessary alerts, and also distributed notification concerning the necessary patches, throughout the VA enterprise. These alerts were widely ignored, and VA networks were savaged as a result. The apparent authorities invested in the CIO in the Clinger Cohen Act, and in the CIO and CISO in FISMA, did not seem to be accepted by VA or its leadership.

As a result, I concluded that there was no longer any point in attempting to introduce cyber security changes in the VA unless there was a clear statement of authority to do so. That was when I requested the General Counsel opinion about FISMA authorities for the CIO and the CISO.

Just prior to the MS Blaster attack, I had requested a clarification from the General Counsel concerning the responsibilities of the

CIO under FISMA for national security and non-national security information and information systems. In a memorandum signed by the General Counsel, dated August 1st, 2003, it was reinforced that the various security functions of the department, specifically information security, physical security, and personnel security, would remain under the authority of their respective offices. According to the memorandum, the CIO was allowed to issue policies pertaining to information security, but the daily operations of security clearance determinations, investigations, physical storage, and related activities wouldn't be placed under the purview of the CIO.

Subsequent to the MS Blaster attack, I requested a clarification from the General Counsel concerning the authority of the CIO to enforce compliance with security legislation and relations. In a memorandum signed by the General Counsel on April 7th, 2004, it was asserted that the CIO cannot order or enforce compliance with information security requirements. Because FISMA used the word "ensure," instead of the word "enforce," the General Counsel stated that the only recourse for the CIO when a security requirement was violated was to complain to the Secretary.

The result of these two opinions was extremely unfortunate for the department. In effect, the first of these memos fragmented security authorities, and the second said that the CIO had no authority to enforce policies or to hold people accountable for violating policies. These memos accurately captured and reinforced the culture of the department, where resistance to central authority, and doing business according to hundreds of different local practices, have always been the norm.

In day-to-day operations, these memos ensured that the fragmentation of security authorities enabled the lack of background investigation for individuals with access to VA networks, systems, resources; the unchecked access to VA information by foreign corporations and foreign nationals, limited to nonexistent logical and physical access controls for major medical systems; the disruption and denial of service from malicious software attacks such as MS Blaster, and hundreds of other negative information security findings, as highlighted in the reports of the independent public auditor, the Inspector General, and the government accountability office.

I would ask the Committee if it agrees that the Clinger Cohen Act and FISMA do not require a Secretary, CIO, and CISO, to set and enforce the security requirements of the FISMA legislation? If FISMA and the Clinger Cohen Act did not convey the authority and accountability for enforcing security and privacy requirements, perhaps the Congress needs to amend these bills to so state. My personal experience is that the mismatch of authority and accountability from the CIO and CISO affect other departments, agencies, to the same extent as affects the VA. And I encourage legislative action to clarify this situation and possibly prevent more serious incidents from occurring.

But the bottom line for the VA was that the two General Counsel memos reinforced the VA culture. And the VA culture is the root cause of this problem. The VA culture can be highlighted even further in the paper trail of nonconcurrences on VA directive 6500, the information security program.

My second recommendation is that policies, procedures, and assignments of accountability regarding security, and privacy issues, cannot be held hostage to the individual interests of the senior officials whose concurrence must be obtained prior to review by the Secretary. In this regard, I invite the Committee's attention to the paper trail of nonconcurrence on VA directive 6500, the information security program.

On January 16th, 2004, VHA non-concurred on VA directive 6500, disagreeing with a blanket approach to background investigations, opposing any requirement to ensure that corporations having access to VA systems and data be American-owned—in other words, subject to U.S. policy, and within the reach of U.S. courts, if U.S. laws are breached.

VHA also opposed any requirements that visitor personnel be escorted at VA facilities, and resisted the ability of the associate deputy assistant Secretary for cyber and information security to establish mandatory penalties for noncompliance.

VHA's nonconcurrence specifically dealt with the offshoring of sensitive information, such as medical records or transcriptions. Other significant nonconcurrences on VA directive 6500 are included in my written testimony for the record.

The memos by the General Counsel and paper trail of nonconcurrence on VA directive 6500 are indicative of a culture of resistance to central authority, and refusal to accept anything other than business as usual. They also highlight the decentralized authority enjoyed by the administrations and program offices, who are empowered to define the role and authority of the CIO as they see fit in order to perpetuate their parochial interests.

Most of all, these documents make it clear that the CIO and the subordinate CISO have no authority to do anything other than to issue policies. Now on top of that, they can only issue policies that the administrations and program offices allow them to issue through the concurrence process. Once issued, the CIO and CISO have no authority to enforce these watered-down policies that they are permitted to put in place.

As a third recommendation, let me suggest to you that the CIO budget, including cyber security and privacy budgets, cannot be held hostage by the administrations and program offices. Since funds are not directly appropriated to the CIO by Congress, security and privacy initiatives depend on the funding support of the very offices that have historically been the cause of the problems being addressed.

Fourth, I recommend you create a legislative requirement that would suspend all executive and senior bonuses in the VA until the environment for which the executive is responsible receives a clean bill of security health from the IG and the competent senior official placed in charge of security. There are more than 26 million veterans and active duty personnel who are uncertain that the loss of their personal information will bring them financial harm. These veterans deserve better, because they have served our country well. Unfortunately, the VA has not served them well, and the VA must make necessary amends. If the VA cannot reinvent itself and change its culture dramatically, then I would beg the Congress to do it for them, and to do it for our Nation's deserving veterans.

Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear here.

[The statement of Mr. Brody appears on p. 76.]

The CHAIRMAN. Thank you, Mr. Brody. Mr. Cook, you are now recognized.

STATEMENT OF MIKE COOK

Mr. COOK. Chairman Buyer, Representative Filner, and esteemed members of the Committee, thank you for inviting ID Analytics to testify——

The CHAIRMAN. Mr. Cook, can you turn that microphone on, and pull it close to you, please? Thank you.

Mr. COOK. It wasn't on, I apologize. Thank you for inviting ID Analytics to testify on ways to help victims of the recent Veterans' Affairs data breach. My name is Mike Cook. I am a cofounder of ID Analytics, a San Diego-based company focused exclusively on stock and identity fraud. I have worked in the field of credit risk and fraud prevention for 20 years. ID analytics helps stop identity fraud through our identity network, a real-time identity fraud prevention system formed through a consortium of leading companies dedicated to protecting their customers from identity fraud.

Our ID network gathers information from applications for credit, change of address, and other identity risk information from companies, including half the top 10 U.S. banks, almost all major wireless carriers, and a leading retail card issuer. Hundreds of times each day our technology helps stop fraudsters from obtaining credit services and merchandise in innocent consumers' names.

We think it's important to make you aware that ID analytics does not market or sell the data we collect in the ID network for any purpose, to anyone.

I am here today because ID analytics has unique expertise and knowledge of data breaches and their risk. Today, we are the only public or private entity that has studied the harm resulting from actual data breaches. Should any Committee member have interest, I would be happy to provide a copy of our white paper analyzing the harm from four actual well-publicized data breaches involving more than 500,000 breached consumer identities.

I would first like to put this breach into context. At this point, no one knows the scope of risk the veterans are facing. The most dangerous data breaches are targeted thefts, where the thief committed the breach solely for the purpose of taking the consumer data. In this case, the purpose of the theft is unclear. Was the thief targeting a laptop, or the data held on it? I don't believe we know that answer today.

If the data is misused, we can expect it to be misused in the following ways: its likely fraudsters will mainly attack the credit card industry. Stolen identities are an asset that sophisticated fraudsters can get the best rate of return by fraudulently obtaining credit cards, and then making fenceable purchases. Secondly, because the file contains so many identities, it is likely that the fraudsters will use the stolen identities once or twice and never again, to increase their approval rate. Low use rates of individual veteran identities will make detection more difficult for the lending community. Again, if the data is misused, sophisticated fraudsters

will spread the misuse of identities across differing locations within a city, or even across different States, to avoid detection.

The worst-case scenario is that the veteran file finds its way to a public distribution source, such as the Internet. If this happens, stolen identities will lose their connection to the VA data breach, and groups of fraudsters might actively trade that data among the broad community. Subsequently, more people might have access, and could misuse those identities on a grander scale. We know from additional research conducted earlier this year, the misuse rate of data traded on the Internet can climb substantially and exceed the average rate of identity theft of 1.5 percent.

Some consumer advocates estimate the value of the stolen identity ranges from $25–$75, depending upon the available personal information associated with that identity. So because of the value of the data itself, wide distribution should be a concern, and should drive a real sense of urgency to try to recover the stolen data as fast as possible.

So what can the VA do now? Over the course of the last year, ID Analytics has developed breach monitoring technology. With this technology, the VA can answer three essential questions about the data breach. The first question the VA can answer is, is the breached data being misused by fraudsters today? Secondly, if it is being misused, can we identify the specific veterans harmed by this misuse, and provide them with additional victim assistance? And thirdly, if the breached file is being misused, in what locations are those breached consumer identities being misused, so that law enforcement can stop the misuse, and potentially recover the breached data file?

How does this technology work? Simply put, when thieves used a breached file, they leave tracks. In order to obtain credit or other goods, in a veteran's name, a fraudster would have to manipulate that veteran's identity information on a new account application. For instance, if a fraudster applies for a credit card in a veteran's name, the fraudster needs to change the address so he or she can collect the new credit card from the bank. The fraudster will change the veteran's phone number for personal and employment verification purposes. He or she may use the same addresses and phone numbers to commit identity theft against other identities that were part of that same breach.

Our ID network, which receives hundreds of thousands of applications and other identity risk events per day, can identify these types of anomalous changes and relationships across a breached file, regardless of the size of the breached file. We believe this technology can be significant to the Department of Veterans Affairs for the following reasons: it can help identify any organized misuse of the personal data that has happened so far. The analysis can quickly identify veterans who may have been victimized, so that additional victim assistance can be expedited to them. It can actively monitor the file for possible misuse. This technology can help provide law enforcement a way to identify those individuals who have either stolen the files or have misused it to commit identity theft, to stop further misuse and to recover the lost file.

The analysis can help determine if the file was in use by more than one individual, or one cohesive group. And finally, breach

monitoring provides a deterrent effect, once publicly announced. Thieves should be aware that if they try to misuse any data from the VA data breach, they do so at their own peril.

Thank you again, Mr. Chairman, for the opportunity to present this testimony.

[The statement of Mr. Cook appears on p. 85.]

The CHAIRMAN. All right. I have two areas I want to touch on, and then I am going to yield to my colleagues.

Yesterday, when the VA made their announcement of credit monitoring, I don't know too much beyond that, nor do I know where they are going or how they define it. My first reaction was, I was concerned. And let me explain why I was concerned.

The concern is that, are we creating a false expectancy among the veterans that the VA is now going to just be doing credit monitoring, and when I look at my current reports, I'm safe, that somehow that is going to provide a safe haven. And that is the reason I did not issue a statement yesterday. I couldn't stand up and cheer, because I still have great fears.

So let me turn to you, and I want you to tell me, "Steve, I agree with you," or "I disagree with you, you should cheer about this." Because here, we take it down to the next step, is that if they know what they are doing, they are going to take this, and it is going to be synthetic identity theft. So Mr. Cook, as you identified that you look at the granulation of the information and then you begin to change it a little bit; so I take Dr. Eugene Spafford, I get your Social Security number, and I got your address, and know what your wife's name is. So I make the application, but I change the last two digits of your Social Security number. So now, I obtained a credit card and begin to make purchases. I do other things that spoil your life, Dr. Spafford, but if all I am doing is monitoring the credit report, then no serious action by me is not going to show up on the credit report, as I understand.

So now, let me yield to the panel, and say, "Steve, you get it right," or "Steve, you got it wrong."

Mr. COOK. Chairman Buyer, we've done a lot of analysis on fraud and how criminals use data. And I don't believe the people, if they use this data, are going to perpetrate synthetic fraud. The reason for that is synthetic fraud is when you don't have any data available to you. So fraudsters could go out and use a name, and create a valid Social Security number, as we have seen, by a method such as Social Security number tumbling, to enable them to get past a validity check. People who perpetrate synthetic fraud do that because they don't have access to data, and the analysis we have done shows that if they perpetrate synthetic fraud, they do not perpetrate identity theft.

So I would probably disagree and say I don't think synthetic fraud is going to be the case here. I think it is going to be identity theft, and I think that credit monitoring might help those consumers who take the credit monitoring up on that offer. It may help them detect some of the fraud that is happening to them. But it is not going to be the only solution that is available to them. Here is the reason for that: credit monitoring is going to tell you that you had an application that was filed in your name. By that point, it is probably too late. Because as I said in my opening state-

ment, if these guys who took the file are sophisticated enough and use it the right way, they will use the identity once or twice, and never again. So by the time that monitoring alerts get to the consumer, it is already out there and there is nothing more they can do about it.

So I think credit monitoring has its place for consumers. If you think about consumers, we all have about a one and a half to three percent chance of having identity theft happen to us. The chance of veterans having identity theft happening to them because of this breached file is far less than that, just because of the magnitude of it. So I think credit monitoring is fine for consumers, if they can afford it. But we think there are better technologies to detect if there is misuse; if there is misuse, to locate where it is so you can go and try to recover the file; and thirdly, to really detect if there is misuse for a specific veteran, and then you can help that veteran out.

Dr. SPAFFORD. Mr. Chairman, monitoring detects after something has occurred, as Mr. Cook already mentioned. But credit fraud is not the only concern that should be present. As I noted in my comments, we now have all of this information on individuals who have ably served their country, and that information can be used to get replacement identification cards, passports, driver's licenses, and other information, for individuals to have a clean record, or even a trusted record, to go out and cause trouble; that when they run up a criminal record or misbehavior under those identities, it is not going to show up in a credit report, but more likely in a criminal report or a civil action. And monitoring is not going to prevent that, or even assist that.

The CHAIRMAN. All right. I mean, if I—by way of consumer products, and if in fact we are into the marketplace to purchase a consumer product, my sensing is that we don't want to just monitor. We want to do data verification, we want to be able to look at identity verification, and examine perhaps even insurance-based products. Because we have a choice: either—gosh, I threw out this suggestion and wow, judiciary Committee runs off yesterday, and they create the claims adjudication process. All I said was we were thinking about it. Isn't that amazing about this institution? It is in consideration and boom, they go off and they do it. Now I have got to tell them, "Wait a minute." So I just want all of you to know, when you read about this today, we are going to put all this a little on hold, so we can understand all this a little bit better.

This is what we need to know from the VA, and I am not going to go with you on this one, unless you are prepared to talk about it today, but if there is a product out there whereby we got to monitor this for almost three years, we need to give them the tools out there when we do this bid on this contract, and if we can purchase that insurance up there using proper algorithms, to what our exposure would be on a contract, is to go with an insurance-based product out there whereby the veteran is protected up to $25,000. That way we wouldn't have to get into the, quote, "claims adjudication Process." We accept the responsibility, we, the government, have lost the data. But those are things for us as members to consider.

The last point I will make before I yield to Mr. Filner is a point that the witnesses discussed, and that we have concerns about, and

that is in our society, we believe in something that is very congruent, and that is if I say that you have the responsibility to do something, then it must be coupled with the authority to act. And if I were to say that you have the responsibility, but you do not have authority, it then creates a syntactic situation, meaning it results in something that is incongruent.

And if you have something that incongruent, you then have an opinion that is called a heterodox. And a heterodox is something that is completely out of the norm of society's communications. So I say to the firemen, "You have the responsibility to put out the fire, but you have no authority to hook up to city water." So the Secretary turns to the CIO and tells him that "You have got the responsibility to do quality assurance; i.e., cyber security, et cetera, but that you have no authority to enforce, or tell anybody to do anything." I am very concerned.

And I appreciate all of your testimonies. Mr. Filner, you are recognized.

Mr. FILNER. Thank you. Your testimonies show you have obviously great expertise. You also give us very specific recommendations, which we can act on, and that is very useful.

You have tried to talk to the VA about the kind of technology that you have and the services you could provide?

Mr. COOK. Yes, sir.

Mr. FILNER. What happened with that?

Mr. COOK. We are continuing discussions with them. We are hoping to be able to provide them services.

Mr. FILNER. As I understood what you do, it goes beyond what their announcement was yesterday.

Mr. COOK. Yes, sir. I looked at the announcement that they made. There was a small piece of that announcement that talked about looking at other breach monitoring, or breach remediation solutions. And I am assuming that that might have been looking at us, and other technologies that are available to do what we do, to which the best of my knowledge, we are the only one to do that.

Mr. FILNER. So they are talking to you and are going to become aware of your expertise?

Mr. COOK. Yes, sir.

Mr. FILNER. I just read an ad for, I think Visa, and they said they have what is called "neural technology."

Mr. COOK. Right.

Mr. FILNER. They are able to provide their millions of cardholders with the knowledge if anything anomalous happens. Is that equivalent to what you are doing, or similar, or——

Mr. COOK. It is similar but different, Visa and other companies provide different modeling techniques. One is the one that you mentioned, where they can look at an account to see if I am using my credit card properly. All right, if I lived in Texas my whole life and all of a sudden I start using something overseas, and I start to buy a lot of fenceable goods, jewelry or something, that is an anomalous pattern in the account behavior, and there are technologies that do that.

We are the only ones that really apply that kind of technique to an identity. So Visa and others can look at an account. We look at an identity, and look at anomalous patterns about an identity, and

how it behaves, how it behaves over time, and then also how it might relate to other people. And that is the way that we are able to detect if a breached file would be misused in an organized way.

Mr. FILNER. Mr. Buyer was concerned about raised expectations for veterans. If we did use your system, are we giving them some of the security that they need, or the assurances that they need?

Mr. COOK. You would be. You had mentioned that your credit monitoring is not going to get your criminal activity, and so when you look at a problem like fraud, you generally have to throw a couple different solutions at it, and you are still not going to get all the fraud that there is. Our technology I think will definitely detect if a fraud is misusing the file, and they are misusing it more than five or six times, in an anomalous way. We would be able to detect that misuse, and then provide that information to the VA.

Mr. FILNER. I thank you, and I hope we pursue that. Again, we will have to analyze competitors. If there are none, then I hope the VA will think about you.

Mr. COOK. May I make one more point?

Mr. FILNER. Yes.

Mr. COOK. On credit monitoring, and I mentioned this. Whatever solution the VA chooses, and we have talked with them about this, it is important not to publish how long that solution is going to be in place. For instance, if you're going to do credit monitoring for free for one year, anyone who took the file and has an intent to misuse a file, will sit on that for one year and one day, and then they will start to use it. So——

The CHAIRMAN. Mr. Cook, I'm sorry. These will go out under an RFP, publicly bid on, and your people are going to know. I just want to let you know the reality of government procurement.

Mr. COOK. Sir.

Mr. FILNER. Mr. Brody, I had used the analogy for this data breach, used the "Katrina" situation. I mean, at first it seems like a natural disaster, and you have to deal with it. But when you look further, you could have predicted the consequences of a category five hurricane, you know what levies would have to be built, and it turned out we didn't do it.

In this case too, some thief that hopefully is not going to use it stole the data. We couldn't have known that, but then if you look further, we could have prevented this disaster. I don't know if there are any policies in place to keep that data from going to the employee's home. I think you are going to have trouble, Mr. McClain, to fire this employee if there are no policies to say you can't do this. I mean, that is a real problem.

But not only did VA not have policies about taking the data home, but you have outlined years and years' long indifference. So it seems to me, it's not just a natural disaster. There is accountability of management, and I assume you would hold responsible for this breach the top management people——

Mr. BRODY. Oh, absolutely. I mean, as Chairman pointed out, the mismatch of accountability and authority was what we lived on a daily basis. I was the associate deputy assistant Secretary for a heterodox.

Mr. FILNER. He made up that word. Now you are going to use it.

Mr. BRODY. But even in the case of MS Blaster, for instance, that one incident where the VA networks were savaged as a result of malicious software attack, a root cause analysis was performed by the Veterans Health Administration, bringing in a distinguished doctor who had a history of doing root cause analyses, and the analysis concluded that the CIO's office was probably at fault because when it issued the warnings to put the patches in place, it didn't sufficiently convince everybody that we were really serious about putting the patches in place.

Mr. FILNER. When you testified to this Committee in your role as CIO, was it?

Mr. BRODY. CISO.

Mr. FILNER. CISO. Were you as frank and as open as you were just now? Were you able to be?

Mr. BRODY. No, I was not.

Mr. FILNER. Was that made clear to you?

Mr. BRODY. Yes.

Mr. FILNER. How do we get around that? It seems to me that the legislation will need to include the independence of the person. It is a difficult thing. You are in a chain of command. If the legislation is giving you authority, not from the Secretary but from the Congress, then I guess we should give you authority to testify, too, without going through OMB and everyone else. I am just trying to think ahead, what the problems could be.

Mr. BRODY. You are certainly thinking through all the right issues, believe me.

Mr. FILNER. Has a successor been chosen to you?

Mr. BRODY. Oh, yes. Yes, he has been in place for roughly two years.

Mr. FILNER. And nothing much has changed, as far as you know?

Mr. BRODY. No. The culture is still the culture.

Mr. FILNER. Your testimony is very disturbing. We knew about it, you heard me say words similar to yours. So I mean, there have been people that have been talking to you, and we have known about it. But you put it in a way that is extremely, extremely disturbing. This is all about the veterans, not about an organization, not about turf, not about covering up. It is about the veterans. They have lost a lot of confidence, obviously. And your testimony makes it apparent that there is going to have to be a broader scale of changes than just figuring out this particular problem, as bad as this is. The recent loss of data affected 13,000 people—and they offered a reward of $50,000. The VA's loss affected more than 26,000,000 people and the data could be sold for more than $500,000,000. The magnitude is incredible. But as big as it is, we can solve the technical issues, but you bring in even a broader problem.

Mr. Chairman, you have been talking about this for several years. I think everybody now understands why. We have a chance as a Committee, as a Congress, to make the kind of changes that will benefit our veterans and keep them secure in the years to come. Thank you.

The CHAIRMAN. Sure.

I appreciate the general line of questioning, and you were very kind to me. I don't want it to be spun out there that I am upset

about credit monitoring. It is monitoring-plus, so I am glad you explore the other tools that are available, and that is what we want to make sure as members, that whatever the request for proposal that goes out, that it has a broader base to it. I think that is what we need to consider as we work with our appropriators, and figure out how they are also going to be paying for this, and out of what pools of money, and where does it come from. So we don't want it to be just monitoring, it is also the other tools.

To correct the record before I get to Mr. Bilirakis, you said you are the only player in this space. Are you aware of a company called Intelius?

Mr. COOK. I am not.

The CHAIRMAN. All right, okay. I just want to let you know there are other players in the space.

Mr. Bilirakis, you are now recognized.

Mr. BILIRAKIS. Thank you, Mr. Chairman. And I have heard that, you know, great testimony, obviously. I have heard Mr. Brody use the term "root cause." We are concerned about the veterans. This is the veterans' Committee. But I think that our concerns really ought to go past that point. No, we are not talking turf, here, anything of that nature. But Dr. Spafford, you were part of this President's—acronyms for every damn thing up here. But you are part of this group, and you all worked on it for approximately a year, from what I understand. Did you all come to the conclusion that there was no authority, enforcement authority that existed among these chief information officers?

Dr. SPAFFORD. When we did our study that was not a specific question we looked at. However, in talking to people across government agencies, and our own experience, we have found that in many places, individual unit directors and military unit commanders feel that they can override policy whenever it gets in their way. And there is a problem throughout in being able to ensure that security policies and procedures are appropriately carried out. Unfortunately, without some training, the people who are making these decisions do not understand the consequences of overriding those decisions.

Mr. BILIRAKIS. Well, PITAC of course was not designed just to look into the VA Department. It was designed for government-wide, right?

Dr. SPAFFORD. Yes, nationally.

Mr. BILIRAKIS. In your recommendations, apparently you all failed to point out and to emphasize this lack of authority to enforce; isn't that true?

Dr. SPAFFORD. We were looking at the state of information technology across the nation, not simply in the government. And so our recommendations were for the state of cyber security as part of the national infrastructure, not simply government itself. So that was not one of the topic areas——

Mr. BILIRAKIS. You were basically given areas to cover, and you were limited to those areas?

Dr. SPAFFORD. Effectively so, yes.

Mr. BILIRAKIS. But you have now come to the conclusion—and as you were speaking, Mr. Brody was shaking his head. I didn't look over at Mr. Cook—that much of the problem is, I mean, first of all,

you all mentioned culture, and God knows that is a hell of a problem. Not only in the VA, but I suppose probably in all departments and agencies. But shouldn't we be concerned that apparently the lack of authority that is so very, very significant here, so very dense in this area, for crying out loud, does not exist, or apparently does not exist, or doesn't exist adequately, in all the other agencies and departments in the government?

Dr. SPAFFORD. My comments about that in particular were based on my own personal experience rather than the Committee. That was a separate report. But yes, I have seen in many agencies, including Department of Defense, there is a lack of concomitant authority to go with the responsibility. In many agencies, such as appears to be at the Veterans' Administration, and in many companies, the person who is given the responsibility for security with no authority, the real position should have a label of "scapegoat," because that is all that one can do, is take the blame, if you can't effect any change. And this is all too common in the area of security because those of us who understand the risks and want to implement the changes are resisted, because it costs money. It changes the way people do things. And so it is a very common problem throughout government and industry.

Mr. BILIRAKIS. Mr. Brody.

Mr. BRODY. I can only concur. My direct observation was at the Departments of Veterans Affairs, Department of Energy, and the Department of Defense. And in all three cases, direct observation, there is no authority resident with the accountability function of these senior IT officials.

Mr. BILIRAKIS. And you all agree that this—I mean, we can talk about maybe solving or fixing this particular problem ultimately, or whatever the case may be. We are spending so much time on this that we should be spending on other veterans' matters; claims, delay in claims, and healthcare, and things of that nature.

I don't know. Does the president know that that significant part of this overall picture, that lack of authority to enforce does not exist? It was not part of your report that went to him.

Dr. SPAFFORD. No, sir.

Mr. BILIRAKIS. So he does not know? I mean, he doesn't know by virtue of this report in any case.

Dr. SPAFFORD. We were asked specifically to look at the status of cyber security research and technology transfer in the country, and how effective it was. That was the nature of that report.

Mr. BILIRAKIS. Well, you have said that, yeah.

Dr. SPAFFORD. Yes. So as to what the president knows or does not know, I can't comment.

Mr. BRODY. I just find it illuminating that the same body that gave us the Federal Information Security Management Act was not aware of this mismatch of accountability and authority.

Mr. BILIRAKIS. So you know, are we accomplishing very much of anything here? If we really don't look to the root cause, not only to the VA, I mean, this same sort of thing is going to happen in other departments and other agencies—Federal Trade Commission, we just got word, and we are hearing about other agencies or other departments. Should we have legislation—and I guess legislation is only as good as the people who are supposed to be carrying it out,

that would mandate, for crying out loud, that there be some sort of authority? We are going to hear from the Counsel in a little while, I guess who is going to tell us that the authority is not there.

But should we have legislation that would do it? Not just with the VA, and of course obviously, it would be something that would be applicable to all of the other Committees, which might be just enough of a reason to kill the legislation, because you know, jurisdictions assigned by other Committees do. But shouldn't we do something like that? I mean, isn't that part of the root cause, getting to the root cause of all this?

Mr. BRODY. I am on record with the Committee on Government Reform as pointing out that the major flaws in FISMA include the accountability versus the authority mismatch, as well as the issue of FISMA not necessarily measuring the right categories of information security.

Mr. BILIRAKIS. And you are on record as saying, and you all are on record as saying that basically you can't ever solve this unless you take care of that particular area; is that right?

Mr. BRODY. Correct.

Mr. BILIRAKIS. Yeah. Let me ask—we understand that houses in the neighborhood of where this took place have also been burglarized apparently during the same period of time. And I guess they haven't been tied—whether the same person did it, or whatever the case may be. But I think that the impression is that the person took this did not know what he or she was doing, or that they did not know what they had. Are we wrong by virtue of holding these hearings and all this publicity out there and that sort of thing? Is it likely that the thief or thieves know by now what they have in their possession?

Dr. SPAFFORD. Based on the reports that I have seen, it is entirely possible because of a delay in reporting that if the thief was only interested in the physical computer, it had already left his or her possession by the time the news was released.

Mr. BILIRAKIS. Why would that be? Why would it have left?

Dr. SPAFFORD. They would have sold it immediately. Those kinds of tests are usually to pay money for drugs or——

Mr. BILIRAKIS. All right. But whoever they sold it to, the problem still potentially exists for that person, right?

Dr. SPAFFORD. Very often, those systems are completely wiped or whatever—so they can't be traced back. But the second part of your question about holding these hearings, I think are very important, and also goes to your earlier question about is something being accomplished? These kinds of problems have been happening for several years, and are going to happen more frequently. And it is very important that we all understand these problems and address them in some way. So I certainly applaud whatever you are doing in this regard.

Mr. BILIRAKIS. Okay. Mr. Brody, you agree, Mr. Cook?

Mr. COOK. I agree. If they do know that they have it, I know what I would do if I did. I would take it in the backyard and bury it.

Mr. BILIRAKIS. You would what?

Mr. COOK. I am sorry. If I knew that I had the information, I would take it in the backyard and bury it in a very deep hole. Because I think that there is so much scrutiny and so much interest in, you know, who has that file. I think there is other data that I would probably try and take——

Mr. BILIRAKIS. Okay. So actually then, you feel that hearings like this will tend to maybe convince the thief that they had better bury it and not try to use it.

Mr. COOK. We have done analysis in different breaches, and in one of the breaches there was a public announcement that was made. And what we noticed was, after the public announcement was made, the use of the file, the use of the names went way down. So we do think the public announcement helps a good deal. A concern that I would have is that over time, that data can get out. And if that information gets out over time, all of a sudden the attachment to the VA data breach might go away, and it just becomes names and Social Security numbers.

Mr. BILIRAKIS. Right.

Mr. COOK. And if that is the case, and if that information finds its way onto the Internet, over time, veterans can see identity theft happening to them from this breach. But we don't know that.

Mr. BILIRAKIS. Okay, thank you. I am feeling a little better. Thank you, Mr. Chairman.

The CHAIRMAN. Thanks very much. Mr. Michaud, you are now recognized.

Mr. MICHAUD. Thank you very much, Mr. Chairman, for having this hearing. I really appreciate your willingness to stay on top of it. I also want to thank the panelists. It has been very informative.

Mr. Brody, you had mentioned that VHA disagreed with the draft directive 6500 regarding the medical transcription services. Can you recall what they said, and why you thought this to be a faulty reasoning for not complying with it?

Mr. BRODY. Yeah. I mean, in general, their position was that the language of their contract with the transcription company was sufficient control. But my office tried to point out to them that number one, they weren't monitoring or auditing whether or not the contractor was in compliance with the contract; number two, that outsourcing to a foreign company created some issues related to whether or not the individuals that had access to this data had criminal background, or potentially, ties to terrorist organizations. And number three, foreign organizations, foreign corporations deny us the ability to seek to address any issues in the U.S. courts, should it come to that.

And when we pointed those things out to them, they, you know, took them under advisement, and went off and did their own thing.

Mr. MICHAUD. Thank you. Second thing, Mr. Brody, specifically was there any information or cyber security weaknesses in the VISTA system? If so, what were they and what could be done to fix them?

Mr. BRODY. The Committee might find this interesting, I recall reading in the VA publication that is distributed in the hallways and near the elevators a few years ago, where there was an article on this done, and it was declared in the article by, you know, senior VA officials, how proud they were that they were able to develop

Vista underground, without any involvement by the headquarters. And so I don't know what the software looks like inside Vista. I do know that as of two years ago, it had no access control whatsoever. And I don't know if that has been corrected to date. So I would encourage the Committee to potentially take a look at—maybe do a security audit of Vista, and see what they find.

Mr. MICHAUD. Thank you. You had mentioned that you had worked with DOD and the Department of Energy, and you mentioned some of the same things about, you know, who was in charge. Did you witness similar problems with the other agencies, as far as security, that you witnessed at the VA? And does the DOE suffer from another agency's similar resistance to change, even though the authority might not have been the same; has it been that resistance in the other agencies, that culture, so to speak?

Mr. BRODY. Overall, yes. I mean, not to quote Yogi Berra, but their similarities are different. And that means that in the national security world, which includes DOD and DOE, there tends to be a little bit greater appreciation for, across the population, for the need to operate more securely. Nonetheless, the decentralization, especially in an environment like DOE, has created similar, fragmented security issues, as exist in many other civilian agencies.

Mr. MICHAUD. Thank you. And is technology difficult to centralize, the IT operation within the VA, do you think?

Mr. BRODY. There are some complexities associated with technology, but overall, technology is not the problem. I mean, the technology complexities relate to, in the case of the VA, some of these very older systems that are no longer supported by the original manufacturer, and those just probably need to be retired or migrated. But overall, the technology part of this problem is not the hard part of the problem. It is the cultural part of this problem.

Mr. MICHAUD. And my last question. In your opinion, do you feel that the 26 million records, is that a national, or non-national security problem?

Mr. BRODY. If you take the strict definition of FISMA, it is a non-national security problem. But I feel that when you begin aggregating the kinds of information that can be contained in those kinds of databases, you are very perilously close to a national security problem.

Mr. MICHAUD. Thank you. Thank you, Mr. Chairman. I yield back the balance of my time.

The CHAIRMAN. Thank you very much. Mr. Moran, you are recognized.

Mr. MORAN. Mr. Chairman, thank you very much.

Mr. Cook, you said something in your testimony or a response to a question, I think, that caught my attention that I'd don't understand. And it dealt with the percentages of Americans that are subject to identity theft, and I think it was one and a half to three percent. And then you indicated that the veterans who were in this computer information were something less. Would you explain that to me?

Mr. COOK. Sure. What I mean by that is, we have done a lot of analysis, and what we know is that the size of the breach is very important to the misuse rate of that breach. If it is misused and

if you are a consumer, you want to be part of a very large breach. Because if you are part of a 26.5 million record breach, then the probability of somebody picking your name out of that fairly large hat and using your name to commit identity theft is very, very small. If you have a—and let us just say, if you put your mail in your mailbox and somebody takes your mail out, I would consider that a data breach of one. So there, you would have a very high percentage of your name being misused. So, the point I was trying to make is, we, all of us have got about a one and a half to three percent probability of identity theft happening to us during the course of a year.

So the probability of identity theft happening to a veteran is one and a half to three percent, and so because now, they are part of a very large data breach, it is only going to increase very slightly for them, okay? But as a whole, it does mean that there will be more victims of identity theft in the U.S. It does mean that.

Mr. MORAN. What then is the value of the 26 and a half million names, the information, then, on the street? Twenty six and a half million is too much data for somebody who would be in the market for identity theft?

Mr. COOK. Well, it is a lot. If you were one person, it would take you—we have done the math on it—it would take you about 12 lifetimes to use that one file. So it is a lot of data for one person to use. If they were to take it and disseminate it out on the Internet and try and sell it in packages, you know, we have heard anywhere from $25 to $75 from consumer advocate groups who have said this is what they hear. So there is a lot of dollars that they could get by selling that data, but again, if I had taken the data and I knew that it was the VA file, I would run away from it because I think there is going to be such intense scrutiny on that file, that people are going to be trying to find someone misusing that data.

Mr. MORAN. What is the occurrence that causes us to know at some point in time that the security has been breached, and the information is being used? What would you expect to be the first sign that there is a real problem?

Mr. COOK. Well, it will be the anomalous behavior patterns that you would see in the file. For instance, there are 70, 60, 50 people in the room today. If all of our data was breached, six months from now if we all started using the same cell phone number, that would be anomalous. If half of us started living in the same apartment complex, that would be anomalous. And that is how we can detect the misuse. It is the events that happen after the breach to a specific identity, and the way that we can pull those things together. And that I think would be your first indication that somebody is actually misusing that file.

Mr. MORAN. And this would be announced? This would become known because some veteran would indicate something bad is happening in his or her life?

Mr. COOK. That is what credit monitoring would require, is that a consumer really kind of placed their own report, and then provide that data to a central source, and that is not being done. And there would be so much noise in that, because again, we have a percentage of identity theft that is going to happen to us. It wouldn't be the consumer saying it, it would be our ability to look at the

breached file, and then look within our ID network and see applications that were filed in those veterans' names, and then determine which of those applications were probably filed by the veteran, and which of those applications might have been filed by a fraud ring who has access to that file.

Mr. MORAN. Thank you.

Mr. Brody, I think you have been asked this question, and maybe Dr. Spafford as well, but for my understanding, is there something unique about the VA that really—I mean, this happened with VA information, so the focus is on the VA. We talk about the culture, the atmosphere, the attitude. Something unique about this place or just any other government agency is the same risk as the VA——

Mr. BRODY. My observation would be that we need to be careful about not focusing entirely on this incident, because again, this was discovered almost by accident. How many more of these kinds of incidents are out there and not just at the VA where we know there are no controls in place to prevent it? We know there are no controls in place at other government departments and agencies, where, you know, larger amounts of information may be on some employee's owned computer, or on some contractor's owned computer. And so maybe the attention we are drawing to this incident could be creating an opportunity for, you know, some other bad actor out there, and that would be an unfortunate turn of events.

Mr. MORAN. But the personnel of the VA aren't any blinder, or culturally resigned to the status quo than any other place?

Mr. BRODY. Not necessarily, no.

Mr. MORAN. Okay, thank you very much. Thank you, Mr. Chairman.

The CHAIRMAN. Dr. Spafford, did you have something you wanted to say to Mr. Moran?

Dr. SPAFFORD. I was simply going to say that there are some better and some worse. A lot depends upon their individual view of the data, versus their mission. So some organizations, as Mr. Brody said, in working with national defense, will be more aware of that value. And in other places where they view that their mission—and unfortunately, this is part of the problem, why this happened. The person who lost the data viewed that his mission was to get his reports done, or get his work done, rather than protecting and serving the veterans that the agency was supposed to be involved with. And where that disconnect occurs, you have more of these problems.

Mr. MORAN. I would think that Mr. Buyer's leadership on this issue and the hearings that we are having, and the focus of the national attention on this issue, would cause other departments and agencies to have a desire to change their ways. Maybe that is just Kansas commonsense, but I hope it works that way in Washington, that this is the catalyst that causes us all to think that, "My gosh, what we are doing isn't quite adequate."

Dr. SPAFFORD. Well, as I noted, and as Mr. Brody noted, this is not the first such incident, and these kinds of things have been going on for years. And whoever is currently in the spotlight takes a fair amount of heat, and vows never to do it again, and then someone else gets caught.

Mr. MORAN. Thank you, Mr. Chairman.

The CHAIRMAN. Mea culpa, mea culpa, mea culpa.

Ms. Herseth.

Ms. HERSETH. Thank you, Mr. Chairman. And I appreciate the questions that I know Mr. Michaud had a chance to pose to Mr. Brody, and Mr. Moran's line of questioning. I hope this presents an opportunity, as I explored in an earlier hearing, to evaluate whether or not we have the same weaknesses within these CIO organization across other Federal agencies, which you had an opportunity to serve in two different agencies. And that while the VA is currently the one taking the heat, that whether it is USDA, EPA, DOE, others, start taking steps, and CIOs start sharing information across agencies, and that we make the decisions in the Congress about the resources at the front, and are they going to be necessary to prevent these types of situations that cost us far more at the back end.

So let me just ask one question, because I know there is probably an interest in moving to the next panel, as well. Mr. Brody, we have had some discussions here about the age of the various files within the VA. Is it technically difficult to encrypt or convert VA's older databases?

Mr. BRODY. It is more difficult to encrypt the databases that are on older hardware platforms, and older software operating systems that are no longer supported by any manufacturer. There are workarounds, and there are some complexities, but it is not impossible. And by and large, the technology part of this problem is not the hard part of this problem. Technology is available to solve most of the deficiencies identified by the IG and the GAO, in the VA.

Ms. HERSETH. So if the technology isn't the problem, it is the resources and the obstructionism that we have to overcome, that is the problem?

Mr. BRODY. More or less, yes.

Ms. HERSETH. Okay. I yield back, Mr. Chairman. Thank you.

The CHAIRMAN. Thank you. I know Mr. Udall has had to step out for just a moment, so let me—we have votes that are going to occur at 12:15 to 12:30. So what I would say to Mr. McClain, I apologize but it is life on the Hill.

All right, so Mr. Brody, I am going to go back to this, and we are going to get into this in the next panel with the General Counsel, about why they made certain decisions in their memoranda. But if I try to follow the logic, that FISMA is not—let me restate this. According to the most recent FISMA report, VA has no agency-wide security policy, is what the recent report says. If you were to design security policies, what would be the key components to be included in that policy?

Mr. BRODY. It would include the confidentiality, integrity, the availability, and the accountability, for the necessary controls on all the VA's system, including the protection of data.

The CHAIRMAN. Dr. Spafford, would you agree with that?

Dr. SPAFFORD. Those would certainly be the core elements of the policy.

The CHAIRMAN. What kind of training would be necessary to implement such a policy? And what kind of time are we talking about?

Mr. BRODY. It would depend because there will be certain roles that would have to be trained. Managers across the agency would need a certain kind of training. Practitioners responsible for actually maintaining security devices would need a certain different kind of training. And by and large, a lot of that training is in place in the VA. We had put in place, following the incident in which some computer systems containing veterans' data were purchased by the television station in Indiana, we had put in place a program of practitioner professionalization, and we took 600 people through that program and certified them. But that is 600 in a population of over 200,000, that all need a significant degree of training.

The CHAIRMAN. And would we have any problems with the VA personnel policies or labor practices?

Mr. BRODY. Those cropped up from time to time. Yes.

The CHAIRMAN. Such as?

Mr. BRODY. Well, I mean—the details escape me at the moment, but you know, a fact of the matter is, whenever we tried to put in place any kind of policy that affected the day-to-day life of the individual, the resistance from HR organization was fairly stiff.

The CHAIRMAN. Interesting. Mr. Udall? You are recognized.

Mr. UDALL. Thank you, Mr. Chairman. Mr. Brody, you talked a little bit about security and issues of security, and I wanted to ask you about—under the Federal Information Security Management Act, are you comfortable with the distinctions between a national security database, and a non-national security database? And how would you define these? And with respect to the specific information that was lost there, which category does it fall into? And are there any things that we should do in order to better protect ourselves, in terms of these definitions?

Mr. BRODY. I would say I understand the definitions, and whether or not I am comfortable with them, I spent 10 years in the intelligence community, so I understand that when you take what would appear outwardly to be non-sensitive information and begin aggregating it so that it starts to become more sensitive, you cross a fine line into what could be classified as national security information. According to the definitions that are incorporated in FISMA, that does not apply in this case. But I would argue that the aggregation of information in VA's systems can be of significant value to those who would wish to do this country harm.

Mr. UDALL. And is there anything we can do to further protect in that area, other than what you have already outlined here today?

Mr. BRODY. Well, I mean I actually raised this issue in 2001 when I arrived at the department. And I was told that that is the responsibility of the office of security and law enforcement, and "Thank you very much for your input." So again, we are dealing with the fragmented security authorities across the department.

Mr. UDALL. Several statements by the VA indicate that the employee who took home the data did so without authorization. If he was already authorized access to the data, what policy or regulation would have required further authorization? and do you recall if the IG or the GAO, or any other entity, ever commented on this as a weakness?

Mr. BRODY. I am not aware of any policy that would have prevented this. Nor am I aware of any comments by any other party.

Mr. UDALL. A changed management system developed after Secretary Principi attempted in 2002 to centralize the CIO function. This new system was characterized by significant non-line reporting. How well did this system work, and did that hybrid system approximate the Federated Management system recently adopted by the VA?

Mr. BRODY. Yeah, I would have to characterize the results of that as not in keeping with the spirit of this Committee's concerns, as addressed in 2002. Once we get to that of a line sort of authority thing, and then in the wake of the MS Blaster incident, we did an analysis internal to my office, and I am sorry that I don't have it present, but I am sure that we can probably draw it out of someone's files, where we determined specifically who had responsibility for configuration control and configuration management in the department. And it turned out that as a result of the efforts by Secretary Principi to put that memo in place in 2002, there were no less than 13 separate places by which configuration control would be managed in the department.

Mr. UDALL. To Dr. Spafford or Mr. Cook, do you have any comments on anything you have heard, or I have raised here?

Dr. SPAFFORD. No.

Mr. COOK. No.

Mr. UDALL. Okay, thank you. Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Mr. Brody, in your testimony you testified to something that we as a Committee had considered, and that was whether to elevate the CIO to the level of an under Secretary. And we thought about that as a Committee when we put together our legislation, and I guess looking back on it, maybe we should have. Really, our inward discussions were dealing with if you have a culture of resistance that I called the "centurions of the status quo," and it is much easier for the three under secretaries to run over the CIO, especially if they can then—they all are competing to win the support of the deputy Secretary, or the Secretary. So I just want to let you know, I got your message. I embrace it, and we as a Committee are going to look back on your recommendations.

Let me turn to Mr. Cook. With regard to data, when an individual feels—you know, they went to the ball game, just had their purse stolen, their pockets were picked, now it is like, "Oh, my gosh. I had 12 credit cards in there. It is now gone. What do I do? Who do I call?" My question to you is, what is the norm before an individual will begin to feel the bad effect?

Mr. COOK. There has been some analysis on that, and FTC I think has done some of the best analysis, and another organization called Identity Theft Resource Center. I think the average—and I'm not sure of this, but I think the average is about six months before they actually see it. Because what happens is you might get an inquiry in your credit reports that you may not be aware of, because you don't have credit monitoring. And then, that account, if it is a wireless account or a credit card account, is open, and then that fraudster might use that account. Some people will take the account, buy fenceable goods, and go bad right away. Others will

use that account over time, as many as 18 months, so that they can do something that the industry calls "bust-out," where they can actually drive the account much higher than what the credit limit is.

And so generally, consumers will find out they are a victim of identity theft because they will get a call either from their credit card issuing bank, or the wireless company, or from a collection company. So it is generally about six months, 7, 8 months out.

Now, if there is a fraudster who steals an identity and uses that identity over and over and over, and that consumer happens to have consumer monitoring—this is a very small percentage of people—then they may be aware of that within as quickly as three weeks, if you will.

The CHAIRMAN. All right. Our challenge here is to build a system, and at the same time take care of the veterans, and produce that product in Congress, as we work with the administration. I want to thank you for taking your time to put together your testimony, and for being here. I appreciate that.

Mr. Brody, thank you. We asked you to do a job, and put a patch over one eye and we tied your good arm to your back, and you did your very best. And I know it was hard, and it was difficult. And we don't view you as a scapegoat, because the more we do our forensics, the better the understanding we have about the culture, and the problems, and the resistance to change Mr. Filner had discussed.

And we are going to embrace your recommendations, along with Dr. Spafford. Once again, let me thank you for helping your country. Your testimony is insightful and valuable to us, as we formulate this legislation.

Any other questions?

[No response.]

This panel is now excused. If we could turn to the second panel. And even though we got a warning that votes will occur. Dr. Spafford, do you have to take off? Do you have to run? Dr. Spafford, do you have to catch a flight?

Dr. SPAFFORD. Later on this evening.

The CHAIRMAN. Okay, could you sit and listen to this panel? Are you going to have to take off?

Dr. SPAFFORD. No, I can——

The CHAIRMAN. That is wonderful, thank you. What I had planned to do, Dr. Spafford, is I would like you to listen to this panel, and then I am going to circle back with you—we could have a discussion. If we can't get it today, are you around Monday, at Purdue University?

Dr. SPAFFORD. No, sir, I will be at a conference——

The CHAIRMAN. At a beautiful resort? Don't answer that.

Dr. SPAFFORD. Allegedly.

The CHAIRMAN. Allegedly, great. Means you're in Toledo? Sorry, nothing against Toledo. All right. Hey, hey, hey.

Sitting on our second panel is the General Counsel for the Department of Veterans Affairs, Mr. Tim McClain. Mr. McClain was confirmed by the Senate as the General Counsel for the Department of Veterans Affairs in April 2001. As General Counsel, he serves as the chief legal adviser to the Secretary of Veterans' Affairs and the department's other senior leaders, and manages the

Office of General Counsel, which is comprised of nearly 400 attorneys assigned throughout the United States.

Mr. McClain also served as the VA Chief Management Officer from January 2005, through November 2005, responsible for the department's budget, financial policy and operations, acquisitions, material management, real property asset management, environmental policy, and business oversight.

Thank you very much for being here. If you would also introduce Mr. Thompson, who accompanies you and you will then be recognized.

Mr. MCCLAIN. Mr. Chairman, thank you very much. Mr. Chairman, Ranking Member, and members of the Committee, accompanying me this morning is Jack Thompson, who is the Deputy General Counsel at the VA, and he has over 30 years of service with the VA as an attorney. Also, I would like to, if I could, ask that my full statement he made a part of the record.

The CHAIRMAN. All right. We do. If you will arise and give me your right hand.

[Witness sworn.]

The CHAIRMAN. Thank you, please be seated. Mr. McClain, you are recognized.

TESTIMONY OF THE HONORABLE TIM S. MCCLAIN, GENERAL COUNSEL, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY JACK THOMPSON, DEPUTY GENERAL COUNSEL

Mr. MCCLAIN. Thank you, sir. And thank you for the opportunity to discuss the legal implications of the May 3, 2006, theft from a VA employee's home, of personal identifying information concerning veteran servicemembers.

This incident brings into sharp focus the Federal laws that address a similar issue; i.e., safeguarding personal information. Both the Privacy Act and the Federal Information Security Management Act, or FISMA, provide a framework for establishing agency safeguards to ensure the security and confidentiality of records. These statutes generally outline agency responsibilities, and require the agency head and senior officials to ensure compliance with the law. Since we were made aware of this terrible situation, the employees of the VA have worked tirelessly to ensure two things: one, that the normal services to veterans, including healthcare, benefits, burial, and memorial services, have continued uninterrupted. And two, that we address this situation in such a manner that it will minimize any adverse impact on a veteran. This is VA's problem, and we intend to address it as one.

Secretary Nicholson has launched VA on a course that will result in VA being the gold standard for information security in Federal Government. That is no easy task. VA is so large, and with so many very vital programs, that it will take a concerted effort on every employee's part to make it happen. Just as VA transformed its health-care system from one of questionable quality in the early 1990s, to today, the recognized leader in healthcare delivery and electronic healthcare records, we are committed to leading the Federal Government in information security.

Along that line, in an October 19, 2005, memorandum, Secretary Nicholson ordered the reorganization of VA's IT operations. In February 2006, the Secretary strongly advised senior agency officials at a senior management retreat that today's IT reorganization was his top priority. In that regard, on April 30th of this year, over 4000 employees were detailed to the Office of Information Technology, as part of this implementation plan. As of the end of the current fiscal year, those employees will permanently be transferred to the Office of Information Technology. This has placed all IT operations and maintenance personnel under the supervisory control of the CIO.

Another major development was announced yesterday by the Secretary. That VA is committed to providing one year of free credit monitoring to individuals whose sensitive personal information, their names and Social Security numbers, may have been stolen as a result of this incident. Providing free credit monitoring will help safeguard those who may be affected, and will provide them with the peace of mind they deserve. This week, VA will solicit bids from qualified companies to provide a comprehensive credit monitoring solution. VA will ask these companies to provide expedited proposals, and be prepared to implement them rapidly, once they are under contract. Once VA hires a credit monitoring company, the department will send a detailed letter to individuals whose sensitive personal information may have been included in the stolen data. This letter will explain credit monitoring, and how those eligible can enroll or opt in for the services. The department expects to have credit monitoring services in place and the letters mailed by mid August. VA will also be soliciting bids to hire a company that provides a data breach analysis, which will look for possible misuse of the stolen VA data. The analysis will help measure the risk of the data loss, identify suspicious misuse of identity information, and expedite full assistance to affected individuals.

These efforts will augment the other aggressive steps VA has already implemented in response to the unfortunate incident. As previously announced, the Secretary has already directed a series of personnel changes in the affected office within the department. The Secretary has also hired a former Maricopa County prosecutor, Richard Romley, as a special adviser for information security. He ordered the expedited completion of cyber security awareness training and privacy awareness training for all of VA employees, and also ordered an inventory of all positions requiring access to sensitive VA data. He also asked that every laptop undergo a security review. And the VA's facilities across the country, every hospital, CBOC, community outpatient clinic, regional office, national cemetery field office, and VA central office here in Washington, observe a security awareness week, beginning next Monday.

Thank you, Mr. Chairman, for the opportunity to testify, and I will be glad to answer any questions from the Committee.

[The statement of Mr. McClain and accompanying documents appears on p. 92.]

The CHAIRMAN. All right. First, I have—have you been present during the discussions on formulating this policy to provide the free credit monitoring? Were you present at these discussions?

Mr. MCCLAIN. Yes, sir.

The CHAIRMAN. Okay. What does free credit monitoring mean?

Mr. MCCLAIN. Well, it will be defined by the bids that are received in response to the RFP that has gone out. Credit monitoring is a package of services that are offered by, for the most part, the three major credit bureaus, and possibly others. And they have different levels of this service that you can actually purchase from them. The RFP will be requesting a very robust package for to cover the veterans, and it will be determined by actually what the bids are in response to the solicitation.

The CHAIRMAN. You got my attention in your testimony when you talked about a comprehensive approach. My sensing for my colleagues is that is where our greatest interest is. And so let me go back to my earlier comments, when I heard about the, oh, credit monitoring. It has to be about more than just that. And that is also our testimony from the first panel. So now, we say, okay, we are going to invite the credit monitoring, you say we are going to do bids to do a comprehensive approach, and then we are also going to do a second—you have got two proposals that are going to be going out; is that correct?

Mr. MCCLAIN. Yes, sir.

The CHAIRMAN. All right, tell me a little bit more about your first proposal for a comprehensive approach. Is that sort of what the gentleman was talking about from analytics, or also Intelius does, out there in the private-sector?

Mr. MCCLAIN. Sir, the comprehensive approach would be the entire—would be everything. In other words, both solicitations that go out, which would include a robust credit monitoring package, and it would include a company to come in and do the data breach analysis.

The CHAIRMAN. Okay. But on a comprehensive approach, are we also saying that you are considering purchase of insurance-based product?

Mr. MCCLAIN. Yes, sir, because that normally comes with your normal commercial credit monitoring package. If you were to go to any of the big three credit bureaus that would be included in the package.

The CHAIRMAN. Mr. McClain, that is a big deal. I think it is a big deal. Because Congress out here just yesterday, the Judiciary Committee immediately goes out there and does the claims adjudication process. And when I brought that up, I talked to the Secretary about that. And he is like, "Whoa, Steve, I know what you are trying to do. Let us see what is available in the commercial market."

Even if we were to do that, do we want to keep it in-house? Would we keep it under you? Would you create a separate agency to do that? You don't want it to be organic, limited in scope, limited in time, a lot of things to think and consider about. But you can notice how heightened members are about the issue, that the Judiciary Committee would run out. So I would welcome the VA to explain this a little bit further as you are formulating this. I think that the VA is saying that we are interested in providing that financial assurance—an insurance-based product while we do this, will make veterans feel a little bit better. Would you agree?

Mr. MCCLAIN. Yes, sir. And we'll be glad to. I'm certainly not the expert in the credit monitoring packages or the insurance, but we'll be glad to provide the Committee with a more detailed reasoning as to exactly what that entails.

The CHAIRMAN. All right. Here is what is happening, is that not only are you learning, VA, more about this; so are we. And that we want to work with you on how you develop your comprehensive approach, as opposed to us, you know; either that or we dictate something and we don't want to have to do that. I mean, we can set parameters, but you are also going to be coming here and asking us to pay for it. Okay?

With that, I yield to Mr. Filner.

Mr. FILNER. Mr. McClain, I think you ought to be ashamed of the testimony you just gave us. You sat through an hour and a half of testimony, detailing some very grave problems in the culture of the VA. We also heard some very technical and very specific suggestions on what we might do, including the weaknesses of just credit monitoring. And you read the same thing that you walked in with, as if you didn't hear anything, nothing is wrong, the Secretary is taking action, you are taking action, everything is fine. You have the lowest guy on administrative leave, and it is not clear that he violated any policy, anyway, and his superior resigned. We just heard of extensive management failures of VA. You don't address that. It didn't happen. You are testifying about a completely different world from the one we heard.

You have the biggest breach of security of identities in the history of this country, and you haven't come to grips with this issue. Your testimony shows the very reason why we have a problem. You don't recognize anything, you don't admit anything, you don't acknowledge anything, you don't want to change anything. This is disgraceful.

Given the testimony from Dr. Spafford, and Mr. Brody, and Mr. Cook, why shouldn't you and everybody above you in the chain be held responsible for the data loss? It was your memos that said there couldn't be any centralization. It was your memos that contradicted the authority of FISMA. It was your memos that said the Secretary is not going to centralize. Why should you not be fired for this incredible breach?

Mr. MCCLAIN. Mr. Filner, first of all, I think that VA has taken this very seriously. I mean, this is——

Mr. FILNER. The first step is to acknowledge a problem. Read your statement again and show me where you acknowledge that there were some errors in the management of your agency. Show me where. I just read your whole testimony. Not one word to show that you understand the severity of the problem. They say the first step in understanding addiction is, you have to get rid of denial. You are still in denial.

Mr. MCCLAIN. Denial that there is a problem——

Mr. FILNER. That there is something—in the culture of the VA management system that caused this.

Mr. MCCLAIN. I believe that the Secretary has testified on more than one occasion in front of this Committee and others, saying that there was a problem, and it has made him mad as hell.

Mr. FILNER. I can see everybody is mad as hell sitting here.

When did you hear about the data breach after May third? When did you hear about it?

Mr. MCCLAIN. May 16th.

Mr. FILNER. You don't think that is a problem in your system? That it took you two weeks to hear something?

Mr. MCCLAIN. I believe it is.

Mr. FILNER. So what are you doing about it?

Mr. MCCLAIN. We are——

Mr. FILNER. You are asking for an RFP, yet you are not doing one thing about the management, as far as I can tell.

Mr. MCCLAIN. Oh, I think that——

Mr. FILNER. Tell me, what are you doing?

Mr. MCCLAIN. We are doing a complete review of information security in every single office in the VA. From the lessons learned from that, and this is being chaired by the deputy Secretary. From the lessons learned, we are going to move forward with implementing changes, so that there is a uniform information security policy throughout the——

Mr. FILNER. What were the lessons you have learned?

Mr. MCCLAIN. Sir?

Mr. FILNER. You said we are going to implement the lessons learned. What lessons have you learned?

Mr. MCCLAIN. That we need to pay more attention to information security, that we have people out there that do not realize that what they have is a veteran's personal data in their hands, or on their laptop, and they are——

Mr. FILNER. Don't talk about other people. What have you learned? I want to know what you have learned. Do you question what you did in those memos in 2003 and 2004 when you gave basically the legal rationale for not doing anything? Would you retract those, or would you redo them? Tell me what you have learned.

Mr. MCCLAIN. Mr. Filner, I would not retract those. I think——

Mr. FILNER. Okay, you are the problem. You are the problem. Until you admit that, it is not going to change.

The CHAIRMAN. I am going to need to recess the Committee. We have six and a half minutes left. We have three votes. So after these three votes, we will return. Thank you. The Committee stands in recess.

[The referenced memos are attached to Mr. McClain's prepared statement and appear on p. 96.]

[Recess.]

The CHAIRMAN. The VA Committee will come back to order, and I yield to the gentleman, Mr. Filner, so he may resume his line of questioning. Mr. Filner, you are now recognized.

Mr. FILNER. Thank you, Mr. Chairman. Thank you for waiting for us, Mr. McClain.

The summary of what I was saying before is that we have a whole series of analysts who agreed on several things, and all my colleagues seemed to agree, also. The issue of authority and resources for the chief information officer or chief information security officer. And you made no comment on that. Your memos on this issue, where you debate the meaning of the word "ensure," reminds me of the president who was trying to debate the meaning

of "is." You are looking for any reason not to get the CISO the authority he needs, and I ask you if you would retract those, and you said, "No."

Do you believe that we have to pass additional legislation to give the CISO authority in your department, although you say here the Secretary could do it on his own? Have you made any steps in changing that authority in the VA? Everybody agreed that is the main thing.

Mr. MCCLAIN. Mr. Filner, regarding the opinions, I do believe the opinions state the state of the law at the time that those opinions were written. In other words, the issues would come in, or questions would come in, and indeed, the case of the April 7th, 2004, opinion, we had three different offices ask us to opine on the particular issue of FISMA.

[The April 7, 2004, memo referred to is attached to Mr. McClain's prepared statement and appears on p. 104.]

Mr. FILNER. Do you think that the CISO ought to have the authority that the three panels all agreed on for good cyber security?

Mr. MCCLAIN. Well, I don't——

Mr. FILNER. You personally, what do you think? Why don't you ask us for legislation that would give the CISO authority? You are hiding behind all these words and these opinions. Do you think you are the General Counsel—do you think the CISO ought to have the authority to enforce the decisions that he makes?

Mr. MCCLAIN. I think that if the CIO had additional authority it would probably make his particular job easier. Is that a good idea? That is really a policy discussion, and not a legal——

Mr. FILNER. Other agencies have interpreted the same law as giving their CISOs that authority, right?

Mr. MCCLAIN. I am not aware of that, sir.

Mr. FILNER. Have you asked other agencies? Did you consult other General Counsels, to see what they said?

Mr. MCCLAIN. No, we didn't.

Mr. FILNER. It seems to me that would be a good thing to do. It looks to me that you all decided he shouldn't have authority, then you found a way to quibble with the word "ensure." When Secretary Principi tried to change, he got resistance from everybody. So that is what I meant when I said you are the problem. You are the problem. You don't even believe the CISO should have authority, the way you said it, "it is a policy issue." I am asking you what you think. We just had the biggest breach in the history of the government, and you are still quibbling about what the word "ensure" means. Should the CISO have the authority to enforce cyber security rules?

Mr. MCCLAIN. Yes, in some form he should.

Mr. FILNER. Well, thank you. Now, would you recommend to us please, by tomorrow, what you would need when you opined that he could actually have that authority? You are the Counsel. Give us some advice on that. Give us the language.

Mr. MCCLAIN. I would be glad to discuss it with your staff, Congressman Filner——

Mr. FILNER. Call me. Don't talk to my staff. You're saying it would be a good thing, so make a recommendation that would

make it happen, since you don't think it can happen under the existing legislation.

Mr. MCCLAIN. Well, I didn't say it couldn't happen under the existing legislation. In fact, both of the opinions refer to the fact that there can be a delegation of authority.

Mr. FILNER. So why hasn't there been?

Mr. MCCLAIN. There has been, to a certain degree, in the reorganization that is already underway.

Mr. FILNER. Has there been any change since May 3rd?

Mr. MCCLAIN. No, I don't believe——

Mr. FILNER. Of this year, since this security breach?

Mr. MCCLAIN. I don't believe so.

Mr. FILNER. So you are not doing anything. You are not focusing on the major problems.

Mr. Chairman, as I said, this is very frustrating. You have been working on this for several years. I have to admit that I didn't pay any attention to you. I should have. And I don't think that Congress did. We have now the opportunity to do what you want to do, and I think we are all going to be behind you. This is not an issue coming from the lone action of one employee. That is what you from the VA keep stressing, because you think he is going to be terminated. We heard that enforcement guidance for cyber security is at best confusing. Some say it doesn't exist. We know that Mr. Brody and others tried to get that authority; it didn't happen.

It all comes back to the policies and the management who makes those policies. Nobody seems to be accepting that responsibility, Mr. McClain. Not the Secretary, not the Deputy, not you. I just can't understand what type of leaders would fail to do their jobs and then try to put the blame on everybody else. When we didn't secure an Iraqi ammo dump, the DOD blamed the troops. When FEMA failed to execute a disaster plan, they blamed the weather. Now, after years of failing to implement a clear, meaningful policy, you blame an employee for breaking some unidentified policy.

Mr. Chairman, I hope that you continue what you have started, and you have backing from all of us, and the American people. We should not tolerate these policies, or the field of leadership that allows them to continue. Thank you, sir.

The CHAIRMAN. Thank you. I have a further line of questioning, Mr. Michaud, but let me make this statement, and I will yield to the gentleman. If you have additional questions, do you?

Mr. MICHAUD. Yes, I have.

The CHAIRMAN. Okay. Prior to the break, I had mentioned what the colleagues with the Judiciary Committee had done with regards to setting up a separate agency to deal with claims adjudication as an administrative remedy for pathway to the tort claims, Federal Tort Claims Act. And I have asked the majority leader to hold that at the moment.

It really is just a great example of the heightened awareness, Mr. McClain, that members of Congress have to, quote, "do something," but that can also get you in trouble. And so I am very sincere in sharing with you, number one, what I had done with the majority leader; number two, my conversation that I just had about 10 minutes ago with Chairman Walsh. I know that the Secretary will be

before this Committee on Tuesday. I plan on attending. And I will see the Secretary again on Thursday.

But over this time period or the next 10 days, we want to work with you. And I took from your testimony an inference, and it is okay, and the inference is that, "we are outside of our lane," and with, "how do we deal with this? We have never had to deal with this before."

So when you say to the Committee that, "We are going to do an RFP, and we are interested in seeing what they are going to bring us," usually that is kind of backwards. We correlate these kinds of things, and let the private sector know what we want. And it is okay, I am not going to be critical of you, because we are interviewing just like you are interviewing, trying to figure out how to best deal with this, because of its scope? And also, how do we pay for it?

I am not a contract lawyer. I have got to yield to you——

Mr. MCCLAIN. I'm not either, sir.

The CHAIRMAN. All right. And so that is why I am not going after you on that. I am just concerned——

Mr. MCCLAIN. Well, Mr. Chairman——

The CHAIRMAN. I just want to let you know, I am concerned about what the Judiciary Committee did. So what I am saying to you, and please convey to the Secretary what the Judiciary Committee just did, I am going to hold that as much as I can, okay, with my relationship with the majority leader, to hold that. Let us craft a product that not only can we begin to monitor, but we can also place the veteran in the assurance that they are not going to have an out-of-pocket loss. We are going to have potentially a disruption of their life. This is going to be uncomfortable. But if we are able to create a product, and there are some out there that can give them up to $25,000 insurance, with regard to the loss, and we make that part of a package, I think it is exactly where the Secretary was in his conversation with me. Not by number, we did not discuss numbers.

But please, I yield to the gentleman.

Mr. MCCLAIN. Thank you, sir. I was just saying that I know that they're working very hard on the statement of work, which will be up with the RFP, and I am sure it will define exactly what we're looking for from the three companies, or even more.

The CHAIRMAN. Well, whoever the "they" is, will the "they" communicate with our staff, and just as important, communicate with the appropriators?

Mr. MCCLAIN. Yes.

The CHAIRMAN. Last thing you want to have happen is put together something that you think is best, but has not been communicated with the appropriators, and you just turn to them and say, "Pay for it."

Mr. MCCLAIN. No, I understand.

The CHAIRMAN. You know, my gosh, you are going to end up just with what they did with Denver, and they zeroed out something because there wasn't the best of communications.

Mr. Michaud.

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

Mr. McClain, The VA directive 6504 dated June 7th of this year stated that, I quote, "the VA employees are permitted to transport, transmit, access, and use VA data outside VA facilities only when such activity has been specifically approved by the employers' supervisor, and when appropriate security measures are taken to ensure VA information and services are not compromised," end of quote.

How does this policy differ from what was done prior to May 3rd of this year?

Mr. MCCLAIN. Congressman Michaud, I'm going to have to not get into that area because of the three pending class-action lawsuits that the actual policies and procedures that were in place at the time are at issue in each one of those lawsuits, and on advice of our attorney, Department of Justice, I can't comment on that.

Mr. MICHAUD. Do you believe that the data involved in the May 3rd incident constituted a national security data breach, or in non-national security?

Mr. MCCLAIN. I have not looked into that or rendered any particular opinion on that issue.

Mr. MICHAUD. Ever been asked to render an opinion?

Mr. MCCLAIN. I have not.

Mr. MICHAUD. So no one at VA is looking at this issue?

Mr. MCCLAIN. Well, I know that it has come up in the hearings, and someone is looking at it. But my office has not been asked to render an opinion on it.

Mr. MICHAUD. Okay, and you have no idea who is looking at it in the VA? Because it has come up in previous hearings.

Mr. MCCLAIN. I believe the—well, the office of information technology is looking into it right now.

Mr. MICHAUD. Okay. Your memorandum of April 7th of 2004, states that FISMA does not require the Secretary to provide the CIO with the enforcement powers to the extent that he chooses to do so. However, he may delegate more authority to the CIO and it is provided for by FISMA. A couple of questions, what specific authority has the Secretary delegated prior to May 3rd of 2006?

And has the Secretary delegated any additional authority since that date? And if so, to which officers?

Mr. MCCLAIN. I don't believe that there was any delegation beyond the actual mandates of FISMA, and the Clinger Cohen Act, and also the Paperwork Reduction Act; kind of the three acts that really control what the CIO does.

And there has been a lot of discussion on what is required at this point, and that is exactly what I was talking about before, is we're currently doing a complete inventory of all information security practices in every office in the VA. And based upon that inventory, that list of best practices and recommendations, I'm sure that there will be further action taken.

Mr. MICHAUD. So you agree that the Secretary can delegate to the CIO the authority that he needs to make sure that these information security issues are upheld?

Mr. MCCLAIN. I believe that—yes, I believe that there is sufficient authority that resides—authority that resides with the Secretary that could be delegated down. Now, the one thing, the one caveat that I want to put on it is that there was some discussion,

in particular, Mr. Brody made his statement that he was frustrated that there was push-back from HR, I guess, when—relating to actual sanctions or penalties against government employees. And of course, that is a problem. When I say "a problem," from an enforcement point of view. Every employee is protected by a lot of Title 5 rules and regulations in the government, and the question would be, could the CIO impose a penalty or sanction, or discipline, on say, a VHA employee that doesn't belong to the CIO? A VHA employee in the State of Washington, for example?

And that would raise tremendous questions under Title 5, Title 38. And those issues would require legislation along some lines in order to accomplish the complete ability to impose sanctions.

Mr. MICHAUD. Even if the Secretary gives him the authority?

Mr. MCCLAIN. The Secretary may not have that authority because of the laws that are in place. That's why I made it a caveat.

Mr. MICHAUD. Does the Secretary know that he has the authority to delegate a lot more than what has been delegated? Has anyone told the Secretary he has that authority?

Mr. MCCLAIN. Yes.

Mr. MICHAUD. So he is aware of it?

Mr. MCCLAIN. Yes, he is.

Mr. MICHAUD. Okay. And has he made any overtures to you that he is looking in that direction, to give all the authority that he can to the CIO?

Mr. MCCLAIN. There have been quite a few discussions, as you can imagine, recently on the issue, and I'm not going to speak for the Secretary, but I believe that there may be action forthcoming.

Mr. MICHAUD. Okay, thank you.

Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Thank you. Ms. Herseth.

Ms. HERSETH. Thank you, Mr. Chairman. I was a little confused by some of the responses. And I know I was a little late getting back in here, but let me just walk through that line of questioning of Mr. Michaud's once again.

Your interpretation is that the Secretary has the authority to delegate certain responsibilities to the CIO?

Mr. MCCLAIN. Yes.

Ms. HERSETH. And that would include enforcement authorities?

Mr. MCCLAIN. Yes, certain enforcement authorities.

Ms. HERSETH. Certain enforcement authorities?

The CHAIRMAN. Like what? Sorry.

Ms. HERSETH. Well—appreciate that. I think that——

Mr. MCCLAIN. That's the next question.

Ms. HERSETH. Let us say, which ones would not be?

Mr. MCCLAIN. When I had just responded in the actual taking disciplinary action against an employee that is not within his department. In other words—let me, if I can, analogize this a little bit. The—under Title 5 of—in Federal civil service, the appropriate person to propose discipline is the employee's supervisor. And so that system is used every day, still in place, and indeed that could be used today, in order to impose discipline on an employee that does not follow published rules and regulations.

Ms. HERSETH. So, separate from disciplinary actions, the Secretary would have the authority to delegate any other enforcement

necessary to ensure compliance by the agency with information security requirements?

Mr. MCCLAIN. I believe so. I mean, there's quite a few things that the CIO could do. I mean, under FISMA and—the CIO has the authority in order to set all of the standards that are for access, for classification, for personnel, those sorts of things, in order to get onto the CIO equipment, the computer equipment, and how to use it, and what to do with it. He can—if you're talking about enforcement—he can prevent someone from getting on, prevent someone from bringing a piece of equipment on——

Ms. HERSETH. Prevent someone from obstruction? Of implementing the requirements?

Mr. MCCLAIN. Yes. Yes.

Ms. HERSETH. Are you aware, you know, your memos have been the focus of a lot of the questions, and even some of the discussion in prior hearings? Are you aware of any similar conclusions that you drew regarding the CIO's enforcement purview of any other General Counsel in any other Federal agencies, reviewing the same type of questions that would come up about enforcement authorities of the CIO?

Mr. MCCLAIN. No, actually that question was asked, and the answer is no, I'm not aware of any others.

Ms. HERSETH. Let me just ask a couple of questions with regard to implementation of the March 2004 Principi memorandum. Your written testimony states that it might be helpful to briefly state what the department has done to implement Secretary Principi's 2004 memorandum. You then state that on April 30th, 2006, approximately 4000 FTE's were temporarily detailed to the office of information and technology. Was that step taken to effectuate the March 2004 memorandum, which calls on then-CIO Robert McFarland, to devise a department-wide cyber security program under FISMA? Or was that a step taken to meet other department requirements or responsibilities, such as the creation of a separate information technology account, in last year's VA appropriations bill?

Mr. MCCLAIN. I think it was a step in direct line with the Secretary's October 2005 decision to order an IT reorganization in the department.

Ms. HERSETH. And do you believe that the items you list in your testimony as addressing the March 2004 memorandum are sufficient actions to have taken in response to that memorandum, in the more than two years since it was released?

Mr. MCCLAIN. I think that it is certainly a large step in the right direction. Are there other things that need to be done? Yes, and certainly the department acknowledges that there is more to be done in order to effectuate not only this memorandum, but the IT reorganization.

Ms. HERSETH. Do you have any thoughts on any of the recommendations Mr. Brody made in his written testimony that was submitted, most of which I think he also restated in his oral testimony today?

Mr. MCCLAIN. No, I have no comment.

Ms. HERSETH. Would you, if you had more time to consider them?

Mr. MCCLAIN. Perhaps.

Ms. HERSETH. I would then request from the Chairman that perhaps you could submit just any thoughts on those recommendations that he submitted to the Committee, from your experience in the last number of years here as General Counsel, on those recommendations.

Mr. MCCLAIN. All right, certainly.

Ms. HERSETH. Thank you. I yield back.

[The March 16, 2004, memo referred to is attached to Mr. McClain's prepared statement and appears on p. 103.]

Mr. FILNER. Point of order: do we have Counsel here? What is the definition of "contempt of Congress?" Those last two answers were in contempt of Congress, Mr. Counsel. They may not meet strict legal criteria, but—we sat here for two hours, asked questions of experts. They made recommendations but Mr. McClain has "no comment," perhaps he will have something to say later. That is just irresponsible; that is contempt of Congress.

The CHAIRMAN. All right. Mr. McClain, I have a series of questions, and it is going to follow the same lines of some issues Mr. Filner brought up, and in particular, Mr. Michaud and Ms. Herseth. I think I just got it for the first time.

Ms. HERSETH. Yeah, I couldn't——

The CHAIRMAN. I saw you look up. My lisp, I work through it.

Mr. FILNER. Now try Snyder——

The CHAIRMAN. One at a time.

You are Senate-confirmed; correct?

Mr. MCCLAIN. Yes, I am.

The CHAIRMAN. And your title is an Assistant Secretary; right?

Mr. MCCLAIN. No, my title is General Counsel.

The CHAIRMAN. General Counsel, but your equivalent rank is Assistant Secretary?

Mr. MCCLAIN. That's correct.

The CHAIRMAN. Are you a senior government official?

Mr. MCCLAIN. Depending on your——

The CHAIRMAN. Are you a senior government official?

Mr. MCCLAIN. I believe I would—the position would be considered a senior government official. Yes, sir.

The CHAIRMAN. Assistant Secretary. How about what is the next level down? Are they assistant, or are they deputies? Deputy Assistant Secretaries? Are they Senate confirmed?

Mr. MCCLAIN. No.

The CHAIRMAN. So would you say that if you are Senate confirmed, that you would be a senior government official?

Mr. MCCLAIN. Probably. Yes, sir.

The CHAIRMAN. Trying to figure this out. How do you see your role as General Counsel? Are you the VA's chief legal officer?

Mr. MCCLAIN. Yes.

The CHAIRMAN. Okay, and how do you see your role?

Mr. MCCLAIN. My role is the final legal word in the department on legal issues that are brought to our attention, in interpreting laws, and interpreting regulations. I am the counsel to the department, and for the most part I provide counsel to the Secretary, the deputy, and the senior leadership.

The CHAIRMAN. Deputy Secretary—so when you say "to the department," access to you is going to come from the Secretary, the deputy, and the three under secretaries?

Mr. MCCLAIN. When you say "access to me?"

The CHAIRMAN. Yeah, they pick up the phone and you answer?

Mr. MCCLAIN. Yes, sir, they will.

The CHAIRMAN. Okay. At what point does that—I am trying to understand. I don't know the culture, so I am just trying to understand. At what point do you not pick up the phone? In other words, at what level is that at? I don't know.

Mr. MCCLAIN. Well, it——

The CHAIRMAN. Everything has a hierarchy. I just don't know.

Mr. MCCLAIN. Oh, for me in particular, I have an open door policy, so I pretty much answer almost everyone's telephone calls, or——

The CHAIRMAN. Yeah, but you got 400 lawyers out there.

Mr. MCCLAIN. Yes, we do.

The CHAIRMAN. You know, you are responsible for them all.

Mr. MCCLAIN. That's right. We have about 270 in the field, and the others here in Washington.

The CHAIRMAN. How long have you been the General Counsel?

Mr. MCCLAIN. Since April of 2001.

The CHAIRMAN. Who is your client?

Mr. MCCLAIN. The department.

The CHAIRMAN. Who is the department?

Mr. MCCLAIN. Everyone in VA.

The CHAIRMAN. I am trying to figure out meetings for which General Counsel is required to attend. They are what? What meetings are you required to attend?

Mr. MCCLAIN. Pretty much any meeting that is scheduled or called for by the Secretary, Deputy Secretary. Any boards or other type of advisory Committees that I'm on, and can be invited to other meetings in the department that are scheduled by the under secretaries or an assistant secretary.

The CHAIRMAN. Are there lawyers from your team that also would work for the under secretaries? Are there any——

Mr. MCCLAIN. Not directly.

The CHAIRMAN. Not directly, okay. So, the way you just said that, you like having line authority over your lawyers?

Mr. MCCLAIN. Yes.

The CHAIRMAN. Really? I bet the CIO does, too.

Mr. MCCLAIN. Probably does. Not over my lawyers, but over his employees, yes, sir.

The CHAIRMAN. Who in your legal department has responsibility for cyber security?

Mr. MCCLAIN. We have a—I believe it's a GS 15, who is responsible for our cyber security, primarily. But ultimately, I would be responsible for cyber security.

The CHAIRMAN. Giving your reaction to my question—so do you personally and professionally have concerns that the CIO could have enforcement authority over one of your employees?

Mr. MCCLAIN. No, I don't. See, when you say—as it turns out, the initial reorganization that I think was ordered back in 2002, when Admiral Gauss was the CIO, turned out that there were a

few, a small number of employees that were actually transferred to the office of information technology. And my information technology employees were transferred at that time. So we're actually functioning under this program, where they are doing work for us, but they actually belong to the CIO.

The CHAIRMAN. So how does it work that if you have a vulnerability in your legal department, and the CIO, who has only the authority over compliance, he can only ensure compliance, has no authority to enforce anything, he would then have to alert you that there is a vulnerability, and that you then have the authority to cure; is that how it is supposed to work?

Mr. MCCLAIN. Yes.

The CHAIRMAN. Okay. So when the FISMA report says that there are these 16 vulnerabilities, and the VA receives an "F," fails, that then means that three under secretaries received a grade of "F," would it not?

Mr. MCCLAIN. I imagine so, yes. The whole department received a grade of "F."

The CHAIRMAN. Uh-huh. So, given the lines of authority as to who is actually responsible for enforcement, it is hard for me to imagine, as the first panel described, that when you grant responsibility without authority, you are setting a position for somebody to be a scapegoat. I don't see how the CIO could be a scapegoat if they had no authority to enforce. Therefore, there is no scapegoat. There are individuals who are responsible, and the individuals who are responsible also have the authority.

That is what is hard for me in all of this. And it is hard for me when I read your opinions. That is why I called it the heterodox, because it is so incongruent of what we do in our society. Because we have a leadership hierarchy in our society, that someone is responsible, has the authority, and therefore can be held accountable. When I take something out of that, it becomes incongruent, and it defies logic. And it makes it hard for us, then, to operate a system; actually, even to perfect change.

So I have some more series of questions for you. Let me go back to when I mentioned the "F."

As the VA's chief legal officer you are also, are you not, responsible to ensure that the VA is compliant with existing law? FISMA?

Mr. MCCLAIN. I'm responsible for interpreting those laws, and how they apply to our business in the VA. Yes, sir.

The CHAIRMAN. Okay, all right. So, when the FISMA report shows 16 vulnerabilities, and that the department has now received a failing grade, I would say that they are not in compliance with an existing statute. When it comes to you as the lawyer, do you worry about that or not worry about that?

Mr. MCCLAIN. Well, I'm obviously concerned about it, and the question is, is it because there was inaction on the part of certain people? In other words, you would want to look at are we indeed violating a law, or not fully implementing a law?

The CHAIRMAN. All right, if the VA receives a failing grade for their audit, how can that be following the law?

Mr. MCCLAIN. Well, if it's not—if the law itself is not implemented within the department, you have a situation where the law is there and it's not being followed.

The CHAIRMAN. Right. Well, that is what I had back in 1999, when I could not get the VA to create a CIO. You are right, we passed the laws, and we are trying to get the executive branch to implement, to execute.

Does this issue of CIO authority affect the General Counsel's office in terms of control over General Counsel's IT assets?

Mr. MCCLAIN. No.

The CHAIRMAN. Okay. So your concerns are more on the personal side, then? Would that be correct?

Mr. MCCLAIN. You mean for office of General Counsel——

The CHAIRMAN. The office of General Counsel, yes.

Mr. MCCLAIN. My only concern is that I have a good IT network that I can rely on and utilize, and that my people in the field can rely on and utilize. And so, as I said, my employees that I had were transferred over to the CIO. And so we are currently operating pretty well right now under that criterion.

The CHAIRMAN. All right. These memos that the members are discussing, I, in my mind, I have this visual of you conducting a brief with three under secretaries, the deputy, and the Secretary. I don't know, did that ever happen? Or you just send them memos, and people just go about their business?

Mr. MCCLAIN. These particular memos—a memo of this nature would come into the office either as an e-mail request or a written request for a General Counsel opinion on how this particular law applies to this set of facts, whatever it might be. That's pretty much how these opinions were initiated. And the opinion would be worked by staff attorneys, and it would then come up the administrative chain to my office. And the opinion would then be reviewed and signed, and sent back to whoever the addressee is on the memo. In other words, the requesting office. I believe one of them was the CIO, or the assistant Secretary for Information Technology, and the Assistant Secretary for Policy and Planning.

The CHAIRMAN. When you have a dispute between a matter of interpretation of law or regulation between two under secretaries, who is your client?

Mr. MCCLAIN. It is the department. I simply will——

The CHAIRMAN. I don't know what that means. The two under secretaries are part of the department. The two under secretaries disagree on something. How about when the CIO disagrees with the three under secretaries? Who is the department?

Mr. MCCLAIN. Well, they all are. And I don't take sides on it. The question would come to me—we have a dispute, "I think the law should be applied this way, someone else thinks the law should be applied that way, please give us your opinion." And that's what we would do. It may be in the middle somewhere, it may not be exactly either person's position.

The CHAIRMAN. All right, use the word "role." What is the role and responsibility of the Secretary of the VA for information security under FISMA?

Mr. MCCLAIN. He is ultimately responsible for ensuring that there is a system in place that ensures the security and accountability of personal information.

The CHAIRMAN. Okay. And was the Secretary aware of this statutory role and responsibility?

Mr. MCCLAIN. I'm sorry, I'm not sure. I would have to ask the Secretary.

The CHAIRMAN. At any time, were you asked to brief the Secretary with regard to his role and responsibility in this area?

Mr. MCCLAIN. No, sir.

The CHAIRMAN. Okay. All right, let me power through this. Hang in here with me, all right?

The General Counsel memo of August 1 of 2003 on information security to the CIO holds that, quote, "FISMA requires the CIO to develop and implement an agency-wide security program to achieve the purposes of FISMA," end quote. Now that sounds pretty good. But then on the February 19th of 2004 memo, what that meant to your office was explained further. The memo suggests that enforcement language in draft directive 6500 be removed that would allow the CIO to hold individuals accountable to the CIO for noncompliance, and that would establish mandatory penalties. In addition, the memo recommended that language empowering the CIO to mandate budgetary commitments of administrations be removed because, quote, "we are not aware of statutory authority."

[The August 1, 2003, and February 19, 2004, memos referred to are attached to Mr. McClain's prepared statement and appear on pages 96 and 100 respectively.]

The CHAIRMAN. Basically, this leaves the CIO with responsibility, but no real authority to make anything happen. That is what we have been discussing here today. So directive 6500 could have been written, could it not, to have empowered the CIO since you then state that the Secretary could have delegated that authority? Because what you have is first you go, "there is no statutory authority," and the Secretary has the authority. Where was the next step of legal counsel back to the Secretary that says, "Mr. Secretary, you can delegate if you want?" But there was no affirmative action was ever taken.

Mr. MCCLAIN. Well, I understand, Mr. Chairman, where you're going. I think the issue that I would ask is, given our opinion, and given the February 19th, 2004, memorandum, that there is no statutory authority for certain issues—and most of the issues were clustered under security clearance and suitability policies, security matters beyond that of the information and information security, and also personnel matters; human relations and labor-management issues, and the memo. And I'm talking in that memo, subparagraphs—paragraph 2A–1, and then 2A, 2B, C, and D, essentially, in that particular memo.

And what we're saying is entirely consistent with all of the opinions read together, is that the current state of law does not give the CIO these particular powers or authorities. That's what the opinions are, at the point in time on the date that they were issued, what is the state of the law as applied to the set of facts that we were asked to analyze.

The CHAIRMAN. Is it a curious thing that this March 16th, 2004, memo has no subject line? The Secretary's memo, March 16th, 2004, has no subject line. Isn't that a curious thing? Or I'm just being——

Mr. MCCLAIN. I note that it does not.

The CHAIRMAN. You are saying, "Steve, your attention to detail is too great?"

Mr. MCCLAIN. Well, no, I——

The CHAIRMAN. It is not a curious thing, I shouldn't make anything of it?

Mr. MCCLAIN. I——

The CHAIRMAN. Okay, doesn't mean anything?

Mr. MCCLAIN. No, sir.

The CHAIRMAN. All right. Let me go to what you had just stated. I got FISMA right here, okay. And you are right, two lawyers can read something that can totally—we can disagree, we can agree to disagree. But I read this thing differently than how you read it. And I am looking at section 3544, "Federal Agency Responsibilities." Now, you just made an interpretation that says the CIO doesn't have this responsibility, it is not granted to him by FISMA. But when I read this, section 3544–A, "The head of each agency shall"—okay, do you have it right there in front of you?

Mr. MCCLAIN. Yes, sir, I do.

The CHAIRMAN. Okay. See where it says, "A, shall be responsible for," this is list A, B, and C, okay? Number two, it says "shall ensure that senior agency officials provide information security for information and information systems that support the operation assets under their control, including," and goes down a whole list. Who are "senior agency officials?"

Mr. MCCLAIN. Pretty much what we had talked about previously. Under Secretary, Assistant secretaries can be senior agency officials, and it may even go further down, and that's in relation to FISMA, and information security. Yeah.

The CHAIRMAN. When I read FISMA, if I wanted to, I can read this to interpret that only a senior agency official would be an under Secretary, and exclude the CIO. Your testimony to me is that the General Counsel and the CIO is the equivalent of a senior agency official. Now, if I go back and I say, "Okay, I accept your testimony here today that you are a senior agency official, the CIO is a senior agency official, the under Secretary is a senior agency official, and now I read this lot, I don't understand how I can get the interpretation from your memo, doing that." Now, if I want to parse what I read and say that a senior agency official does not apply to what, you and the CIO, then I could come up with that memo, as it has been drafted.

Mr. MCCLAIN. I think the spirit of the opinion obviously is interpreting FISMA. But I think that what's important to realize, and what I get out of this, applying these sorts of requirements to senior agency officials, is that there is a department-wide requirement, and is specially imposed on senior agency officials, to ensure that this system of protection for personal information is in place and operative. It is not giving it or requiring it of a single person, or a single head in the department. It is literally spreading it out and saying, "You're a senior agency official, you have this responsibility."

The CHAIRMAN. The section of FISMA that makes the Secretary responsible for implementation of this statute, 3544, states that the head of each agency shall—and again, I am going to say it—"ensure that senior agency officials provide information security for in-

formation, information systems, the support the operations and assets under their control." Under the Secretary's March 16 memo, assuming that it had been implemented sooner than last October, wouldn't the CIO also fit under these provisions a FISMA? That is what I just asked, because he would be a senior agency official under the authority of 4000 agency employees.

The reason I ask this question, Mr. McClain, is that I have this sense that these memos essentially were efforts to box the CIO.

Mr. MCCLAIN. No, sir.

The CHAIRMAN. Well, that is what has happened by that legal interpretation. You disagree with that?

Mr. MCCLAIN. Yes, sir, I disagree with that. I don't disagree that the CIO perhaps wanted additional authority that was just simply not there in statute, but the opinion is the legal opinion as to what the law provides.

The CHAIRMAN. All right. Why did it take until October 19th of 2005, over a year and a half, for the VA to take just the first step in acting on Secretary Principi's memo? A glacial pace?

Mr. MCCLAIN. Sir, I don't have an answer for that.

Ms. HERSETH. Mr. Chairman.

The CHAIRMAN. Did Mr. McFarland—yes, ma'am?

Ms. HERSETH. Well, before you went too far down this, may I just follow up on a——

The CHAIRMAN. Yes.

Ms. HERSETH. You just stated that the CIO perhaps wanted more authority than your interpretation of the statute allowed; right?

Mr. MCCLAIN. Yes.

Ms. HERSETH. But not too long ago in response to some of the other questions—does your interpretation of the statute, however—I mean, where does the enforcement authority, or the authority that the CIO was seeking resides in the Secretary? Because getting back to this whole issue of what authorities the Secretary could have delegated, I am still trying to figure out, and I think the Chairman was raising this at the beginning of his second line of questioning, when he began again; tell me the distinction between your interpretation of the statute, and the authorities granted to the CIO, versus authorities that the Secretary has that could be delegated. Is there a distinction?

Mr. MCCLAIN. Yes.

Ms. HERSETH. Okay. So I am going to let you explain the distinction, and then re-ask the question that I believe the Chairman did, which is, at what point could you have, or did you communicate with the Secretary about the possibility of delegating some of the authority that the CIO was seeking that the Secretary may have had to delegate, separate from an interpretation of the statute that didn't give, in your opinion, the authorities the CIO was the seeking?

Mr. MCCLAIN. Let me give you one example of some additional authorities that reside in the Secretary that could have been delegated. At the Secretary's discretion, no requirement.

First of all, FISMA requires the CIO to have certain responsibilities and duties and such. The Secretary could delegate further, and if—I would go back to the August, 2003 opinion, which was essentially an opinion on who has authority over the national, versus

non-national type of files, and also physical security versus actual paper, that sort of thing. And the opinion was that as the law currently stood, that authority over the national type of data, if there was any in VA, and physical security, resided in the office of law enforcement, within the department.

Had the Secretary desired to make a change, he could have delegated that authority to the CIO. So there was already something in place.

Ms. HERSETH. I yield back.

The CHAIRMAN. You know I was really concerned when Bob McFarland left. And you are also quite aware of being on the inside of that, you have had three under secretaries that were pretty strong in their opinions. You are also equally strong in an opinion. The Secretary had delegated to the deputy Secretary to work this one, work this issue. And Mr. McFarland was pretty stressed, because he felt that he was not getting a concurrence with his policies.

So let me ask about the directive 6500. Is directive 6500, is it still in a development or a concurrence process?

Mr. MCCLAIN. I believe—and I believe that 6500 is in our EDMS system, Electronic Data Management System—Document Management System. Still, within the office of information technology, for internal concurrence within that office.

The CHAIRMAN. Under your federated approach —I know you don't like the word "box." All right, let me rephrase this. Under your federated model, are your present interpretations that the CIO does not have these lines of authority to enforce, is that what is going to happen in your federated model? You are going to take that present opinion that you have held for the last several years, and apply it to the federated model?

Mr. MCCLAIN. Well, I think several things have changed. One is that this particular issue that we were wrestling with talked about ISOs, and in particular the March 2004 memo from Secretary Principi, I believe was a reaction, as Mr. Brody said, to the Blaster worm situation, where the CIO didn't have control, any sort of supervisory control over ISOs out in the field, and there were over 400 of them.

As of April 30th of this year, with the detailing of personnel into the office of information technology, that situation no longer exists. The CIO has direct supervisory authority over the ISOs, plus the other IT backbone or maintenance type people, even in the field.

The CHAIRMAN. But if I am an under Secretary at the VA, and the CIO is giving me directives on compliance where I am noncompliant in a particular area, and I ignore him, what is the CIO's recourse, legally?

Mr. MCCLAIN. Legally, I'm not sure he has one. Administratively, he should bring this directly to the deputy.

The CHAIRMAN. Yeah, so he has got no authority. How about if I make the CIO, the Committee here decides to follow our instincts of a couple years ago and make the CIO the equivalency of an under Secretary? Does it matter?

Mr. MCCLAIN. In other words, would it change our interpretation of FISMA?

The CHAIRMAN. No, we are going to change FISMA. We are not going to let this stuff happen anymore. We are going to come up with our recommendations to change so they are not subject to interpretation. But if we g+o in and we make the CIO and under Secretary equivalent, and give him lines of authority and the ability to enforce—actually, let us go to the ability to enforce. Would you say that that under Secretary, the CIO then would not have the ability to enforce anything within the jurisdictions of the other three under secretaries?

Mr. MCCLAIN. No, if you passed—if Congress passed a law along the lines that you just outlined, then the law would provide the authority.

The CHAIRMAN. But unless we do that, your position is it is not there; it rests with the Secretary. The Secretary can grant that authority, could he not? He can grant, he can also remove. Secretary can remove certain authorities from the other three under secretaries, could he not?

Mr. MCCLAIN. Yes, he could.

The CHAIRMAN. Ah-hah. Was that ever recommended to the Secretary, or the deputy? That you can remove certain authorities, you can grant authority to the CIO, but—never?

Mr. MCCLAIN. I'm not aware, sir.

The CHAIRMAN. Well, I could see in disciplinary actions a challenge between granting authority or powers to someone who is not of an equal, you know, if they are under the under Secretary. That is what we are going to have to do.

Mr. Filner.

Mr. FILNER. Just a quick question, if I can. Does the VA have a policy of executive bonuses? Bonuses to the senior staff?

Mr. MCCLAIN. Not to political appointees, but to Senior executive service.

Mr. FILNER. Okay, so you don't get a bonus?

Mr. MCCLAIN. No.

Mr. FILNER. So none of the political appointees do?

Mr. MCCLAIN. That's right.

Mr. FILNER. And what is the first level that may get one?

Mr. MCCLAIN. Career, who are SES.

Mr. FILNER. Were those bonuses given last year?

Mr. MCCLAIN. I imagine they were. But I have no personal knowledge of it.

Mr. FILNER. And when FISMA audits gave the department an "F," did you take that in any way personally, or share in that responsibility?

Mr. MCCLAIN. As to the department getting an "F?" I think the entire department has to share in that.

Mr. FILNER. Yes, but personally? Nothing happened to any person as a result? Nobody got pay cuts, or reprimands, or censure, or anything?

Mr. MCCLAIN. Sir, I don't know. I would not normally be involved in that.

Mr. FILNER. But you didn't?

Mr. MCCLAIN. I did not.

Mr. FILNER. I mean, there is simply no accountability here.

The CHAIRMAN. I made a note here, Mr. Filner. When we come back here and discuss how to put together this legislation, Mr. Michaud, that we even should consider writing in our bill, we can seek compliance and say that there shall be no bonuses until the department is compliant with FISMA. If you got an "F," and we are giving bonuses, we shouldn't be giving that. Maybe we can put it on a sliding scale, get them to a "B," you know? You know, I haven't been beyond giving my kids money for a good grade.

All right. I want to thank you for—to my colleagues for being here, and let me just say in conclusion, Mr. McClain, I know you are here today also to defend your legal department and the individuals who wrote these legal opinions. I am stressed by them. I am stressed by them because I think that they were a contributing factor, and we ended up with a legal opinion that I am going to say for the umpteenth time, that is a heterodox opinion, and it was a contributing factor in the face of 16 unmitigated deficiencies, and something has to change.

And we want to work with you. Please let the Secretary know, with regard to the issue that I brought up earlier one when we were asking for that proposal, that it also included insurance. Please let him know that we are going to work cooperatively here, in a bipartisan fashion, to make sure that we hold the Judiciary product until we can let them know that we are going to work in a positive manner, okay.

Mr. Michaud.

Mr. MICHAUD. Thank you, Mr. Chairman.

Just one last question, Mr. McClain. Being legal counsel to the department, and through my experience in the Maine Legislature, where the attorney general offices are legal counsel to State departments, you can take different stances in different areas. Have you, at any time, while we have been dealing with this whole issue of the CIO, given verbal legal advice to the agency that this is the way you saw the law, but you were directed, or asked by a senior official, "I want to do this, can you justify this, as well?" Have you ever taken——

Mr. MCCLAIN. No.

Mr. MICHAUD. No? Okay, thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much. All members will have five legislative business days to submit any statement that they may like. At this point, the hearing is now concluded. Thank you.

[Whereupon, at 2:10 p.m., the Committee was adjourned.]

APPENDIX

Committee on Veterans' Affairs
Congressman Steve Buyer
Academic and legal implications of VA's data loss
June 22, 2006
10:30 a.m.

Good morning ladies and gentlemen. We are here today to receive testimony on best practices from experts in the fields of information security and data breaches. We will also hear from the Department of Veterans Affairs general counsel about the legal implications of VA's information security breach and data loss.

This hearing is part of a series that will help us determine how to correct the problems at the department. We are systematically examining key aspects of the security breach and reviewing the best practices and thinking in the realm of information security.

Last week, we heard testimony from the VA Inspector General and from the Government Accountability Office that provided historical context. The context is sobering: As far back as 2002, the GAO recommended that VA centralize its IT security management functions and establish an information security program.

VA's own inspector general has gone on record with a similar litany of warnings that have been largely, if not completely, ignored.

VA's assistant inspector general for audit told us the IG has reported VA information security controls as a material weakness in its annual Consolidated Financial Statements since the fiscal year 1997 audit. The VA IG's Federal Information Security Management Act audits have identified significant information security vulnerabilities since FY 2001.

A reasonable person might ask what the VA is waiting for . . .

The IG and GAO, our investigations have shown, are not alone in their support for centralized IT management.

On June 8, I held a roundtable with information technology experts from business, including Goldman, Sachs & Company, EMC Corporation, VISA, Citigroup, TriWest and the American Bankers Association. At my invitation, Military Quality of Life and Veterans Affairs Appropriations Subcommittee Chairman Jim Walsh also attended.

These experts offered candid appraisals that emphasized the importance of centralized information security management. None, from a good business sense, could endorse VA's approach – the federated model which *still* allows a significant degree of decentralization.

"I see the federated approach as an excuse for lack of controls," one expert said.

As part of our approach, the Subcommittee on Disability Assistance and Memorial Affairs held a hearing last Tuesday on information security at the Veterans Benefits Administration.

Yesterday, the Subcommittee on Health examined how the Veterans Health Administration maintains security and integrity of the electronic health records of patients.

Both systems face challenges. We are aware of the problems at the benefits administration. The VA IG has testified that at VHA, tens of thousands of veterans' health records have been sent by unencrypted email and were made vulnerable to interception.

Problems with control of access to data, password protection, and even a failure to terminate access for long-departed employees create the conditions for disaster.

The more we learn about the awful *results* of decentralization – in contrast to the bright promises offered by some senior VA officials – the more we see that the system has no departmental standards.

More important, the system – if you call it that – doesn't identify who is in charge of developing policy, implementing policy, or enforcing policy.

It does not have to be this way: today, experts from the academic world will provide insights into cutting-edge information security theory and concepts.

The recent passing of management expert Professor Peter Drucker reminds us that not all expertise is to be found in the world of practice: we have much to learn from those who earn their pay strictly for the work of their minds.

We will then turn to the department's general counsel, the Honorable Tim McClain, who will provide testimony regarding the legal implications of VA's data breach.

I will also be interested in learning more about the legal review process for VA's information security directive for the past three years.

Also, I want to learn more about the adequacy of VA's legal authorities to provide credit counseling and compensation to veterans affected by the loss of their personal information.

Next week, completing this series of hearings, the full committee will receive testimony from former VA chief information officers. Finally, we will hear from Secretary of Veterans Affairs Nicholson and the department's senior leadership with an update on the progress being made at the department.

Please be sure to note these important dates on your schedules.

This weekend, we learned that a laptop, stolen from a contractor working for the city of Washington, D.C., compromised sensitive information on thousands of city employees.

What we are now seeing is that data security has broad implications across the country and across government.

What we would *like to see* is VA moving from "worst disaster" to "best practice."

This is important work and I look forward to today's testimony.

Thank you all for being here today.

Your testimony will help us develop a solution that will ensure the integrity of information security at VA, help veterans who may have become victims of fraud, and potentially help other agencies safeguard against data compromise.

Our first panel includes Dr. Eugene Spafford, Ph.D., who is a Professor of Computer Science, and is the Executive Director for the Center for Education and Research in Information Assurance and Security at Purdue University. Next we have Mr. Bruce Brody,
Vice President, Information Security for INPUT, and
former Associate Deputy Assistant Secretary for Cyber and Information Security with the U.S. Department of Veterans Affairs. Finally, we have Mr. Mike Cook, Vice President of idAnalytics.
I look forward to your testimony.

Panel 2

Thank you for coming. Sitting on our second panel is the General Counsel for the Department of Veterans Affairs, Mr. Tim S. McClain. Mr. McClain was confirmed by the Senate as General Counsel for the Department of Veterans Affairs (VA) in April 2001. As General Counsel, he serves as the chief legal adviser to the Secretary of Veterans Affairs and the department's senior leaders, and manages the Office of General Counsel, which is comprised of nearly 400 attorneys assigned throughout the United States.

Mr. McClain also served as the VA Chief Management Officer from January 2005 to November 2005, responsible for the department's budget, financial policy and operations, acquisitions and material management, real property asset management, environmental policy and business oversight.

Thank you for coming.

If you will please stand and raise your right hand:

> Do you solemnly swear that the testimony you are about to give, including answers to questions of Committee members is the truth, so help you God?

Please be seated. Mr. McClain if you will now provide your testimony.

Closing:

Thank you for your testimony. As a reminder to all, this is the second of several hearings the Committee will hold on the VA data theft and IT security.

All Members will have 5 legislative days to provide opening statements or remarks relating to this hearing. Without objection, so ordered.

Again, thank you all for coming. This hearing is now adjourned.

Full Committee Hearing-Aaron
6/22/2006
10:30 AM

U.S. Congresswoman
Ginny Brown-Waite

Representing Citrus, Hernando, Lake, Levy, Marion, Pasco, Polk, and Sumter Counties

Committee on Veterans' Affairs Opening Statement
Oversight Hearing on Security Breach
6/22/2006
10:30 AM

Mr. Chairman,

Thank you for holding this hearing. I also want to thank all of the witnesses from the academic, legal, and private sectors for appearing today.

I was pleased to hear yesterday that the VA will provide free credit monitoring to veterans impacted by the security breach. However, I fear that credit monitoring alone might not be enough to protect our veterans.

I am interested to hear from today's witnesses about the wide-reaching effects this breach

could have on veterans. Other non-financial areas of their lives could be at risk, from their ability to get a security clearance to future problems during a routine traffic stop.
As Congress explores legislative solutions to this problem, it is imperative that we consider these possible consequences.

The men and women of our armed forces have made substantial sacrifices to ensure that we can all enjoy our freedom. These individuals answered the call in our time of need; it is only fitting that we take care of them in theirs. As members of Congress, we have an obligation to ensure that this happens.

Submit for record

Rep. Corrine Brown
House Committee on Veterans' Affairs
Hearing on the Academic and Legal Implications of VA's Data Loss
Thursday, June 22, 2006, 10:30 a.m.
334 Cannon House Office Building

Thank you Mr. Chairman and Mr. Evans for calling this hearing and working in a bipartisan fashion to get to the bottom of this data theft mess and figure out how to stop it from happening again.

This hearing focuses on the academic perspective of the issue, but we cannot lose sight of the fact that these are not just numbers or figures. These are human beings. People who have served this country and protected its freedoms.

The freedoms that allow business to thrive and technology to make our standard of living so much better, is what is causing so much trouble now.

In yesterday's Health Subcommittee hearing, Dr. Snyder made a good point. Previously, it was hard to get a hold of large numbers of medical records for the simple reason that the paper file was bulky and heavy. Too cumbersome to be of much use to anyone.

When I first came to Congress, the main worry for veterans was how to reconstruct their file for benefits, because much of their military file was lost in the St. Louis fire.

Now we have the file, but must protect what we have from those who would do harm.

We must always remember that these files do not belong to us, or the VA. We are borrowing these files for the purpose of serving the veteran. The VA is only

the custodian of these records. We must do all we can to treat them accordingly.

SILVESTRE REYES
16TH DISTRICT, TEXAS

COMMITTEE ON ARMED SERVICES
RANKING MEMBER
SUBCOMMITTEE ON STRATEGIC FORCES
SUBCOMMITTEE ON READINESS

COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON
TERRORISM, HUMAN INTELLIGENCE, ANALYSIS
AND COUNTERINTELLIGENCE

Congress of the United States
House of Representatives
Washington, DC 20515

WASHINGTON OFFICE:
2433 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4831
FAX: (202) 225-2016

DISTRICT OFFICE
310 NORTH MESA, SUITE 400
EL PASO, TX 79901
(915) 534-4400
FAX: (915) 534-7426

http://www.house.gov/reyes/

STATEMENT OF CONGRESSMAN SILVESTRE REYES (TX-16)

House Veterans Affairs Committee,
Full Committee Oversight Hearing on the Legal Implications of the Theft from a VA Employee's Home of Personal Data Regarding Millions of Veterans, Active Duty Military Personnel, and Spouses

June 22, 2006

Mr. Chairman,

I would like to thank Mr. Spafford, Mr. Brody, Mr. Cook, Mr. McClain, and Mr. Thompson for joining us today. I would also like to thank Chairman Buyer and Ranking Member Filner for scheduling this important hearing.

We are here to discuss the legal implications of the theft of personal data belonging to 26.5 million veterans, active duty military personnel, and spouses. The loss of this information has left millions of people feeling defenseless against the possible trauma of identity theft. To date, the stolen computer containing the personal information has not been recovered.

It has recently come to light that the administration may have had knowledge of this incident for up to two weeks before notifying the FBI and 19 days before notifying veterans. As we are all aware, 19 days is an ample amount of time to wreak permanent havoc upon a person's credit record. Veterans should have been notified of the theft immediately.

Also disturbing is the fact that the VA has taken few, if any, definitive steps in the areas of information technology and security to safeguard our veterans from misuse of their stolen information. Instead, we should be doing everything within our power to reduce veterans' vulnerability and to ensure that this sort of incident does not occur in the future. It is of the utmost importance to protect these men and women, as they fought to protect our country.

This Committee has previously held several hearings on the subject of information security and technology at the VA. We have heard from many key witnesses who have made excellent recommendations about needed improvements.

PRINTED ON RECYCLED PAPER

In the wake of the recent incident, it may be easy to blame the employee who took the laptop home, but it seems apparent that there are also systemic problems at the VA that need to be addressed. Designating a department to be responsible and accountable for the implementation, upkeep, and management of security measures for the VA would go a long way toward preventing future problems.

On June 7, 2006, nearly 150 House Democratic Members sent a letter calling on the President to provide emergency funding to aid the veterans and service members affected by data theft.

Also, to help those affected by this incident and to prevent similar problems in the future, I have co-sponsored H.R. 5588, the Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006, which would provide real security for the military families at risk of identity theft. This bill enacts the following through the VA:

- Free credit monitoring for a year and free credit reports for two years
- Free credit fraud alerts for veterans for one year
- Free credit freeze for veterans for one year
- Increased protection of veterans' sensitive information
- Prompt notification to veterans if their personal information has been compromised by a data breach
- Creation of an Ombudsman for Data Security in the VA who would be responsible for assisting veterans that are victims of a data breach or identity theft

Although it was announced on June 20, 2006, that the VA intends on providing free credit monitoring for the veterans who may have been affected by this incident, it is unclear how the VA will fund this service. Credit monitoring costs approximately $30 per year, and this cost seems unmanageable when you multiply it by 26.5 million.

We need concrete information on that issue, and real solutions about how the VA is going to help those affected by the recent theft while preventing future problems. Every veteran deserves to feel secure, especially where his or her personal information is concerned. It is the least we can do for them, after they have done so much for our country.

Mr. Chairman, again I would like to thank our panelists for sharing their insight into this important matter. I look forward to hearing their testimony.

The Honorable Stephanie Herseth
House Committee on Veterans' Affairs
Academic and Legal Implications of VA's Data Loss
June 22, 2006

Good morning Mr. Chairman. I am pleased we are holding this hearing today to analyze information security, data breaches, and identity risk management at the VA. I want to also welcome the VA and private sector witnesses before us today and thank you for your insightful testimony.

The topic of today's hearing is both critically important and timely given the recent loss of nearly 26.5 million veterans and active-duty servicemembers private information. Indeed, the federal government as a whole and the VA specifically must improve its data security measures and enhance its respect and recognition for citizens' privacy and health information laws.

I am glad that the VA has taken a number of important steps to prevent a similar incident from happening again and has announced that they will provide free credit monitoring to people whose sensitive personal information may have been stolen in the incident. While these are important developments, the VA must take additional aggressive steps to better protect veterans personal information and assist those who have been affected.

After reading the witnesses testimony, and listening to witnesses from earlier hearings about this topic, it appears that the root causes of the poor information security management at the VA are 1) resistance to change by VA central authority and 2) the lack of proper authority by the Chief

Information Officer to enforce information security requirements. I hope that at the conclusion of our series of hearings on VA information data security we will work to implement changes that address these chronic problems.

Chairman Buyer, again thank you for holding this hearing. I look forward to hearing from today's witnesses.

Congressman Tom Udall (NM-3)
House Veterans Affairs Committee
Oversight Hearing on Academic and Legal Implications of the VA Data Loss
June 22, 2006

Mr. Chairman,

It was exactly one month ago today that the VA announced it had lost a massive amount of personal information on 26.5 million veterans. Since then, we have continued to learn more about the information itself, about what led to the loss, about who is responsible, and about what must be done to fix the situation and work toward preventing a similar situation from occurring in the future. The series of hearings held by this committee have greatly helped in the process, and I am particularly looking forward to today's testimony in hopes it will better give us an understanding of exact changes needed in the VA.

Dr. Spafford, your depth of experience in IT security and data management clearly gives great weight to your comments about the problems that led to the VA data loss. Reading through your testimony, I was struck by how the most fundamental lessons of IT security taught to your students were either ignored or unknown to the VA. You state that there were two basic problems in the VA: that there is no centralized and observed, and that no sanctions are imposed when an employee violates security policy, thus creating a climate of contempt for the policies.

The first is an obvious problem which this committee, led by the Chairman and Ranking Member, has strived to resolve. The second is an issue which must be rectified by the Secretary – and we are now learning that the employee who lost this data has not been fired, as was earlier reported, but rather has been proposed for dismissal, a process which continues one month after the data loss.

The testimony of Mr. Brody alleges a "willful disregard for responsible behavior and blatant contempt for established federal security and privacy requirements by senior VA leadership." While there clearly is reluctance, indeed even a culture of aversion, toward change, I am interested to hear further, Mr. Brody, how you perceive the VA leadership approached these areas of concern. Your experience as CISO resulted in questions of authority and centralized control, questions which continue today to the great distress of veterans throughout this country.

Mr. Chairman, I strongly believe that substantial change is needed in how the VA approaches data security, not only through policy changes, but also through attitude and cultural changes. It must be made clear to everyone at the VA from the Secretary on down that this change is needed to help better serve veterans, and this in itself must force the change to occur. As has been mentioned before, this is not a problem faced solely by the VA, and it seems that weekly we are hearing of new breaches of IT security at various government agencies. I greatly hope this series of hearings will shed some light on how the problem can be fixed. Otherwise, we will only continue to see our veterans

compromised by an inattentive, indifferent VA, and that simply cannot occur. Thank you, Mr. Chairman.

Testimony before the House Committee on Veterans' Affairs
Hearing on
"Oversight Hearing on the Academic and Legal Implications of VA's Data Loss"

22 June 2006

Statement of
Eugene H. Spafford

Professor and Executive Director
Purdue University Center For Education and Research in Information Assurance and Security (CERIAS)

Chair of The U.S. Public Policy Committee
of The Association For Computing Machinery (USACM)

Member of the Board of Directors
of the Computing Research Association (CRA)

Introduction

Thank you Chairman Buyer and Ranking Member Evans for the opportunity to testify at this hearing.

By way of self-introduction, I am a professor at Purdue University with a joint appointment in the department of Computer Sciences and the school of Electrical and Computer Engineering. I also have courtesy appointments in the departments of Philosophy and Communication. I am also the Executive Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we have a set of affiliate university programs working with us in a number of states, including Iowa, North Carolina, the District of Columbia, Ohio, Virginia, Idaho, and New York. CERIAS also has a close working relationship with a dozen major commercial firms and government laboratories.

In addition to my role as an academic faculty member, I also serve on several boards of technical advisors, and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I was a member of the most recent incarnation of the President's Information Technology Advisory Committee (PITAC) from 2003 to 2005. I have been working in information security for 25 years.

I began this document by listing my affiliations with ACM and CRA. This testimony is not an official statement by either organization, but is consistent with their overall goals and aims. ACM is a nonprofit educational and scientific computing society of about 80,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. The Computing Research Association is an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is particularly interested in issues that affect the conduct of computing research in the USA.

The Nature of the Problem

We are here as a result of a significant breach of security and privacy at the Veterans' Administration reported in May of this year. The theft of a computer system may have revealed personal details of several million veterans and active-duty military personnel. This incident exposes those personnel to an increased risk of identity theft, credit fraud, and other criminal activity.

Identity theft, coupled with the general lack of accuracy and data provenance[1] tracking of large databases by government and industry, means that those individuals' good names and records may be besmirched by people who misuse the exposed personal information. This is a special risk for some of our active-duty personnel and veterans because they may find themselves denied security clearances through no fault of their own. Another possibility is that they will find their names added to the TSA's "No Fly" list because someone else has misused their identity.

This problem is not unique to the VA, however. A recent article in Computerworld[2] stated that since the start of 2005 there have been nearly 200 computer security breaches resulting in significant disclosures of personal information. Nearly 90 of those incidents have occurred this year, and the total number of records disclosed by all those incidents exceeds 88 *million*. What is more, those are only the *detected and disclosed* incidents; it may well be the case that several times that many incidents have occurred.

For decades, professionals in the field of information security have been warning about the dangers of weak security, careless handling of data, lax enforcement of policies, and insufficient funding for both law enforcement and research. Our warnings and cautions have largely been dismissed as unfounded or too expensive to address. Unfortunately, we are seeing the results of that lack of attention with incidents such as what happened at the VA. In addition we have seen new levels of sophisticated computer viruses and spyware, increasing cyber activity by organized crime, and significant failures of security across a wide variety of public sector entities and government agencies, including the Department of Defense.

I will not go into depth about the failures at the Veterans' Administration that led to this particular incident. Your committee has been conducting an investigation of the factors underlying those failures, and the testimony so far appears to be exposing those problems.

I will make special note of two information security failures present in this case, however, that I have seen time and time again in government, industry, academia and elsewhere. I often refer to these problems when I teach the basic information security classes at Purdue; I will now be able to associate these with the May VA incident as a specific example.

1. There is no centralized point of authority to ensure that rules, procedures and good practices are instituted and observed. There are good people at the VA who understand what needs to be done, and many of them try to do the right thing. However, there is no centralized position that has all three components necessary to effectively manage information security: resources, accountability, and authority. There should be a CIO or CISO (Chief Information Security Officer) who has adequate funding and trained personnel to carry out a comprehensive security plan. That office (and management above

---

[1] Data provenance is the labeling of data with information about where it came from, where it has been copied, and details about how it was derived. This can be used to determine if the data is accurate, or from whence errors might have been introduced.

2 June 20, 2006 article: "Flurry of New Data Breaches Exposed," by J. Vijayan and T. Weiss.

it) also must be held accountable for failures to satisfy necessary standards and successfully pass audits. Last of all, that same office must have authority to make changes, shut down systems (if necessary), and terminate employees for cause. Accountability without authority means the position is simply a focus for blame when failures occur; authority without resources means that only limited organizational problems can be fixed; and resources without accountability may simply lead to fraud, waste and abuse.

2. An employee or contractor makes an arbitrary decision to violate security policies so as to make his job easier. This is done without understanding why the policy is structured as it is, and without understanding the potential consequences of the violation — until it is too late, if even then. Unfortunately, we see this happening all the time, and it is usually the case that – even if detected – no sanctions are imposed so long as the work gets done and nothing untoward appears to happen. This builds a climate of contempt for the policies, and the mistaken belief that end-users are capable of making policy decisions involving enterprise security. If something untoward does happen, often the guilty parties are scolded, but nothing further occurs: an attitude of "failures are commonplace" overrides any thought of holding guilty parties fully accountable.

There are other information security problems at the VA and elsewhere in the government, which were not directly involved in the May disclosure incident. It is beyond the scope of this hearing and this testimony to document and describe all of them. It is also beyond the scope of this testimony to summarize the magnitude of cyber threats currently facing our information infrastructure, including the Veterans' Administration. There are many reports describing these threats, including reports from the PITAC, the GAO, the National Academies, the Department of Justice, and many commercial entities. From these reports the following general trends may be derived:

- The number of reported attacks of various kinds is increasing annually;
- Attacks are becoming more sophisticated and more efficient;
- Few perpetrators are ever caught and prosecuted;
- An unknown (but probably large) number of attacks, frauds and violations are not detected with current defenses;
- A large number of detected attacks are not reported to appropriate authorities;
- The problem is international in scope, both in origin of attacks and in location of victims;
- The majority of the attacks are enabled by faulty software, poor configuration, and operator error.

Undoubtedly the magnitude of the problems are greater than have been reported, and more has occurred than has been detected. Regrettably, I believe the situation is going to get worse because the problems have been ignored and neglected for too long to be quickly remedied.

As a long-time educator and researcher in this field, I can state that my peers and I can offer few immediate solutions. Although we have several good programs at colleges and universities across the United States, we are producing too small number of students to meet the demand. In part, this is an issue of enrollment, as nationally we do not get enough good students seeking de-

grees in the area. We also have only a small number of programs involved in training of practitioners, and even fewer that are involved in quality graduate education and research.

Exacerbating both of these problems is a lack of resources. Outside of a few underfunded programs through the NSF that award competitive grants to faculty, and a few Congressionally-directed allocations to some university projects around the country, there is almost no funding for basic research, capacity development, or infrastructure acquisition for programs in information security; as an example, CERIAS at Purdue is the nation's leading center in multidisciplinary information security research and education with over 80 faculty, and it has never received any government support (although some individual faculty have received funding from agencies such as NSF for their individual research). As is the case with many of our peer institutions, our ability to make progress in education and research is limited mostly by lack of resources.

Some Recommendations

In February 2005, the President's Information Technology Advisory Committee issued a report, based on hearings and considerable study by many experts. That report was entitled Cyber Security: A Crisis of Prioritization.[3] It described the nature of the problems with cyber security and some of the trends. It also analyzed the (inadequate) Federal response to those challenges. It outlined, in some detail, an agenda to begin to address some of our cyber security problems. The response to that report was that action was only taken on one of the four recommendations, and the PITAC was disbanded.

I encourage members of the committee to carefully read the PITAC Cyber Security Crisis report. I participated in the research and writing of that document, and it goes into considerable detail on the problems and issues behind our cyber security deficit, as well as making some concrete suggestions of how those issues might be addressed.

I also suggest that the committee might find my testimony to the House Armed Services Committee on October 27, 2005 to be of interest.[4] The topic was ""Cyber Security, Information Assurance and Information Superiority." In it, I discussed cyber threats to US systems, and I also outlined some suggestions for how those threats might be mitigated.

Last of all, I have included a set of recommendations from the ACM US Public Policy committee regarding privacy of personal data. There is no comprehensive privacy legislation in the US as there is in many other countries. This has led to an *ad hoc* approach to privacy regulations in government and in the commercial sector, which in turn has enabled many of the abuses and disclosures we have seen recently. It is difficult to create a culture of protection of personal data when privacy is treated as an afterthought, and when frequently it is seen as appropriate to circumvent privacy protections to reduce cost or effort. Thus, as you consider what changes at the

---

[3] Available online at <http://www.itrd.gov/pitac/reports/index.html>.

[4] Available online at <http://homes.cerias.purdue.edu/~spaf/usgov/newHASC.pdf>

VA might improve cyber protections for the data on our veterans, you might find these recommendations by the USACM to be of value.

Specific Q&A

The committee did not pose specific questions for me when I was invited to appear.

This concludes my written testimony. I will be pleased to provide additional information if requested.

USACM

The Public Policy Committee of ACM

USACM Policy Recommendations on Privacy

June 2006

BACKGROUND

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data — including copies of video, audio, and other surveillance — needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Committee of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

RECOMMENDATIONS

MINIMIZATION

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.
5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (*opt-in*); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (*opt-out*). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)
7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.
15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.

16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.
23. Maintain *provenance* — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de-identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in identifying experts and applicable technologies.

For more information about USACM, please contact the ACM Office of Public Policy at (202) 659-9711 or see <http://www.acm.org/usacm/>.

Statement for the Record of
Bruce A. Brody, CISSP, CISM
Vice President, Information Security, INPUT
Before the
Committee on Veterans Affairs
U.S. House of Representatives

June 22, 2006

Mr. Chairman, Ranking Member Evans, and Members of the Committee. My name is Bruce Brody. As a veteran, I am very thankful for the opportunity to address this distinguished Committee today.

I am the Vice President for Information Security at INPUT, a market research firm based in Reston, Virginia. From 2001 to 2004, I was the Associate Deputy Assistant Secretary for Cyber and Information Security at the Department of Veterans Affairs, and from 2004 until January of this year, I was the Associate Chief Information Officer for Cyber Security at the Department of Energy. I believe I am the only person ever to have served as the Chief Information Security Officer (CISO) at two Cabinet-level Departments.

During the period from 2003 until my retirement from federal service early this year, I served as a member of the Information Security and Privacy Advisory Board, created by Section 304 of the Federal Information Security Management Act of 2002, to advise the National Institute of Standards and Technology, the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to federal information systems. In that capacity, I gained very broad insight into the information security and privacy practices of many federal agencies. I would also note that my federal service was interrupted by a three-year stint in private industry where I gained a lasting appreciation for the practical application of risk management principles in dealing with security and privacy issues.

My position at INPUT affords me the opportunity to provide neutral analysis and insights to nearly 1,200 corporations concerning information security developments in the federal government. I do not work for any federal customers. In recent months, I have also been approached for dozens of interviews to the media concerning the flaws of

the Federal Information Security Management Act (FISMA), the challenges of implementing Homeland Security Presidential Directive 12 (HSPD 12) and the loss of private information that was in the custody of the Departments of Veterans Affairs and Energy. I am hopeful that I can provide this Committee with some background, details and personal perspectives to assist in bringing this unfortunate incident to some degree of resolution.

In my summary remarks, I provide an overview of my experiences with the Department of Veterans Affairs that form the basis for several recommended corrective actions for this Committee to consider. I realize that not all of these corrective actions are within the purview of this Committee, but I am confident that your colleagues in other committees will realize the need to act.

Like members of this Committee and my fellow veterans, I view the loss of the personal information of more than 26 million veterans as willful disregard for responsible behavior and blatant contempt for established federal security and privacy requirements by senior VA leadership. While I doubt that my personal information was compromised in the recently-disclosed loss of information from the Department of Energy, I empathize with the hundreds of individuals holding security clearances who are only now learning that their personal information was compromised.

I urge this Committee to look carefully at the following factors, which I believe contribute to the decades of information security and privacy neglect at the Department of Veterans Affairs that have been documented by the Inspector General and the Government Accountability Office.

First and foremost, someone with the appropriate substantive expertise has to be empowered to set and enforce privacy and cyber security requirements, to include the physical security requirements for how such records are maintained and the personnel security requirements for whom access to such records is allowed. It is my recommendation that this Committee legislate the requirement for someone to function in the private sector role of a Chief Security Officer, possibly with the title Undersecretary for Risk Management.

The responsibilities of the Chief Security Officer would be to directly advise the Secretary concerning information, physical and personnel security, privacy, and other risks to VA information, facilities, resources and the veterans whose interests VA must protect. The position must be equal in stature with the Administration Undersecretaries and, under the supervision of the Secretary and with congressional oversight, would promulgate security and privacy policies across the Department, enforce accountability for compliance, oversee implementation of remediation strategies for removing identified shortfalls and coordinate the Department's budget related to these issues.

When I was first introduced to this Committee as the new VA CISO in April 2001, I thought that the Secretary had hired me for the purpose of implementing effective cyber security controls. However, I learned over time that the apparent authorities invested in the CIO in the Clinger Cohen Act and the Paperwork Reduction Act, and in the CISO in Computer Security Act of 1987, the Government Information Security Reform Act of 2000 and finally in FISMA, were not accepted by VA or its leadership.

I quickly learned that the Department's Chief Information Officer (CIO) only had authority to "advise, encourage, support and persuade" the Administrations insofar as information technology programs were concerned. In addition, I learned that the CIO had no authority to "direct" compliance with – at that time – the Paperwork Reduction Act. These points were captured in a memorandum from the Assistant General Counsel dated October 6, 2000.

Difficulties with this "advise, encourage, support and persuade" approach to the CIO's management authority were raised at a March 12, 2002 Oversight Committee hearing by both Chairman Buyer and Ranking Member Carson who questioned the ability of the then-CIO to get the job done without "line authority." Later that year, Secretary Principi took actions to direct the centralization and enhanced line authority of the CIO function, presumably acting at least in part on the recommendations of this Committee. Unfortunately, the Secretary's direction met with bureaucratic inertia and cultural resistance and was never fully implemented.

For many decades, the culture of the VA has been one that enables and promotes fierce resistance to change, stiff opposition to central authority and active refusal to adopt

best security practices. In my three and a half years at the VA, I faced these chronic issues on a continuous basis. Whenever a security initiative was introduced, it was common practice for the Administrations and Program Offices to resist, impede and obstruct the initiative both to prevent any diminution of local authority and to interfere with anything other than business as usual.

Subsequent to my arrival at the VA, the Government Information Security Reform Act (GISRA), followed by the Federal Information Security Management Act (FISMA) were enacted in 2000 and 2002, respectively. Not being an attorney, I cannot offer legal opinions about what the words of those statutes mean. I can only apply common sense to the purpose of these important pieces of legislation. It seemed to me that if, after all was said and done, the opinion of the Assistant General Counsel issued in October of 2000 was correct, then the Congress went to nonsensical amounts of effort to produce the legislation and provide such details concerning specific responsibilities.

It became all the more apparent that clarification was needed following the MS Blaster malicious software incident in the second half of 2003.

In advance of what proved to be the serious malicious software attack represented by MS Blaster, my office provided the necessary alerts, and also distributed notification concerning the necessary patches throughout the VA enterprise. These alerts were widely ignored, and VA networks were savaged as a result. The ensuing recriminations included a review by a medical doctor in the Veterans Health Administration (VHA) who was supposedly renowned for conducting root cause analyses. His analysis of this incident concluded that the CIO's Office was at fault for not convincing the Administrations and the Program Offices that we were really serious when we told them to install the required patches to mitigate the attack.

Thereafter, the Office of Inspector General became heavily involved in criticizing the absence of common security controls as well as the recommended configuration control board structure of NIST Special Publication 800-40. The OIG mistakenly pointed at the Office of the CIO as the responsible office for those deficiencies.

From my perspective, these negative accusations did not compute. The apparent authorities invested in the CIO in the Clinger Cohen Act and in the CIO and CISO in

FISMA did not seem to be accepted by VA or its leadership. As a result, I concluded that there was no longer any point in attempting to introduce cyber security changes in VA unless there was a clear statement of authority to do so. That was when I requested the General Counsel opinion about FISMA authorities for the CIO/CISO.

Just prior to the MS Blaster attack, I had requested a clarification from the General Counsel concerning the responsibilities of the CIO under FISMA for national security and non-national security information and information systems. In a memorandum signed by the General Counsel on August 1, 2003, it was reinforced that the various security functions of the Department, specifically information security, physical security and personnel security, would remain under the authority of their respective offices. According to the memorandum, the CIO was allowed to issue policies pertaining to information security, but the daily operations of security clearance determinations, investigations, physical storage and related activities were not to be placed under the purview of the CIO.

Subsequent to the MS Blaster attack, I requested a clarification from the General Counsel concerning the authority of the CIO to enforce compliance with security legislation and regulations. In a memorandum signed by the General Counsel on April 7, 2004, it was asserted that the CIO cannot order or enforce compliance with information security requirements. Because FISMA used the word "ensure" instead of "enforce" the General Counsel stated that the only recourse for the CIO when a security requirement was violated was to complain to the Secretary.

The result of these two opinions was extremely unfortunate for the Department. In effect, the first of these memos fragmented security authorities and the second said that the CIO had no authority to enforce policies or hold people accountable for violating policies. These memos accurately captured and reinforced the culture of the Department, where resistance to central authority and maintaining the historical 'norm' of doing business according to hundreds of different local practices have always been the practice. In day to day operations, these memos ensured that the fragmentation of security authorities enabled the lack of background investigations for individuals with access to VA networks, systems and resources; the unchecked access to VA information by foreign corporations and foreign nationals; limited to non-existent logical and physical access

controls for major medical systems; the disruption and denial of service from malicious software attacks such as MS Blaster in 2003; and hundreds of other negative information security findings as highlighted in the reports of the independent public auditor, Inspector General and Government Accountability Office.

I would ask the Committee if it agrees that the Clinger Cohen Act and FISMA do not require the Secretary, CIO and CISO to set and enforce the security requirements of the FISMA legislation. I would also ask the Committee if it agrees with the opinions of the VA General Counsel.

If you accept the legal opinion of the VA General Counsel, then the Secretary, Deputy Secretary and Undersecretaries are the only officials who had the authority to implement and enforce the policies, procedures, accountability and culture that would have prevented the loss of the 26 million records that bring us together today. I would be quite surprised if that position regarding responsibility for information security oversight was part of the Secretary's in-briefing to the Department.

If, as I suspect, the Committee does not agree with the VA General Counsel, then corrective action must follow. If FISMA and the Clinger Cohen Act do not convey the authority and accountability for enforcing security and privacy requirements, perhaps the Congress needs to amend these bills to so state. My personal experience is that the mismatch of authority and accountability for the CIO and CISO affects other departments and agencies to the same extent that it affects the VA, and I encourage legislative action to clarify this situation and possibly prevent more serious incidents from occurring.

But the bottom line for the VA was that the two General Counsel memos reinforced the VA culture, and the VA culture is the root cause of this problem. The VA culture can be highlighted even further in the paper trail of non-concurrences on VA Directive 6500, Information Security Program.

My second recommendation is that policies, procedures and assignments of accountability regarding security and privacy issues cannot be held hostage to the individual interests of the senior officials whose concurrence must be obtained prior to review by the Secretary. In this regard, I invite the Committee's attention to the paper trail of non-concurrence on Draft VA Directive 6500, Information Security Program.

Draft VA Directive 6500 represented the effort of my office to modernize a 1999 VA information security and privacy policy. Following extensive discussions with the Office of Inspector General and GAO auditors, VA Directive 6500 was intended to put in place the necessary policy to reduce security vulnerabilities; remove the causes of negative IG, GAO and independent auditor findings, including the information security "material weakness"; comply with all FISMA and Privacy Act security and privacy requirements; and establish a means for enforcing accountability for non-compliance with the policy.

The MS Blaster experience and VA Directive 6500 drafts are the quintessential VA examples of the lack of accountability and the culture of obstructionism. The concurrence process for VA Directive 6500 became a frustrating, albeit illuminating, exercise in forcing the Administrations to put into writing their individual positions on information security fragmentation and the CIO's authority. The Committee's attention is invited to this paper trail in order to witness first-hand the culture of resistance that is at the heart of the current incident.

On January 16, 2004, VHA non-concurred on VA Directive 6500, disagreeing with a blanket approach to background investigations, opposing any requirement to ensure that corporations having access to VA systems and data be American-owned – in other words, subject to U.S. laws and within the reach of U.S. courts if U.S. laws were breached. VHA also opposed any requirement that visitor personnel be escorted at VA facilities and resisted the ability of the ADAS for Cyber and Information Security to establish mandatory penalties for non-compliance. On January 23, 2004, the Acting Assistant Secretary for Policy, Planning and Preparedness non-concurred with the Directive, providing the ill-informed statement that information does not lend itself to the oversight and management of one organizational entity, and further emphasizing the need to keep fragmented the security disciplines of cyber security, information security, information management, physical security, enforcement authority, continuity of operations and personnel suitability and security. On February 19, 2004, the General Counsel non-concurred on the Directive because it failed to clarify the "limited" role of the CIO, and it reiterated that the CIO could only "ensure" and not "enforce" compliance.

The General Counsel further instructed that language be removed that pertained to the CIO holding people accountable for non-compliance.

The memos by the General Counsel and the paper trail of non-concurrence on VA Directive 6500 are indicative of a culture of resistance to central authority and refusal to accept anything other than business as usual. They also highlight the decentralized authority enjoyed by the Administrations and Program Offices, who are empowered to define the role and authority of the CIO as they see fit in order to perpetuate their parochial interests. Most of all, these documents make it clear that the CIO and the subordinate CISO have no authority to do anything other than issue policies, but on top of that, they can only issue policies that the Administrations and Program Offices allow them to issue through the concurrence process. Once issued, the CIO and CISO have no authority to enforce the watered-down policies that they are permitted to put into place.

As a third recommendation, let me suggest to you that the CIO budget, including cyber security and privacy budgets, cannot be held hostage by the Administrations and Program Offices. Since funds are not directly appropriated to the CIO by the Congress, security and privacy initiatives depend on the funding support of the very offices that have historically been the cause of the problems being addressed.

During the Fiscal 2004 budget year, the Administrations held hostage the budget of the Office of Cyber and Information Security subject to a review by low-level field personnel who, in some instances, were significant violators of cyber security practices. Final funding release was not granted until late June 2004, leaving only the final Fiscal Year quarter to execute a substantial portion of the entire year's budget.

Fourth, I recommend you create a legislative requirement that would suspend all executive and senior bonuses in the VA until the environment for which the executive is responsible receives a clean bill of security health from the IG and the competent senior official placed in charge of security. Here again, the Committee will find an illuminating paper trail concerning the efforts of OCIS to implement mandatory Senior Executive Service performance appraisal criteria, which, although approved by the Secretary, could not be effectively enforced.

Fifth and finally, the Committee needs to look very closely at the workforce mix in the critical area of privacy, cyber and information security controls. The Committee has been dealing with issues pertaining to the culture of the VA on numerous occasions over the past decade. It is truly unfortunate that it takes another crisis to highlight the continuing need for culture change at the VA. I am not optimistic that the VA culture will change, nor am I optimistic that this incident will be the last of its kind at the VA.

There are more than 26 million veterans and active duty personnel who are uncertain if the loss of their personal information will bring them financial harm. These veterans deserve better, because they have served our country well. Unfortunately, the VA has not served them well, and the VA must make the necessary amends. If the VA cannot reinvent itself and change its culture dramatically, then I would beg the Congress to do it for them, and to do it for our nation's deserving veterans.

Toward that end, I note that it has been the policy of the VA over the past few years to replace contractor staff with full time VA employees. Since cyber and information security is a very dynamic field of expertise where static approaches will inevitably be overwhelmed by rapid advances in attack methodology, regular technology enhancements are essential. The agility, training and expertise to implement these new technologies will be difficult to achieve with a workforce governed by federal personnel processes and regulations.

As a veteran, my heart goes out to our war wounded, those who have sacrificed so much to keep us free and safe. I would encourage this Committee to develop programs that help those war-wounded to transition into such highly specialized high technology occupations.

Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.

Written Testimony of ID Analytics Corporation

Oversight Hearing on the Veterans Affairs Data Breach

Washington D.C.
June 22, 2006

Chairman Buyer, Ranking Member Evans, and distinguished members of the Committee:

Thank you for inviting ID Analytics to testify on ways to help victims of the recent Veterans Affairs data breach.

My name is Mike Cook. I am a Co-Founder of ID Analytics, a San Diego-based company focused exclusively on stopping identity fraud. I have worked in the field of credit risk and fraud prevention for 20 years

ID Analytics helps stop identity fraud through our ID Network, a real-time identity fraud prevention system formed through a consortium of leading companies dedicated to protecting their customers from identity fraud. Our ID Network gathers information from applications for credit, change of address, and other identity risk information from companies including half of the top ten US banks, almost all major wireless carriers, and a leading retail credit card issuer. Hundreds of times each day, our technology helps stop fraudsters from obtaining credit, services and merchandise in innocent consumer's names. We think it's important to make you aware that ID Analytics does not market or sell the data we collect in the ID Network for any purpose, to anyone.

I am here today because ID Analytics has unique expertise and knowledge of data breaches and their risks. To date, we are the only public or private entity that has studied the harm resulting from actual data breaches. Should any Committee member have interest, I would be happy to provide a copy of our White Paper analyzing the harm from

four actual, well publicized data breaches involving more than 500,000 breached consumer identities.

I would first like to put this breach into context. At this point, no one knows the scope of risk veterans are facing. The most dangerous data breaches are targeted thefts, where the thief committed the breach solely for the purpose of taking consumer data. In this case, the purpose of the theft is unclear. Was the thief targeting a laptop or the data held on it? I don't believe we know that answer today.

If the data is misused, we can expect it to be misused in the following ways:

- It is likely the fraudsters will mainly attack the credit card industry. Stolen identities are an asset, and sophisticated fraudsters can get the best rate of return by fraudulently obtaining credit cards and then making fenceable purchases.
- Because the file contains so many identities, it is likely that the fraudsters will use the stolen identities once or twice and never again to increase their approval rate. Low use rates of individual veteran identities will make detection more difficult for the lending community.
- Again, *if* the data is misused, sophisticated fraudsters will spread the misuse of the identities across differing locations within a city or even across different states to avoid detection.

The worst case scenario is that the Veterans file finds its way to a public distribution source, such as the Internet. If this happens, the stolen identities will lose their connection to the VA data breach and groups of

fraudsters might actively trade that data among the fraud community. Subsequently, more people might have access and could misuse those identities on a grander scale. We know from additional research conducted this year that the misuse rate of data traded on the Internet can climb substantially and exceed the average rate of identity theft of 1.5%.

Some consumer advocates estimate that the value of a stolen identity ranges from $25 to $75 depending on the available personal information associated with that identity. So, because of the value of the data itself, wide distribution should be a concern, and should drive a real sense of urgency to try to recover the stolen data back as fast as possible.

So, what can the VA do now?

Over the course of the last year, ID Analytics has developed breach monitoring technology. With this technology, the VA can answer three essential questions about the data breach

1) Is the breached data being misused by fraudsters today?
2) If it is being misused, can we identify the specific veterans harmed by this misuse and provide them with additional victim assistance?
3) If the breached file is being misused, at what locations are those breached consumer identities being misused so that law enforcement can stop the misuse and potentially acquire back the breached data file?

How does this technology work? Simply put, when thieves use a breach file, they leave tracks. In order to obtain credit or other goods in a

veteran's name, a fraudster would have to manipulate that veteran's identity information on a new account application. For instance, if a fraudster applies for a credit card in a veteran's name, the fraudster needs to change the address (so he or she can collect the new credit card from the bank). The fraudster will change the veteran's phone number for personal and employment verification purposes. He or she may use these same addresses and phone numbers to commit identity theft against other identities that were part of the same breach. Our ID Network, which receives hundreds of thousands of applications and other identity risk events per day, can identify these types of anomalous changes and relationships across a breached file, regardless of the size of the breached file.

We believe this technology can be significant to the Department of Veterans Affairs for the following reasons:

- It can help identify any organized misuse of the personal data that has happened so far;
- The analysis can quickly identify veterans who may have been victimized so that additional victim assistance can be expedited to them;
- It can actively monitor the file for possible misuse;
- This technology can help provide law enforcement a way to identify those individuals who have either stolen the file or have misused it to commit identity theft, to stop further misuse and to recover the lost file;
- The analysis can help determine if the file is in use by more than one individual (or one cohesive group);

And finally, breach monitoring provides a deterrent effect once publicly announced. Thieves should be aware that if they try to misuse any data from the VA data breach, they do so at their own peril.

Thank you again, Mr. Chairman for the opportunity to present this testimony.

Mike Cook, co-founder, ID Analytics
Mike Cook co-founded ID Analytics in March 2002. Cook has spent 20 years in risk and fraud-related roles and half of that time in senior executive positions at various companies. Since joining the company, Cook has conducted extensive research on the methods and schemes of fraudsters, resulting in the development of industry-standard solutions that combat the most difficult-to-detect types of identity fraud. Frequently quoted in the media, Cook has authored the National Fraud Ring Analysis, the first National Data Breach Analysis and is invited to present at a variety of events.

About ID Analytics
Established by a team with deep experience in fraud prevention, ID Analytics is the Identity Risk Management Company. ID Analytics helps its clients spot identity risk at any point in the customer lifecycle and determine the next best step in verifying an identity using the ID Network™, the first and only national system developed exclusively to manage identity risk.

Today the ID Network is in use by companies representing over half the credit and retail card market in the US, as well as leading wireless, retail bank and online consumer finance companies. ID Analytics has also expanded into Europe where it has co-invested with industry leaders to examine regional identity fraud and develop customized solutions for that market. Unlike traditional fraud prevention techniques, ID Analytics' ID Network approach empowers organizations in both the US and UK to stay up-to-date and combat new and emerging challenges associated with identity fraud.

Awards and Testimonials

- Heralded "Top 10 Technology Companies to Watch" by Bank Technology News
- Awarded "Most Outstanding Emerging Growth Company" by the San Diego chapter of the American Electronics Association (AeA)
- Won "Breakthrough Innovation in Information" at the San Diego T-Sector's annual InFusion Awards
- Deemed "Cool Vendor" by Gartner Group
- Named Most Innovative Product Award Finalist by the University of California, San Diego (UCSD) Connect
- Winner of San Diego AeA's Annual High Tech Awards in the Technology and IT Services category

At this time, ID Analytics does not conduct any business with government.

STATEMENT OF
THE HONORABLE TIM S. MCCLAIN
GENERAL COUNSEL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
JUNE 22, 2006

Mr. Chairman and Members of the Committee,

I am pleased to be here this morning to discuss certain legal implications of the May 3, 2006, theft from a VA employee's home of personal-identifying information concerning veterans, service members and some spouses.

As you are aware, three class-action lawsuits have been filed alleging that the Department has violated the Privacy Act and the Administrative Procedure Act in the theft of these records. Two of the lawsuits name as defendants, in their individual capacities, the Secretary, the Deputy Secretary and the employee from whose home the records were stolen. The lawsuits seek amounts that could total billions of dollars from the United States because of this theft. Because of those pending lawsuits, it would be inappropriate for me to discuss how the relevant laws apply to the facts giving rise to those suits.

Legal Aspects of the Data Loss

The Privacy Act applies to individually-identified records, such as those stolen on May 3, about individuals that the Agency retrieves by the names of those individuals, regardless of the storage media used to maintain the records. The BIRLS database involved in the VA data loss is an example of an electronic, Privacy Act-protected set of records.

The Federal Information Security Management Act (FISMA) applies to Federal information and information systems, including systems operated by VA contractors.

Both the Privacy Act and the Federal Information Security Management Act provide a framework for establishing agency safeguards to ensure the security and confidentiality of records. These statutes generally outline agency responsibilities and do not address the duties and responsibilities of individual Government employees except as to the willful and intentional disclosure of Privacy Act-protected information.

The HIPAA (Health Information Portability and Accountability Act) Privacy and Security Rules do not apply to the stolen data. Within VA, only the Veterans Health Administration is an entity covered by the HIPAA Privacy and Security

Rules. The data involved in the loss all either came from Department of Defense personnel records or were created by VBA as part of its claim adjudication process. It is our opinion that these are not activities covered by the HIPAA Privacy Rule.

Legal Aspects of Federal Information Security Management

Under the Federal Information Security Management Act (FISMA), the Secretary must provide protection from "unauthorized access, use, disclosure, disruption, modification or destruction" of VA information and information systems by:

(1) complying with information security standards required by law, the Office of Management and Budget (OMB), and, as to national security information and information systems, the President;

(2) requiring VA "senior agency officials" to provide security for their information and information systems, in accordance with the FISMA-mandated risk analysis process;

(3) creating, through the Chief Information Officer (CIO) and senior agency information security officer (ISO), an agency-wide information security program, conformance with which shall ensure that the information security standards are met and the risk analyses are performed;

(4) providing for sufficient personnel trained in information security requirements; and

(5) requiring annual reports from the CIO "in coordination with other senior agency officials."

FISMA requires the Secretary to delegate to the CIO sufficient authority to "ensure compliance" by the agency with the above information-security requirements. This must include the authority to (1) create and operate the agency-wide information security program; (2) establish information security policies and procedures and control techniques for the agency, which, when followed, will ensure compliance with all of the above requirements; (3) train and oversee personnel with significant responsibilities for information security; and (4) assist senior agency officials concerning their information security responsibilities, including the analysis process.

The agency-wide security program directed by FISMA should provide systematic guidance for the conduct of the risk analysis process, security awareness training for all VA personnel, periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, a process for remedial action, procedures for detecting security incidents, and plans for ensuring continuity of operations for information systems. The policies and procedures should interpret, explain, and apply to VA the applicable external standards and provide guidance for the application of these standards to VA

operations. The control techniques should permit monitoring of the numerous activities in which programs are required to engage to determine that they are accomplished in accordance with applicable standards and that any appropriate remedial actions are timely undertaken. The program, policies, procedures, and control techniques, and any other actions, should be developed in mutual coordination, cooperation, and collaboration between the CIO and program officials.

FISMA does not prescribe the means for the CIOs' "ensuring compliance." The legislative history indicates that, by establishing the senior ISO, Congress intended to implement the GAO-observed information-security best practice of establishing a "central management focal point to ensure adequate attention to information security." That does not necessarily require delegation to the CIO of direct control over agency programs, because such control is not the only means by which the information security-objectives may be accomplished. For example, even without direct control over certain programs, a CIO could endeavor to ensure compliance with governing standards through training and otherwise influencing the behaviors of key program-security personnel. While an agency head certainly may choose to confer certain enforcement powers on the CIO, e.g., the ability to sanction program officials outside the CIO's immediate organization for noncompliance with departmental policies, we do not read FISMA to require it.

Ultimately, an agency head is responsible for the agency's compliance with FISMA. If he or she determines the agency is otherwise able to operate in full compliance with FISMA's information-security requirements, he or she need not provide the CIO with enforcement powers. In that circumstance, the CIO's recourse for perceived non-compliance would be to exercise the prerogative of directly reporting to the agency head, which is mandated by the Paperwork Reduction Act of 1995 (44 U.S.C §3506(a)(2)(A)).

Mr. Chairman, at the Committee's June 14, 2006 hearing, you took issue with an April 7, 2004 opinion issued by my office to two VA Assistant Secretaries (including the CIO) regarding the extent of the authority granted by FISMA to the CIO. This opinion followed an earlier (August 1, 2003) opinion of my office, and I have attached copies of both opinions to this statement. Consistent with our understanding of the Act, we advised in those opinions that:

- FISMA clearly contemplates that Department officials will comply with the information-security program, policies and procedures developed by the CIO, receive assistance and training from that office regarding these responsibilities, and cooperate with the information-security techniques of that office;

- However, FISMA places upon the Secretary the responsibility for ensuring agency compliance with its provisions, and leaves to his

> discretion how to do so. The Secretary could, if he chose, delegate to the CIO various enforcement powers.

We also stated specifically in the April 4 opinion that in a March 16, 2004 memorandum to departmental officials, then-Secretary Principi had tasked the CIO with devising and developing a Department-wide cyber-security program under FISMA, and had directed cooperation in the implementation of those policies as they were developed. In this memorandum, the Secretary also announced his "intention" to imbue the CIO with all power and authority needed to carry out his responsibilities for cyber security, to "include certain administrative and supervisory authority over employees directly involved in the implementation of cyber security policy under appropriate directives, policies and personnel regulations" which the Secretary indicated "[were then] being drafted to effectuate my intentions."

We indicated in our April 7, 2004 opinion that the Secretary's memorandum signaled his intention to delegate enforcement powers to the CIO that, we anticipated, would be specified in the written directives he signaled would be forthcoming. We understand you, however, to be of the view that the Secretary's March 16, 2004 memorandum itself constituted a delegation to the CIO of any and all enforcement authority deemed necessary to ensure security-policy compliance throughout the Department.

It may be helpful to briefly state what the Department has done to implement Secretary Principi's 2004 memorandum. In an October 19, 2005, memorandum, Secretary Nicholson ordered the reorganization of VA's IT operations. In February 2006, the Secretary advised senior Agency officials at a senior management retreat that VA's IT reorganization was his top priority. In that regard, on April 30, 2006, approximately 4,000 FTE were temporarily detailed to the Office of Information and Technology (OIT) as part of the implementation of the October 19 memorandum. As of the end of the current fiscal year, those employees will be permanently transferred to OIT. At that point, all IT operations and maintenance will be centralized in OIT. As you know, the VA Chief Information Security Officer is in OIT, which recently issued VA Directive 6504 establishing mandatory security requirements for all VA information systems.

Mr. Chairman, I would add that, similar to FISMA, neither the Paperwork Reduction Act nor the Clinger-Cohen Act of 1996, which also prescribe duties of the CIO, imbue the CIO with specific enforcement powers over employees of other elements of an agency.

Thank you, Mr. Chairman, for the opportunity to testify on these very important issues.

Department of Veterans Affairs

Memorandum

Date: August 1, 2003 VAOPGCADV 12-2003

From: General Counsel (024)

Subj: Responsibilities Regarding National Security and Non-National Security Information and Information Systems

To: Assistant Secretary for Information and Technology (Agency Chief Information Officer – CIO) (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

QUESTION PRESENTED:

What is the nature and extent of the authority and responsibility of the VA Chief Information Officer (CIO) contemplated by the Federal Information Security Management Act of 2002 as to national security information and information systems?

DISCUSSION:

1. Senior managers from your offices have informally requested clarification of your respective responsibilities concerning the protection of national security information and information systems, following the enactment of the Federal Information Security Management Act of 2002 (FISMA), which is part of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002). FISMA is codified at 44 U.S.C. §§ 3541-3549.

2. FISMA is intended to provide a centralized comprehensive framework for ensuring the effectiveness of security controls over both national security and non-national security information and information systems.[1] The Act contemplates the development of effective management and oversight of information security, the use of risk of harm analyses as an assessment device for all information systems, the establishment of minimum controls to protect both types of information and information systems, and improved oversight of information security programs. See 44 U.S.C. §§ 3541, 3542.

[1] FISMA defines a "national security system" as an information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency ... the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or ... is critical to the direct fulfillment of military or intelligence missions; or [that] is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. 44 U.S.C. § 3542(b)(2).

2.

Assistant Secretary for Information and Technology (Agency Chief Information Officer – CIO) (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

3. FISMA expands upon the responsibilities of the agency CIO that have been conferred by other statutes, such as the Clinger-Cohen Act, the Paperwork Reduction Act, and the Chief Financial Officers Act.[2] FISMA requires the agency CIO to perform the following duties: develop and maintain an agency-wide information security program;[3] develop and maintain information security policies, procedures, and control techniques to ensure compliance with all security requirements imposed by the Office of Management and Budget and by the President; train and oversee personnel to the extent such personnel have significant responsibilities for information security; and assist program agency officials[4] with their security management responsibilities. See 44 U.S.C. § 3544(a)(3). Pursuant to FISMA, the CIO must designate a senior agency information security officer (senior ISO) to carry out the agency CIO's responsibilities under FISMA; the senior ISO is to head an office with the mission and resources "to assist in ensuring agency compliance with FISMA." 44 U.S.C. § 3544(a)(3). Thus, the senior ISO is responsible for performing the CIO's FISMA security duties.

4. Historically, security for classified national security information has been addressed through Presidential Executive Order. The President has prescribed a system for safeguarding classified national security information in the current

---

[2] Sections 303, 308, and 310 of title 38, United States Code, are applicable to the functions of VA's CIO as well.

[3] The components of the agency-wide information security program include the following:

(1) periodic risk assessments;
(2) policies and procedures that
  (a) reduce security risks to an acceptable level,
  (b) ensure that security is addressed throughout the life cycle of each agency information system, and
  (c) ensure compliance with FISMA, information security standards issued by OMB, agency-determined minimal acceptable system configuration requirements, and other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;
(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
(4) security awareness training;
(5) periodic testing and evaluation of effectiveness of the agency's information security;
(6) a process for planning, implementing, evaluating, and documenting remedial action to address deficiencies in information security policies, procedures, and practices;
(7) procedures for detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[4] Senior program officials are responsible for applying the risk-based approach to securing the information and systems supporting the operations and assets under their control. 44 U.S.C. § 3544(a)(2); H. R. Rep. 107-787, at 78.

3.

Assistant Secretary for Information and Technology (Agency Chief Information Officer – CIO) (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

Executive Order that requires agency heads to designate a senior agency official to direct, administer and oversee the agency's classified information program. See Secs. 5.4(d) and 6.1(ii) of Exec. Order 12958, as amended; 68 Fed. Reg. 15315, 15329, 15333 (Mar. 28, 2003).

5. The Secretary has assigned this responsibility to the Deputy Assistant Secretary for Security and Law Enforcement. As the VA senior agency official, the Deputy is responsible, consistent with law, directives, and regulation, for establishing procedures to ensure that classified national security information, and information systems that collect, create, communicate, compute, disseminate, process, transmit, destroy or store classified national security information have controls that prevent unauthorized access and ensure integrity. Id. at Sec. 4.1(f) and (g) and 5.4(d); 68 Fed. Reg. at 15325, 15329.

6. As indicated above, FISMA adds an additional requirement to national security information and information systems safeguarding. According to the legislative history of FISMA, Congress intended that agencies adopt an agency-wide security program that addresses both national security and non-national security information and information systems. H.R. Rep. 107-787, at 79. The program must include policies and procedures that ensure compliance with standards and guidelines for national security systems issued in accordance with law and as directed by the President, i.e., Executive Order 12958, take into account risk assessments, and provide for cost-effective reduction of information security risks. 44 U.S.C. § 3544(b). The VA CIO is responsible for developing and maintaining the VA security program, including establishing the necessary policies, procedures, and control techniques for ensuring that all VA national security and non-national security systems are secure, at least as measured by all applicable criteria.

7. Thus, for each VA national security information system, the VA CIO must see that the agency provides information security protections commensurate with the risk and magnitude of harm for information maintained in such systems and implements all other applicable national security system standards and guidelines, 44 U.S.C. § 3547, H.R. Rep. 107-787, at 82-3. Further, the VA CIO is required to establish and keep current effective techniques to guide and control the operation of the VA national security system to ensure adherence to the agency security program. The VA senior agency official – the Deputy Assistant Secretary for Security and Law Enforcement – must operate, control and manage the VA national security system subject to and in conformance with the policies, procedures, and control techniques that are promulgated by the VA CIO for VA national security system safeguarding.

4.

Assistant Secretary for Information and Technology (Agency Chief Information Officer – CIO) (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

8. FISMA does not require transfer of the operation of national security information systems to the CIO. Indeed, FISMA states that it does not "supersede any authority of ... an agency head, as authorized by law and as directed by the President, with regard to operation, control, or management of national security systems...." See E-Government Act of 2002, P.L. 107-347, Title III § 301 (c)(2), 116 Stat. 2955 (codified at 44 U.S.C. § 3501 note). See also Secs. 5.4(d) and 6.1(ii) of the Executive Order. This provision reaffirms that the Secretary retains authority, consistent with the Executive Order, to designate who will operate the national security systems in VA. This authority enables the Secretary to designate who will conduct the day-to-day operations, and control and manage the daily functioning, e.g., security clearance determinations, investigations, physical storage. But, as stated above, the operations, control and management of VA national security systems are subject to and must comply with the policies, procedures and controls in all portions of the VA information security program applicable to VA national security systems.

HELD:

FISMA charges the CIO with certain security responsibilities, a major one being the development and maintenance of information security policies, procedures, and control techniques to ensure security requirements issued by the President and OMB regarding national and non-national security systems, are met. FISMA requires the CIO to develop and implement an agency-wide security program to achieve these purposes.

While the daily operation, control and management of national security systems remains with the senior agency official as per the Secretary's direction under Executive Order 12958, such operation, control and management must be exercised in conformance with and subject to the security policies, procedures and control techniques promulgated in the VA information security program by the CIO.

Tim S. McClain

Tim S. McClain

Department of Veterans Affairs

Memorandum

Date: FEB 19 2004

From: General Counsel (023)

Subj: VA Directive 6500, Information Security Program

To: Assistant Secretary for Information and Technology (005)

1. We have reviewed draft VA Directive 6500, Information Security Program. We do not concur in the draft Directive for the reasons discussed below.

2. The draft directive, which implements the Federal Information Security Management Act (FISMA), is written so broadly that it appears to subject matters other than cyber, information and information systems security to Chief Information Officer (CIO) jurisdiction. As we advised in OGC Advisory Opinion 12 – 2003, while FISMA charges the CIO with information and information systems security responsibilities, the daily operation, control and management of national security systems remains with other senior agency officials, as per the Secretary's direction under Executive Order 12958, but must be exercised in conformance with and subject to the security policies, procedures and control techniques promulgated in the VA information security program by the CIO. We believe the draft Directive should be re-written to clarify the limited role of the CIO. We list the following as some examples:

a. We are concerned with the aspects of the draft Directive that concern the VA security and law enforcement function, and security clearance and suitability policies and operations.

(1) We are especially concerned with the security clearance and suitability policies and operations aspects, e.g., paragraphs 2e(2)(d), 2e(4)(h), 3b(7), 3c(13), 3c(14), 3c(15), 3d(4), 3d(5). The Secretary has assigned the responsibility for security clearance and suitability policies and operations to the Deputy Assistant Secretary for Security and Law Enforcement. We note that the rules and regulations on security clearance and suitability background investigations are complex and involve more than information and information systems security issues. A 1999 Office of Personnel Management (OPM) Security Appraisal faulted VA for having inadequate policies in this area. As a result, such comprehensive guidance has been under development for several years as a revision to Directive and Handbook 0710 and has involved a number of Offices. At a point where they were close to final concurrence, the Office of Security and Law Enforcement (OS&LE) advised our office that your office

2.

Assistant Secretary for Information and Technology (005)

advised it to cease promulgation of these policies as they would be included with the soon to be issued 005 policies. Directive 6500 does not contain the comprehensive guidance that is required on VA's policies and procedures for background investigations. Given the importance of this subject, as well as the OPM criticism, it is imperative that draft VA Directive and Handbook 0710 be issued as soon as possible. We are aware of no reason preventing the revision to VA Directive and Handbook 0710 from being issued concurrently or in close proximity with VA Directive 6500. In any event, we think it inappropriate for draft VA Directive 6500 to include other than appropriate references to Directive and Handbook 0710.

(2) The following paragraphs of the draft Directive also inappropriately concern matters of VA security and law enforcement function: 2e(2)(e), 2e(4)(b), and 3d(7).

b. Paragraphs 2c, 2e(1), 2e(3)(c), 2e(4)(a)2, 2e(4)(f), 2e(4)(i), 2e(4)(j), 2e(4)(k)1, 3c(18), and 3d(3) all appear to involve security matters beyond that of information and information systems security.

c. The following paragraphs of the draft Directive inappropriately concern human resources and labor relations matters and policies: 2e(1)(b), 2e(2)(c), 2e(4)(f), 2e(4)(m), 3b(9), 3(c)(6), 3(c)(7), 3g(8), and 4z, 4aa, and 4bb.

d(1). Although we believe that FISMA confers upon the Chief Information Officer (CIO) the legal authority to issue mandatory Department-wide cyber and information security policy and to "ensure" compliance with that policy, we are unable to find FISMA or other statutory authority empowering the CIO to "enforce" the mandatory cyber and information security policy or impose sanctions or penalties for policy violations. As an administrative matter, the Secretary could grant such enforcement authority to the CIO. However, it is not a matter of statutory right granted to the CIO or the Office of Cyber and Information Security (OCIS) by FISMA or any other legislation.

(2) Accordingly, we suggest that language pertaining to enforcement by the CIO, holding individuals accountable to the CIO for noncompliance, and establishing mandatory penalties be removed from subparagraphs 2c, 2e(4)(m), 3b(3), 3c(2), 3c(7), 3g(2), 3g(7), 3g(10).

(3) In addition, we are not aware of statutory authority that would empower the CIO to mandate budgetary commitments of Administrations or Staff Offices other than the Office of the Assistant Secretary for Information and

4.

Assistant Secretary for Information and Technology (005)

background investigations, and Lisa Hardzog (273-6465) is available to answer any questions concerning legal issues with respect to FISMA implementation.

Tim S. McClain

Tim S. McClain

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON
March 16, 2004

MEMORANDUM FOR UNDER SECRETARIES, ASSISTANT SECRETARIES, DEPUTY ASSISTANT SECRETARIES, AND OTHER KEY OFFICIALS

Cyber Security is everyone's responsibility and all employees are accountable for protecting VA's computer and information systems. Specifically, I have tasked the Assistant Secretary for Information and Technology and Chief Information Officer (CIO), Robert McFarland, with responsibility to devise and implement a Department-wide cyber security program under the Federal Information Security Management Act (FISMA). I expect all employees to fully support and cooperate in the implementation of the Department's cyber security policies.

It is my intention to ensure that Assistant Secretary McFarland has all the power and authority necessary to carry out the heavy responsibilities associated with cyber security in the Department. This will include certain administrative and supervisory authority over employees directly involved in the implementation of cyber security policy. Appropriate directives, policies, and personnel regulations are being drafted to effectuate my intentions. In the meantime, I expect full cooperation with the CIO's initiatives in cyber security.

Anthony J. Principi

Anthony J. Principi

Department of Veterans Affairs

Memorandum

Date: April 7, 2004 VAOPGCADV 5-2004

From: General Counsel (024)

Subj: Request for Advice Relating to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549

To: Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

1. In a December 29, 2003, written request, the Acting Assistant Secretary for Information and Technology, the VA Chief Information Officer (CIO), asked us to define the extent of the legal authority of the CIO (including the Office of Cyber and Information Security) under FISMA to: (1) issue mandatory Department-wide cyber and information security policy; (2) enforce compliance with that policy by all VA personnel and components; (3) hold VA personnel accountable when there has been willful non-compliance with that policy; and (4) set the scope, direction, and budgetary priorities of the Department as to information security.

2. We have also been asked for guidance concerning the authority of the CIO with respect to several specific practices and programs. In a January 21, 2004, request, OCIS requested our opinion with respect to its authority to establish rules concerning (1) the practice of sending protected health information to companies in countries where VA cannot determine compliance with information security standards, and (2) the use by such companies of medical equipment purchased from and maintained by foreign-owned vendors whose access to the medical equipment gives the vendor indirect access to the VA information network. In a January 23, 2004, request, the Acting Assistant Secretary for Policy, Planning, and Preparedness requested our opinion with respect to the CIO's authority under FISMA to oversee and control the information and information systems supporting VA's Personnel Suitability and Security Program, national security classified documents, and the Department-wide Continuity of Operations Plan (COOP). Fundamentally, the December 29, 2003, January 21 and January 23, 2004, requests all raise the same issue, namely, the extent of the authority of the CIO under FISMA over agency programs. This issue was addressed, in part, in our August 1, 2003, opinion, VAOPGCADV 12-2003, and again in our memorandum of February 19, 2004, both of which are attached. This memorandum elaborates on the positions taken therein.

3. FISMA was enacted as part of the E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002), and designated Subchapter III of Chapter 35 of Title 44. Under FISMA, the Secretary must protect VA information and

2.

Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

information systems[1] from unauthorized access, including by (1) complying with information security standards required by law (including FISMA), the Secretary of Commerce,[2] the Office of Management and Budget (OMB), and, as to national security information and information systems, the President;[3] (2) requiring VA "senior agency officials" to provide security for their information and information systems, including by performing the FISMA-mandated risk management process;[4] and (3) creating and implementing, through the Chief Information

---

[1] FISMA incorporates the definition of "information system" contained in the Paperwork Reduction Act, which is codified at 44 U.S.C. §§ 3501-3520. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C. § 3502(8). The term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology. 44 U.S.C. § 3502(6). These terms are not limited according to medium or form, e.g., electronic v. paper. OMB Circular A-130, which established policy for the management of Federal information resources and was issued by OMB pursuant to the Paperwork Reduction Act, the Clinger-Cohen Act, the Government Paperwork Elimination Act, and other legal authorities, defines "information system" as a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, *whether automated or manual*. OMB Circular A-130, (6)(j) (emphasis added). OMB Circular A-130 defines "information" (which is not defined in the Paperwork Reduction Act) as any communication or representation of knowledge such as facts, data, or opinions *in any medium or form*, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. OMB Circular A-130, (6)(q) (emphasis added).

[2] Under 40 U.S.C. § 11331 (as modified in the E-Government Act of 2002, Pub. L. No. 107-347), the Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology (NIST), prescribe compulsory and binding standards pertaining to Federal information systems, to include minimum information security standards for categorizing information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. See also 15 U.S.C. § 2789-3.

[3] In the January 23, 2004, memorandum to the Acting Assistant Secretary for Information and Technology, the Acting Assistant Secretary for Policy, Planning, and Preparedness stated that VA does not maintain a classified national security information system as defined by FISMA, and, additionally, does not have original classification authority. We clarify that the definition of a national security system under FISMA includes a discrete set of *any* information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information by an agency that is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order to be kept classified in the interest of national defense. See 44 U.S.C. § 3542(b)(2)(A) (emphasis added). We believe that this definition encompasses all classified documents stored or maintained by the Assistant Secretary regardless of the medium. See also NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System.

[4] The FISMA-mandated risk management process must include: (1) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; (2) determining levels of information security appropriate to protect such information and information systems in accordance with Secretary of Commerce, OMB and Presidentially-mandated standards; (3) implementing

3.

Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

Officer (CIO) an agencywide information security program, conformance with which shall ensure FISMA compliance by VA. 44 U.S.C. § 3544(a), (b).

4. It is clear from paragraph 3 that FISMA has imposed new security duties upon senior VA program officials, e.g., the Assistant Secretary for Policy, Planning and Preparedness, the Under Secretary for Health, namely, performance of the required risk management process on all of the information and information systems under their jurisdiction,[5] and compliance with the other information security requirements contained or referenced in FISMA.[6] In meeting these responsibilities, FISMA contemplates that they follow the information security program and the policies and procedures developed by the CIO, receive assistance and training from that office regarding these responsibilities, and cooperate with the information security control techniques of that office, as well.

5. As to the CIO, the Secretary must delegate to that official authority to "ensure compliance" by the agency with all information security measures required by FISMA. Under this authority the CIO must, amongst other things, (1) create and operate the agencywide information security program and (2) establish information security policies and procedures and control techniques for the VA, both of which, when followed, will put the Department in compliance with the FISMA-mandated information security requirements. The CIO's information security program must

---

policies and procedures to cost-effectively reduce risks to an acceptable level; and (4) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented. 44 U.S.C. § 3544(a)(2).

[5] Information and information systems that support the operations and assets of the Department include, as required by FISMA, those provided, used, or operated by another agency, contractor, or other source on behalf of the Department. 44 U.S.C. § 3544(a)(1)(A), (b).

[6] OMB has stated the following:

> While awareness of IT security requirements and responsibilities has spread beyond security and IT employees, more agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. This particular issue requires the Federal government to think of security in a new manner. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, *contrary to law* and policy, and significantly endangers the ability of agencies to safeguard their IT investments . . . FISMA emphasizes accountability for agency officials' security responsibilities, e.g., the role of agency program officials in ensuring that the systems that support their operations and assets are appropriately secure.

OMB's FY 2002 Report to Congress on Federal Government Information Security Reform (May 16, 2003), pp. 11 and 16 (emphasis added).

4.

Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

provide for several actions, a key one of which is the risk management process in which senior agency officials must engage.[7]

6. Further, the CIO must also promulgate VA policies and procedures that will guide the Department to compliance with FISMA. Such policies and procedures should convey the mandatory information security standards (see item (1), paragraph 3). They should apply the standards to VA, explaining and interpreting to make them effective in the VA context. They are mandatory for the entire Department to the extent they transmit the standards issued in law, by the Secretary of Commerce, OMB, or the President, because, as indicated above, compliance therewith is required by FISMA. The CIO may need to develop other policies and procedures designed to achieve VA compliance with FISMA; they would become mandatory upon issuance by the Secretary. The control techniques should permit CIO monitoring of the numerous activities in which the Department is required to engage to determine that they are accomplished in accordance with applicable standards. As discussed below, FISMA does not contain authority for the CIO, by his own right, to order or enforce compliance with information security requirements. The CIO clearly is expected to precipitate compliance, however, not only by issuing clear guidelines for compliance but also by providing assistance to senior managers and training and oversight to relevant program personnel. The program, the policies, procedures, and control techniques, and any other actions, should be developed through cooperation, collaboration, and coordination between the CIO and program officials.

7. Paragraphs 1 and 2 pose questions and circumstances asking whether the CIO statutorily is given authority to mandate, enforce, "hold accountable," control budgets, order changes in specific agency practices, and even take over aspects of agency programs. FISMA does not contain explicit language to that effect. The legislative history of FISMA does not reveal any such intent by the Congress. While FISMA requires the Secretary to delegate to the CIO authority to "ensure" compliance with FISMA,[8] 44 U.S.C. § 3544(a)(3), it does not prescribe the means for ensuring compliance. "Ensure" is susceptible of meaning other than having direct control. For example, "ensure" could also refer to obtaining compliance

---

[7] Another action, which is relevant to the January 23, 2004, inquiry, is the mandate that the agencywide information security program include "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." 44 U.S.C. § 3544(b)(8).

[8] "Ensure" is defined as "to make sure, certain, or safe: guarantee." Merriam-Webster's Collegiate Dictionary, 11th ed. (2003).

5.

Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

by providing ample guidance, training, oversight and other assistance. Other legislation, including extensive provisions in title 38 of the United States Code, vests substantial authority in VA Administration and Staff Office heads to administer their respective programs, including their information systems. See, e.g., 38 U.S.C. Pts. I and V. It is a basic canon of statutory construction that courts will construe statutes harmoniously, whenever possible, to give maximum effect to all statutes involved. See Tennessee Valley Authority v. Hill, 437 U.S. 153, 1989-90 (1978); Morton v. Mancari, 417 U.S. 535, 549 (1974); Posadas v. National City Bank, 296 U.S. 497, 503 (1936). Thus, in order to give full effect to both FISMA and the title 38 provisions, we conclude that "ensure" contemplates the utilization of means other than direct control of Administration and Staff Office assets or the programs mentioned in the subject inquiries.

8. To the extent that the subject practices and programs involve information or information systems – as they likely do – the senior agency officials having jurisdiction over those program assets are required by FISMA to conduct the FISMA risk management process, including taking any indicated remedial security measures. Further, in conducting the risk management process, those officials must adhere to the other requirements of FISMA, e.g., requirements issued by the Secretary of Commerce, OMB, and the President, training relevant personnel as to their information and information systems. Finally, they must comply with the agencywide security program and policies and procedures promulgated by the Secretary as to those assets. The CIO must guide, inform, and assist the program officials as they act to meet these new FISMA security obligations. If the CIO believes that there are deficiencies in an approach to securing information and systems, the CIO should recommend remedial actions.[9] If the CIO believes that a VA program remains in noncompliance with the above information and information systems security requirements, notwithstanding, the CIO's recourse, under FISMA, would be to report to the Assistant Secretary or Administration or Staff Office Head, and if necessary, the Secretary.

9. Ultimately, the Secretary is responsible for the agency's compliance with FISMA. The Act does not disturb his discretion in deciding how to accomplish that compliance. Specifically, FISMA does not require the Secretary to provide the CIO with enforcement powers. To the extent that he chooses to do so, however, he may delegate more authority to the CIO than is provided for by

[9] In carrying out the responsibility of "assisting agency senior officials with their security responsibilities," we would envision under FISMA that, after detecting possible non-compliance, the CIO would first attempt to resolve the problem, which might entail recommending remedial actions, requesting that the program office submit an explanation, and otherwise collaborating with the program office to reach a mutually satisfactory FISMA-complaint result.

6.

Assistant Secretary for Information and Technology (005)
Assistant Secretary for Policy, Planning, and Preparedness (008)

that Act. In that regard, we note that, by memorandum of March 16, 2004, a copy of which is attached, the Secretary has, on a limited basis, done exactly that. Besides declaring his intent that all personnel support and comply with the Department-wide security program, the Secretary specifically stated that the CIO has "certain administrative and supervisory authority over employees directly involved in the implementation of cyber security policy," and that this intent will be included in appropriate Department issuances now being prepared. Thus it would appear that the Secretary anticipates that this narrow additional authority will be addressed in the Department directive under consideration by the CIO, and other implementing materials.

10. The December request for guidance on the drafting of the Departmental directive on information security asked for suggested language to be used in that directive. Our February 19, 2004, memorandum replied, at least in part, to that request. Lisa Hardzog of my staff is available at 273-6381 to answer questions concerning this memorandum, and review proposed language for the information security program directive being prepared by the CIO.

Tim S. McClain

Tim S. McClain

Attachments

cc: Office of Inspector General (50)
Under Secretary for Health (10)
Assistant Secretary for Human Resources and Administration (006)
Acting Assistant Secretary for Congressional and Legislative Affairs (009)

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
U.S. House of Representatives, Congress of the United States

Thursday, June 22, 2006 Hearing

Written Statement of Leon A. Kappelman, Ph.D.
Professor of Information Systems
Director Emeritus, Information Systems Research Center
Fellow, Texas Center for Digital Knowledge
Associate Director, Center for Quality & Productivity
Information Technology & Decision Sciences Department
College of Business Administration, University of North Texas

Members of the House Subcommittee on Oversight and Investigations of the Committee on Veterans' Affairs, thank you all for this opportunity to share my observations and recommendations about the Department of Veterans' Affairs. I previously had the honor of testifying before this Committee in March, 2002 and submitted a written statement for your hearing held on May 22, 2006. I have worked with VA on their cyber security, enterprise architecture, project management, IT workforce, IT contingency planning and continuity of operations, as well as other efforts. I have done similar work for the Executive Office of the President, as well as many other public and private enterprises.

As for the question of whether security for data and information should be centralized at VA, my answer is simply "absolutely." Centralized IT security (meaning all personnel, dollars, policies, and other IT security resources) is essential to ensuring effective cyber security at VA. More than that is needed (including effective and engaged leadership and a concerted and consistent effort to change VA's culture of indifference), but without centralization cyber security at VA is doomed to failure (as recent events indicate).

It is like asking whether national security should be centralized. If not for the relative newness of digital information, and the relative slowness of human thinking processes to change, we would not be asking such questions. But like national security in the USA, IT centralization at VA cannot be about totalitarianism or dictatorship. It too should be centralization with representation. And as our own nation's history demonstrates, this can be successfully done.

As they have done in the past, VA's two major divisions (health care and financial services) will provide an abundance of reasons why centralization of IT security is not necessary or impractical. This is simply balderdash. Moreover, VA's history since the passage of Clinger-Cohn over a decade ago indicates that when left to their own devices they will not comply with laws or management directives regarding IT centralization. I am also aware that many efforts to unify VA's culture and/or operations have been subverted by VA in the past (for example, the OneVA effort and countless prior attempts to centralize IT and cyber security). This kind of behavior should not be tolerated by a US Congress that still holds VA's "purse strings."

Response to Post-Hearing Questions for
John H. Thompson, Deputy General Counsel
Department of Veterans Affairs

1. How would VA determine its standard for "Gross Negligence" in the context of work-related actions or inactions by a VA employee? Cite as necessary.

To sustain a charge of gross negligence before the Merit Systems Protection Board (MSPB), the agency must show acts which are reckless or willful. *Martinez v. Dept. of Agriculture,* 22 MSPR 365 (MSPB1984). For conduct to be considered reckless it must evidence disregard for, or indifference to, the consequences, even if no harm is intended. *Social Security Administration v. Carr,* 78 MSPR 313 (MSPB); *see also Gottshall v. Air Force,* 37 MSPR 27 (MSPB 1988).

2. The following questions refer to the May 3, 2006 burglary of a VA employee's Maryland home, the loss of VA data resulting from that burglary, and other related actions. (The employee's name should not be used in your responses):

a. Date and time you first learned about the potential loss of data?

Approximately 1:30 p.m. on May 10, 2006.

b. Who told you or otherwise communicated with you about the potential loss of data?

The Chief of Staff, Mr. Thomas Bowman.

c. Where were you when you learned this information?

My office at VA headquarters.

d. How was the information provided to you (phone, e-mail, etc.)?

Mr. Bowman handed me a copy of a May 5, 2006 memorandum, subject: "Possibly Lost Veteran Data", bearing the name of Mark Whitney, Information Privacy/Security Officer, Office of Policy, Planning and Preparedness (copy attached). Mr. Bowman said it indicated personal data may have been lost as a result of the May 3 housebreaking, and he asked that I have an OGC opinion prepared regarding the Department's obligations to notify any individuals identified in the lost data.

e. **What level of confidence did you have regarding this potential loss?**

The May 5 memorandum described the housebreaking and theft but was vague in many respects regarding the scope of the data loss. It also indicated the most critical data had been encoded in a manner ("SAS code") with which I was unfamiliar. As a result, I did not upon reading that document appreciate the full extent of the loss.

f. **What is the maximum time the employee who was burglarized could reasonably delay providing notice of the theft to VA officials to avoid meeting the "Gross Negligence" threshold you defined in #1 if he believed the lost data included at least one million names and social security numbers of living veterans?**

To my knowledge, the employee did not delay notifying his superiors and discipline has not been proposed on that account.

g. **List the names of anyone else who learned of the potential loss of data from your source of this information at the time you were notified and explain those circumstances.**

I was alone in my office when Mr. Bowman made me aware of the loss, so no one else learned of it from him at that time. I subsequently passed on the memorandum to a subordinate in the Office of General Counsel when I made the assignment.

h. **What is the maximum time that any employee who was consulted or advised regarding this data loss in their professional capacity, who understood that the loss represented a serious problem for the agency and a possible liability for the U.S. Government, could delay providing notice of this loss to more senior VA officials to avoid meeting the "Gross Negligence" threshold you defined in #1?**

As I indicated above, disciplinary action has not been proposed against the individual whose house was broken into on the basis of any delay in notifying his superiors. Your question assumes gross negligence could be found and disciplinary action taken based upon a mere delay in notification, which I do not know to be the case.

i. **List all individuals you notified about this data loss prior to May 16, 2006. Include date, time, circumstance.**

The only person I notified prior to May 16 was Assistant General Counsel Deborah McCallum, to whom I made the assignment for the opinion requested by the Chief of Staff. I did so by virtue of a handwritten

"buckslip" that was delivered to Ms. McCallum within minutes after the Chief of Staff requested the opinion.

j. **Were you the author of the memorandum provided to VA on May 16, 2006 that stated VA's responsibilities regarding the Privacy Act notifications to individuals whose personal data may have been compromised?**

No, but I was in the chain of review it received before going to the General Counsel for approval and signature.

k. **Either provide a copy of the memorandum referenced in 2.j. above or summarize VA's responsibilities under the Privacy Act for providing such notice.**

A signed copy is attached.

What would be the minimum number of personal records – each containing a living veteran's name, social security number and date of birth – that if lost, should prompt a VA employee to notify their supervisor?

I believe the loss of even one such record should prompt notification of one's supervisor.

9354

Department of Veterans Affairs

Memorandum

Date: MAY 16 2006

From General Counsel (02)

Subj: VA Legal Responsibility to Notify Individuals about Possible Compromise or Loss of Their Individually-Identifiable VA Information

To: Chief of Staff (00A)

1. In response to a specific incident, the Office of General Counsel was asked to address the legal responsibility of the Department of Veterans Affairs (VA) to promptly notify individuals in writing about the loss or possible compromise of their individually-identifiable VA information to individuals who do not have a need to access the information in the performance of their VA duties.

2. Under the Privacy Act, 5 USC 552a(e)(10), and the HIPAA Security Rule, 45 C.F.R. Parts 160 and 164, Subparts A and C (which applies to VA patient-specific information in VHA's possession and control), the Department has the legal obligation to mitigate the damage that an individual may suffer as a result of the possible compromise or loss of individually-identifiable VA information associated with that individual. This duty to mitigate includes the duty to notify the individual of the possible compromise so that he or she may also take steps to protect his or her identify. VHA, in consultation with OGC, drafted standard notification letters that it has used to notify VHA patients of previous disclosures or compromises of individually-identifiable VHA data. Copies of the standard letters are attached.

3. OMB has endorsed this position as reflected in the attached draft response to a Congressional inquiry. As reflected in the attached OMB response, the Department of Defense takes a similar position. Further, States are enacting laws that require such notification by private entities. Finally, the Federal Trade Commission may require entities subject to its jurisdiction to pay for consumer redress for compromise of individually-identifiable information protected under the Fair Credit Reporting Act.

4. Under this legal analysis and given the facts in the May 5, 2006, memorandum provided for our review, VA has a legal duty to notify the individuals whose information was stored on the stolen VA computer of the theft and possible compromise of their VA data. The VA office responsible for the data has the responsibility of providing the requisite notice. Again, the attached VHA letters may be used as models in drafting the requisite notice letters.

5. The memorandum that was provided for our review does not appear to document VA's complete compliance with an additional legal requirement. The Federal Information Security Management Act (FISMA) requires agencies to notify the Federal incident handling center, law enforcement, and agency Inspectors

2.

Chief of Staff (00A)

General when significant incidents occur. 44 USC 3544(b)(7)(C). We assume that VA has complied, or is complying, with the *Computer Security Incident Handling Guide*, Special Publication 800-61 (National Institute of Standards and Technology, January 2004) in addressing this incident.

Tim S. McClain

Tim S. McClain

Attachments

Date

Veteran Name
Address
City, State

Dear Mr. :

On <Insert Date>, the Department of Veteran Affairs (VA) aware of a breach in our data security. As a result, information identifiable with you was potentially exposed to others. This information included your name and social security number. It is possible that your name and social security number could be used without your knowledge. As this situation could lead to identity theft, we want to inform you and help you protect yourself in case someone should attempt to misuse this information.

Although the risk of anyone using this information is very small, we are enclosing letters addressed to the three major credit agencies regarding this unfortunate event for you to sign and mail to them so that they are aware of this incident. We are also enclosing postage-paid envelopes for your convenience. The credit agencies will watch for any unusual financial activity using your identification. Also enclosed is information on an agency that specializes in assisting people with ensuring their credit and identity is secure. The firm is Identity Guard and they may be contacted at 1-800-214-4791 or by mail at Identity Guard Service, P.O. Box 222455, Chantilly, VA 20153-2455. VA will reimburse any cost you incur related to using this service for up to one year. Please send any bills you may receive for this service and the use of the credit agencies to: <Insert Information> .

We apologize for any inconvenience this may cause, but believe it is important to inform you of the risk resulting from this incident. Again, we want to reassure you that we have no evidence that your protected information has been misused. We will keep you apprised of any further developments.

If you have any questions regarding this or encounter any problems, please contact <Insert Name and Title> at <Insert Number> .

Sincerely,

<Insert Title>

Date

Equifax
P.O. BOX 740241
Atlanta, GA 30374-0241

To Whom It May Concern:

On <Insert Date> the Department of Veteran Affairs (VA) became aware of a breach in our data security. As a result, information identifiable with certain individuals in our database was potentially exposed to others. It is possible that these individuals' name and social security number could be used without their knowledge. As this situation could lead to identity theft, we want to inform your organization so that you may place an alert on the credit files of these individuals should there be any attempt to misuse the information.

The individual identified below has been notified of this situation. We appreciate any immediate assistance you can provide to insure this individual's file is protected from any unauthorized use.

Veteran name
SSN:
Address
City and State

If there is any additional information you need, please contact <Insert Name and Title> at <Insert Number>.

Sincerely,

<Insert Title>

I am aware of this situation and concur with placing an alert on my credit file to protect against unauthorized use:

_____ _____
Veteran Name DATE

Questions for the Record
For the House Committee on Veterans' Affairs
June 30, 2006

Bruce A. Brody, CISSP, CISM
Vice President, Information Security, INPUT

Your testimony recommends that the Committee legislate a Chief Security Officer, possibly with the title Undersecretary for Risk Management.

1. How does the Chief Security Officer differ from the Chief Information Officer, and what kind of authority would this position have?

Answer: My recommendation is that the Chief Security Officer be separate from and at least co-equal with the Chief Information Officer. Two points are worth noting. First, the Chief Security Officer would incorporate all security responsibilities for the department, including information, cyber, physical and personnel security, as well as privacy and emergency preparedness. By so doing, security would no longer be fragmented along legacy and parochial interests, and all security issues would benefit from one voice and one champion in the department. Moreover, cross-over security concerns such as background investigations for IT personnel or physical security of data centers would be better integrated. Second, the separation of duties issue with the CIO would no longer be a factor. Although FISMA would require the senior agency information security officer report to the CIO, separating security from the CIO would eliminate the possibility that security prerogatives would be subordinate to information technology "features and functions" priorities, or to budget cuts at the expense of other information technology pressures.

My recommendation to elevate the position possibly to the level of an Undersecretary is merely an acknowledgement that, without a seat at the executive table that is co-equal with the Undersecretaries for Health, Benefits and Memorial Affairs, security becomes a distraction and an annoyance to the executive team. Within this proposed new Enterprise Risk Management organization, the senior risk management executive is charged with harmonizing the risk assessment process and standards across the organization and de-conflicting risk reporting prior to it being forwarded to the senior leadership as a whole. For senior leadership, this risk management process becomes "one-stop shopping."

In addition, for the following reasons, Enterprise Risk Management is a logical step in consolidating and coordinating personnel, physical, document and cyber security under one set of management principles:

- Federal audit standards (FISCAM) required by GAO already measure the effectiveness of controls common to each risk management discipline.
- On its face, and Enterprise Risk Management organization suggests a bridge between the sometimes competing statutory oversight requirements of the CFO

Act, the Clinger Cohen Act, the Federal Information Security Management Act and OMB Circular A-130, Appendix III.

- Additionally, recent internal debates at the VA concerning personnel and physical security standards and programs – a debate that included the Office of General Counsel – could be resolved through this more efficient and centralized risk management approach.

This position would have the authority not only to set policy, but to enforce it by holding people accountable for non-compliance. A very effective first step in this process would be to suspend all executive bonuses in the department until the executive receives a clean bill of security health for the environment over which the executive has purview. Sadly, this measure might be the only effective way to ensure that security receives the proper attention and priority at the senior levels of the department.

2. Who currently controls information security at VA? How will a centralized IT system help provide better control over the security of information?

Answer: It is not clear that anyone controls information security at the VA. When I was hired in March 2001, I thought the Secretary had charged me with this responsibility. I came to find out, through the legal opinions of the General Counsel, that the Office of the CIO had no authority to enforce compliance, and that ancillary security functions that affected information security were scattered around the department. In actual practice, hundreds of local IT directors across the department had control over whatever security was being deployed, or disregarded, and that I had no ability or authority to compel them to operate in accordance with departmental policies or Executive Branch regulations. In such a decentralized enterprise, security is under the "control" of hundreds of different local IT chiefs, which means security is not under anyone's control.

It is safe to say that information security cannot be successful under a decentralized management and authority model. I am not aware of a single successful decentralized or "federated" information security model anywhere in government or industry, but I am aware of numerous successful centralized security models.

Centralized IT authority and centralized information security authority provide overall better control of security for a variety of reasons. First, the rigor of a comprehensive defense-in-depth security architecture can only be achieved by central management, through the implementation and operation of standard controls and countermeasures across the entire enterprise. Second, the lack of qualified and competent security practitioners in the VA begs for a centralized model, where precious expertise can be applied on a far more efficient basis. Third, there can be no excuses for the continued neglect of and inattention to information security responsibilities at the local level when these responsibilities are centralized under a qualified and competent executive. Fourth, significant efficiencies and economies of scale can be achieved through the central acquisition and operation of enterprise-wide security technologies and capabilities,

eliminating the current redundancies and potentially saving the department hundreds of millions of dollars while increasing the overall security posture.

Given that the decentralized model has resulted in decades of neglect and inattention to the department's collective information security responsibilities, it would appear that the only reasonable alternative would be centralization.

Response of Mike Cook, Co-Founder, ID Analytics,
to Written Follow-Up Questions from
Chairman Steve Buyer, House Committee on Veterans' Affairs

"Oversight Hearing on the Academic and Legal Implications of VA's Data Loss"

1. **Is credit monitoring alone sufficient?** Credit monitoring is not sufficient to address problems arising from a data breach. While credit monitoring does provide some protection from identity theft for some consumers, there are inherent problems with credit monitoring, as well as some shortcomings. The inherent problems with credit monitoring are:

    a. The amount of consumers who actually sign up for credit monitoring, even if provided at no cost is very low. Generally, anywhere from 5-15 percent of breached consumers will sign up if offered free credit monitoring (breached employees tend to sign up at a higher rate than non-employees). Publicity may push enrollment somewhat higher for the VA breach, but it is highly likely that a substantial majority of veterans will not enroll in this service. Once enrolled, at the end of the free term period, many consumers will choose not to re-enlist to the fee based service. Therefore, while credit monitoring solutions do afford some protection, it is only for those consumers who might sign up, and keep, the service over time.

    b. Credit monitoring solutions require that the breached consumer self-police their own credit histories. We do not know if consumers actually review the alerts that are provided to them, and if they do, if the consumer knows specifically what to do with the alert. However, while many consumers might self-police their credit report file, it places a burden on a consumer who has already been burdened by the data breach.

    c. Credit monitoring cannot distinguish between identity theft caused by the VA breach and identity theft that occurred independent of the breach. This creates an overbreadth problem as veterans who use the service will naturally assume that any identity theft they find is directly attributable to the breach, when the theft may be entirely independent. This risk of incorrectly attributing identity theft to the VA breach is substantial. The 2003 FTC Identity Theft Survey conducted by Synovate found that the U.S. population has a 1.5% chance of falling prey to identity theft in a typical year. This risk occurs regardless of a data breach. In contrast, analyses of actual data breaches show that misuse rates stemming from a breached consumer file can be as low as 0.098%.

    Credit monitoring solutions also have some shortcomings:

    a. Credit monitoring can not measure the rate of misuse, or determine if there might not be any misuse stemming from the breached file.
    b. The location of misuse can not be determined, if the breached file is misused. Therefore, while specific consumers might be able to limit the misuse of their identity, the breach file will not be found using credit monitoring.
    c. Breach monitoring (ID Analytics' technology for detecting misuse of a breached file) analyzes 100% of the consumers on a breached file, and does not require consumers to sign up for anything.

2. **What other safeguards should be in place?** Veterans who are concerned about identity theft can place a fraud alert on each of their three national credit files. In some states, concerned veterans can put a security freeze on their file. The security freeze option is not instant (typically takes 3 days to lift or reinstall the freeze) and may cost the veteran money. Of course, we believe that the VA should analyze the entire breach file for misuse.

3. **Can you provide us an estimate regarding how much will credit monitoring for the veterans whose data was mishandled will cost?** No. That figure would depend on negotiations between credit monitoring providers and the Department of Veterans Affairs.

4. **ID Analytics has access to huge amounts of data. How does the company keep its data secure?** ID Analytics' protection of the privacy and security of consumer data starts with the company's business model. ID Analytics collects data for one purpose only - to stop identity fraud. Unlike most other companies in the fraud prevention and credit monitoring fields, ID Analytics does not market or sell the personal data it collects. We never share information from our ID Network with customers. Clients receive only our risk scores and explanations of the scores.

   ID Analytics has met and satisfied security audits by some of the largest financial, wireless, health care, and retail card institutions in the country. For security reasons, we will describe our security practices only at a high level, but can provide more detail in a less public forum.

   ID Analytics defends against internal as well as external threats through a combination of constant vigilance, state-of-the-art intrusion detection systems, industry leading network equipment, well thought out software configuration and leading edge server management practices.

   Site security include use of picture badges for employees, multi-factor authentication locks, motion sensitive video cameras, and limiting employee access to secure facilities based on a "need to know." Employees undergo an internal education program to prevent pretexting and phishing.

   ID Analytics employs sophisticated, multi-layer firewall architecture to create security zones for the data network, based on ICSA-certified security hardware and software. Personal data is protected by end-to-end encryption.

5. **Using ID Analytics product, if fraudsters upload these identities to the Internet in order to sell them, how quickly will VA be able to detect misuse of these identities and perhaps recover them?** If, in a file of 26.5 million veterans, there is misuse of one or two veterans' identities, it will be impossible to detect the misuse and locate the file. However, if a fraudster (or a collection of differing criminals) uses just a dozen or so of those names in activity involving wireless, credit card, or retail credit accounts, ID Analytics should be able to detect that misuse within days, weeks or months of their misuse. The reason for the "days vs. months" is driven by the amount of time between breach analyses. We had suggested to the VA that ID Analytics could screen the breached names on a quarterly basis. If the VA chose to screen the names on a monthly basis, any misuse would be found anywhere from one day to 60-90 days sooner. Recovery of the misused identities requires law enforcement involvement, and law enforcement would only be able to recover physical identities downloaded off the Internet and held at the fraudster's site. If the identities were put on the Internet, locating the sites that were trading those identities could likely be impossible (unless law enforcement was

able to catch those fraudsters who were misusing the file and they were persuaded to provide information on where they obtained the identities).

6. **How long should the fraud alert be active for credit monitoring?** Indefinitely, if the breach analysis detected misuse. Until misuse is detected, I believe a fraud alert is not necessary.

7. **How long should credit monitoring be in place?** Indefinitely, if the breach analysis detects misuse. Until misuse is detected, I do not believe credit monitoring is necessary subsequent to the VA data breach.

○