FAILURE OF VA'S INFORMATION MANAGEMENT

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 25, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-48

28-124.PDF

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2007

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

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, *Indiana, Chairman*

MICHAEL BILIRAKIS, *Florida*
TERRY, *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
May 25, 2006

WITNESSES (CONTINUED)

INFORMATION FOR THE RECORD

POST-HEARING QUESTIONS FOR THE RECORD

FAILURE OF VA'S INFORMATION MANAGEMENT

THURSDAY, MAY 25, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, D.C.

The Committee met, pursuant to call, at 9:05 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [Chairman of the Committee] presiding.

Present: Representatives Buyer, Bilirakis, Stearns, Moran, Brown of South Carolina, Miller, Boozman, Brown-Waite, Campbell, Filner, Gutierrez, Brown of Florida, Michaud, Herseth, Strickland, Hooley, Reyes, Berkley, Udall, and Salazar.

THE CHAIRMAN. The House Committee on Veterans' Affairs dated May 25, 2006, will come to order. If somebody will get the door for us, please.

By way of housekeeping, we only have the Secretary for about 45 minutes, and then there's a hearing on the Senate side that starts at 10:00 o'clock. He will be taking Mr. McLean with him. Others of his staff will remain, and step forward at the table when the Secretary leaves.

I will give an opening, and then I'm going to yield to Mr. Strickland for an opening, and then we are going to immediately go to questions. What I would propose is, because we only have him for 45 minutes, is that I do a unanimous consent that each member may have three minutes to do questions, so we try to give quick latitude to all the members. Any objections?

[No response.]

All right. And hearing no objections, so ordered.

The purpose of this hearing is to learn more about the recent loss of personal data belonging to as many as 26.5 million veterans and some spouses experienced by the Department of Veterans Affairs. We have a meltdown in VA's information Management. According to

VA, this meltdown has resulted in a catastrophic failure to safeguard sensitive personal data. Last Monday, the Department of Veterans' Affairs released a statement acknowledging that a data analyst took home electronic data which he was authorized to access at work, but not authorized to bring home. The burglary of his home and the theft of his computer resulted in the loss of that data. This serious incident was not communicated to this Committee until Monday, May 22nd, 19 days after the theft, and one hour prior to its release to the public.

We must answer some pressing questions, which include: how did this breach of information Management happen, what will we do to protect veterans from identity theft, what policies and regulations are in place in the department that should have stopped the mismanagement of information, and what is the VA doing to eliminate the vulnerabilities associated with the security of sensitive information? And there are many others from my colleagues.

And let me be clear. We are here today to inform America's veterans and their families what the government is doing to protect them against fraud and ease their efforts to protect themselves. Our veterans and their families must be assured of how you, Mr. Secretary, will safeguard the information they place in your hands. Whether or not any identity fraud results from the theft of this computer carried home by this VA employee, what is clear is that damage has been done.

Speaking as one of those millions of veterans such as even yourself, Mr. Secretary, the prospect of fraud, theft, of the awful prospect of repairing damaged credit, is bad enough. For that stress to be caused by our own Federal Government is deeply disturbing, and I know everyone here agrees it is intolerable. There will unfortunately be a certain percentage of the 26.5 million veterans that will have to deal with identity theft in the normal cause of life. And now some of them will blame the VA. So that's going to be a challenge for you.

Beyond the very personal dimension: this incident has implications regarding the larger picture of control over VA information technology. Over the last seven years we've seen compelling evidence of information security problems at the VA, and I refer to the Committee hearings which I've chaired. On May 11th of 2000, the GAO stated that computer security, quote: "..is critical to VA's ability to safeguard its assets, maintain the confidentiality of sensitive information, and ensure the reliability of its financial data. The VA IG acknowledged the department-wide weaknesses in information security systems that continue to make VA's program and financial data vulnerable to error and fraud," end quote.

At a September 21, 2000 hearing, GAO stated, quote, "Serious computer security problems persisted throughout the department and VHA, because VA had not yet fully implemented an integrated se-

curity management program, and VHA had not effectively managed computer security at its medical facilities," end quote.

At the April 4, 2001 hearing, the IG continued to, I quote, "identify significant information security vulnerabilities that place the department's data systems at risk of unauthorized access and disclosure." The IG testified that, quote, "many of these vulnerabilities exist in violation of VA policy," end quote.

At a March 13, 2002 hearing, the IG repeated findings of the vulnerabilities of VA's information technology.

Then almost four years ago today, on May 20th and May 21st, a WISHTV 8 I-Team led by Karen Hensel in Indianapolis, Indiana, went to Goodwill and bought three computer hard drives. Two of those hard drives she learned were never cleansed, and they contained hospital patient records from the Roudebush VA Hospital in Indianapolis. The names of veterans, their Social Security numbers, home address, phone numbers, pages and pages of government credit card numbers, information regarding veterans' arrest records, whether they were receiving drug and alcohol counseling, whether they were disabled. There was one of the veterans was blind, disabled, and living alone and was a combat veteran. It discussed his case. One of the patients was HIV. A hundred twenty of those computers were sold at a surplus sale without ever having been cleansed.

So we went through all the hearings on that. "Oh, the controls are going to be in place, we assure the Committee."

At the September 26, 2002 hearing, the IG testimony stated that, quote, "Penetration testing completed during the past two years verified that the VA's information system could be exploited to gain access to sensitive veteran health and benefit information."

At a March 17, 2004 hearing, the VA testified that, quote, "there was a glide path in place for the meeting, the 2004, April 2004 deadline for the beginning of the VETSNET deployment. VETSNET has been in development for a decade. I've been told that VETSNET will not deploy in 2006 and maybe not even now till 2007."

As Chairman of the Subcommittee on oversight and investigations, and now the Chairman of this Committee, I have led a bipartisan effort to centralize VA's IT infrastructure and control over its IT systems. Last November, this House voted unanimously, 408 to zero, to centralize IT management with the department's chief information officer. Both the department and the Senate have sadly resisted such centralization of VA's IT architecture. Even the Independent Budget of the VSOs opposed centralization of VA's IT infrastructure in their 2007 budget.

The VA Inspector General in his November 2005 report entitled, "major management challenges of fiscal year 2005," stated that, quote, "VA has not been able to effectively address some significant information security vulnerabilities and reverse the impact of its his-

torically decentralized management approach."

The report went on to say that, quote, "While the VA has accelerated efforts to improve Federal information security, more needs have to be done to put security improvements in place that effectively eliminate the risk and vulnerabilities of unauthorized access and misuse of sensitive information," end quote.

Look where we are here today, Mr. Secretary. This Committee, this Congress, we have asked to empower the CIO to put his arms around this one, and that was resisted. We also—I have even asked about letting the VA be on parity with other departments with regard to political appointments. That has been resisted. And now what we have is, we have some management questions. This isn't just an issue of a low-level employee. There is very serious mismanagement of information technology that is at stake.

So with that context, I believe there is a damaged trust, angered veterans and families, and there are systematic flaws. And Mr. Secretary, this is a defining moment of your leadership.

With that I yields now to Mr. Strickland.

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

MR. STRICKLAND. Mr. Chairman, I would yield to my colleague from California, Mr. Filner, and I would ask that my statement be entered into the record, please.

THE CHAIRMAN. Thank you, Mr. Strickland. All the members may have opening statements, and your statements will be submitted for the record.

[The statement of Mr. Strickland appears on p. 68]

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

MR. FILNER. Thank you, Mr. Chairman, and thank you for this hearing. Thank you for your opening remarks. I associate myself completely with them. You laid out a complete record, I think that we don't have to repeat, so I appreciate your strong attitude toward this issue.

We are now presented, as the Chairman said, with a catastrophic problem. The VA simply did not protect essential personal information entrusted to its care. Now, and for the next few decades maybe, a potential sort of Damocles hangs over the financial well-being of over 26 million veterans, unless this data is recovered.

In the last five years, as the Chairman outlined, a host of agencies, the VA Inspector General, the GAO, prominent IT consultants have reported that VA has many problems with information security. We found multiple failures under the Federal Information Security Management Act, and the performance reviews required by that Act. We note that three or four information security recommendations to the VA by the Government Accountability Office in March 2002 have yet

to be implemented. Outside contractors have noted related problems. And how does VA react? With indifference.

Internal VA recommendations to strengthen the control of information meet with resistance. Even Secretary Principi's directive to centralize information technology at the VA in 2002 was met with indifference. It was not implemented.

In the last few years, this Committee and its Subcommittees have chronicled problems related to unclear lines of IT management authority throughout the VA, from information security Officer training in the VBA to sensitive information releases on unscrubbed computer hard drives at VA medical centers, a host of very expensive major computer project failures and delays.

We rarely see accountability, neither in the IT or the information security world at the Veterans Administration. The individual responsible for the release of the unscrubbed hard drives was soon promoted. Again, VA seems to react with indifference to its problems in this area.

As Chairman Buyer pointed out, the problem before us today is not unexpected. It has sprung from a culture of indifference, at the Veterans Administration, and has grown strong among the leaders who have allowed it to grow. The most important agent in information control and security in an organization is its leadership. When they are not proactive, Mr. Secretary, bad things happen. And a very bad thing has happened that we are looking at today.

Too much time transpired before Congress was notified. Sure, you needed to hope that the thing was found, but you could have briefed the Chairman and others in this body about that, what happened. Too much time transpired before veterans were notified. And when you did notify them, you left it to them to go contact their credit bureau, or their banks. You didn't say, "We will take care of it, we will be behind you, we will pay for the problems that you might have." VA's message was, "Trust us, we will handle it." Well, we should now question if even after this wake-up call, you are up to the task.

Certainly this administration has proclaimed its need to collect information on our citizens. On May 11th, President Bush defended those actions by noting that the privacy of ordinary Americans is fiercely protected in all of our activities. Well, I think this data debacle before us today clearly demonstrates the folly of the President's attempt to place us at ease regarding the Administration's ability to fiercely protect our privacy. This does not meet my definition of fierce protection. I only see indifference.

Mr. Chairman, I appreciate again this opportunity to look into this incredible disaster.

THE CHAIRMAN. Thank you, Mr. Filner. And I associate myself with Mr. Filner's comments.

Testifying now will be Secretary Nicholson. Secretary Nicholson

is accompanied by the Honorable Alan Pittman, the Assistant Secretary of Human Resources and Administration; the Honorable Robert J. Henke, Assistant Secretary for Management; Retired Army Major General Bob Howard, the Acting Assistant Secretary for Information Technology; Pedro Cadinez, Jr., Associate Deputy Assistant Secretary for Cyber and Information Security, and the Acting Deputy Assistant Secretary for Information Technology; Dennis M. Duffy, Acting Assistant Secretary for Policy, Planning, and Preparedness; Michael Mclendon, Deputy Assistant Secretary for Policy; and the Honorable Tim Mclean, the Department's General Counsel.

All the individuals who I have just identified, if you would please stand, I'm going to swear all of you in. Would you please raise your right hand.

[Witnesses sworn.]

Mr. Secretary, you are now recognized.

TESTIMONY OF HON. R. JAMES NICHOLSON, SECRETARY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY HON. R. ALLEN PITTMAN, ASSISTANT SECRETARY FOR HUMAN RESOURCES AND ADMINISTRATION; HON. ROBERT J. HENKE, ASSISTANT SECRETARY FOR MANAGEMENT; MAJOR GENERAL (RET.) ROBERT HOWARD, ACTING ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY; PEDRO CADENAS, JR., ASSOCIATE DEPUTY ASSISTANT SECRETARY FOR CYBER AND INFORMATION SECURITY AND ACTING DEPUTY ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY; DENNIS M. DUFFY, ACTING ASSISTANT SECRETARY FOR POLICY, PLANNING AND PREPAREDNESS; MICHAEL MCLENDON, DEPUTY ASSISTANT SECRETARY FOR POLICY; HON. TIM S. MCCLAIN, GENERAL COUNSEL; AND HON. GEORGE J. OPFER, INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS

SECRETARY NICHOLSON. Mr. Chairman and members of the Committee, thank you for giving me the opportunity to appear before you today, to explain a devastating occurrence that has happened in my agency. It has come to my attention recently. It was announced to all on Monday of this week.

I am the person ultimately responsible to our veterans, and therefore, the responsibility for this situation rests on me. A VA employee who was a data analyst took home electronic data files from the VA. He was not authorized to do so, nor were they encrypted. His house was burglarized and the data were stolen. This happened on May 3rd. If that wasn't bad enough, I wasn't notified about this event

until May 16th. As a veteran myself, I have to tell you that I am outraged. I am frankly mad as hell. But I must carry on, and lead the efforts to get to the bottom of this, and take corrective actions to see that it doesn't happen again.

My compass for this is the veterans. How do we best take care of them now, and mitigate the effects of this on them? These stolen data contained identifying information including names and dates of birth for up to 26.5 million veterans, and some of their spouses. In addition, that information, plus Social Security numbers, was available for some 19.6 million of those veterans. Also included possibly were some numerical disability ratings and the diagnostic codes which identified the disabilities being compensated.

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

On May 3rd, the employee's home was broken into in what appears to local law enforcement to have been a routine breaking and entering; that is, a random burglary, not a targeted one. And the VA data were stolen. The employee has been placed on administrative leave pending the outcome of an investigation with which he is cooperating.

As I have said, I am a veteran too, and I am outraged at the loss of our veterans' personal data. And I am outraged at the fact that an employee would put us all at risk by taking it home in violation of VA policies with which he was very familiar. I am also very outraged that it was not until May 16th that I was notified of this incident. And I am upset about the timing of the department's overall response once the burglary became known. I will not and have not tolerated inaction and poor judgment when it comes to protecting our veterans.

Appropriate law enforcement agencies, including local police, the FBI, and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. It is possible that the thieves remain unaware of the information they possess, or how to make use of it. Because of that, we have attempted to describe the equipment stolen, the location from which it was stolen, and other information, in quite general terms. We have not and do not want to provide information to the thieves that might be more helpful as to the nature of what they have. We still hope that this was a common theft, and that no use will be made of the VA data.

From the moment I was informed, the VA began taking all possible steps to protect and inform our veterans. However, there were those in the law-enforcement community who wanted me to wait longer before announcing this theft, so as to pursue leads and keep the bur-

glars in the dark. I chose to inform our veterans nevertheless, but limiting the details of where and when initially, so as not to tip our hand to the robbers. Whether it is one veteran or the numbers we are talking about here today, the VA needed to act in a manner that maintained a balance between protecting our veterans, and informing the crooks.

Another very disturbing aspect of this circumstance is that although it happened on May 3rd, and the VA employee informed his bosses of this fact on that day, I was not made aware, as I said, until May 16th. Equally disturbing is that Federal law enforcement and investigating agencies were not informed immediately, either. It wasn't until May 10th that the VA IG became aware of it. I cannot explain these lapses in judgment on the part of my people. It makes me really angry and disappointed, and after the IG finishes his investigation as to exactly what went on, I plan to take decisive actions.

The VA now also has begun a relentless examination of our policies and procedures to find out how we can prevent something like this from happening again. We will stay focused on the problems until they are fixed. I have formed a special task force under the deputy secretary to examine comprehensively all of our information security programs and policies, to bring about a ringing change in the way we do business. Ever since 1999, the VA has gotten low marks from the IG on its information and a cyber security programs. Last year, the GAO flunked the VA on its cyber security system. This has to change.

This situation is exacerbated by the fact that the Assistant Secretary for IT, who had been at the VA that's the beginning of 2004, has just recently resigned. He came to the VA from the private sector, Dell Computers, and has now returned to the private sector. We do have—and think we have recruited a good replacement, but he is not in place at this time.

Ironically, we, the VA, continue to get very exemplary evaluations on electronic medical records systems. And during Hurricane Katrina, the system and our people performed heroically to evacuate hundreds of patients and save many lives. We are also off to a strong start on our IT reformation to centralize all of our IT applications, except for development.

What this suggests is that we can get this information and cyber security mission done right, also. I am also pleased that just yesterday the President announced his intention to nominate a brilliant recently retired Navy Admiral to head up our office of policy and planning, where this incident arose from. He should be on board very soon.

Additionally, we are taking direct and immediate action to address and alleviate veterans concerns and to regain their confidence. I have taken the following actions so far:

Directed that all VA employees complete the VA cyber security

awareness training course, and complete the separate general employee privacy awareness course by June 30, 2006.

I have also directed a memo be issued requiring all VA employees to sign annually an employee a statement of awareness that includes there are awareness of privacy act, unauthorized disclosing or using, directly or indirectly, information obtained as a result of employment in the VA, which is of a confidential nature, or which represents a matter of trust, or other information so obtained, of such a character that its disclosure would—or its use would be contrary to the best interest of the VA, or the veterans being served.

And certify their awareness on the loss of, damage to, or unauthorized use of government property, through carelessness, or negligence, or through maliciousness, or intent.

In addition, the department will immediately be conducting an inventory and review of all current positions requiring access to sensitive VA data. The inventory will determine whether positions in fact require access to data. We will then be requiring all employees requiring access to sensitive VA data to undergo an updated national agency check and inquiries, and/or a minimum background investigation, depending on the level of access required by the responsibilities associated with their position. Because it has come to my attention also that we know virtually nothing about these people that have access to these enormous amounts of data. For example, this individual having the entire veterans' file, one person who has not to our knowledge had a background check for 32 years.

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

VA is working with Congress, the news media, and veterans service organizations and other government agencies, to help ensure that those veterans and their families are aware of the situation, and of the steps they may take to protect themselves from misuse of their personal information. VA is coordinating with other agencies to send individual notifications to all 19.6 million individuals whose Social Security numbers were stolen, instructing them to be both vigilant in order to detect any signs of possible identity theft, and how to protect themselves.

In the meantime, veterans can also go to www.firstgov.gov for more information on this matter. This is a Federal Government web site capable of handling large amounts of Web traffic. Additionally, the VA has set up a manned call center that veterans may use to get information about this situation, and learn more about consumer identity protection. That toll-free number is 1-800-333-4636. The call

center operates from 8:00 a.m. to 9:00 p.m. Monday to Saturday, and it will as long as it is needed. The call center handles up to 20,000 calls an hour. Through the end of the day on yesterday, concerned veterans had made a total of 105,753 calls to this number.

I want to acknowledge the significant efforts of numerous government agencies in assisting the VA in preparing for this announcement of May 22nd. Agencies at all levels of the Federal Government pitched in to ensure that our veterans had information on actions they could take to protect their credit. Hundreds of people worked around-the-clock last weekend, writing materials to inform the veterans, and setting up call centers and a Web site to ensure maximum dissemination of the information. And I want to personally thank each of these agencies and the people therein for their selfless efforts on behalf of our veterans.

Three nationwide credit bureaus have established special procedures to handle inquiries and requests for fraud alerts from our veterans. Experian and Trans-Union have placed a front-end message on their existing toll-free fraud lines, bypassing the usual phone tree of instructions for placing a fraud alert. Equifax has set up a new toll-free number for veterans to place fraud alerts.

The new procedures became operational on Tuesday. The bureaus report a spike in phone calls 171 percent of normal, and in requests for free credit reports, through the annual free credit report web site. The Federal Trade Commission also experienced high call volumes about the incident earlier this week. On Monday, the Office of Comptroller of the Currency notified its examiners of the theft. On Tuesday, the Office of Comptroller posted an advisory on an internal network available to its banks, and instructed examiners to direct their banks to the advisory. It explains what happened, and asked the banks to exercise extra diligence in processing veterans' payments. The advisory also reminds the banks of their legal obligations to verify the identities of persons seeking to open new accounts, to safeguard customer information against unauthorized access or use, and attaches a summary of relevant laws and regulations.

I briefed the Attorney General and the Chairman of the Federal Trade Commission, the co-chairs of the President's Identity Task Force shortly after I became aware of this occurrence, and they have been very cooperative as well.

Task force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report that they are entitled to under the law.

Additionally, the task force met on Monday to coordinate the comprehensive Federal response, and to recommend further ways to protect affected veterans, and increased safeguards to prevent the recurrence of these incidents. On Monday, following the announcement

of this incident, I also issued a memorandum to all VA employees. The purpose was to remind them of the public trust we hold, and to set forth the requirement that all employees complete their annual general privacy training and VA cyber security awareness training for the current year, by June 30. Following that, all will be required to sign a statement of commitment and understanding, which will acknowledge consequences for noncompliance.

Information security is challenging business. And ultimately, it depends on the integrity and the work ethics of the workforce.

THE CHAIRMAN. Mr. Secretary, if you could summarize your conclusion, please.

SECRETARY NICHOLSON. I wanted to just, for purposes of one graphic, and this was not the equipment that was involved in this so I can use—but this is a hard drive. This little piece of equipment that is smaller than my wallet has 60 gigabytes. The information that we are dealing with here, this entire roll of our veterans and the data on it is five gigabytes. So you could put 12 times that on that piece of equipment that fits easily into one's pocket. All of us carry a cell phone, a Blackberry, or a personal digital assistant, and they contain vast amounts of data.

I promise you that we will do everything in our power to structure a policy and a regulatory regime that make clear what is proper use of this data by our employees. We will train employees in these policies, and enforce them. We have already begun discussions regarding immediate automatic encryption of all sensitive information. We will work with the President's task force very closely. VA's mission to serve and honor our nation's veterans is one we take seriously. The 235,000 dedicated VA employees are deeply saddened by any concern or anxiety this incident is causing to our veterans and their families. We honor the service of our veterans and what they have done for our country, and we are working hard to keep this most unfortunate circumstance from causing them undue pain and anxiety. Thank you.

[The statement of Secretary Nicholson appears on p. 96]

THE CHAIRMAN. Thank you, Mr. Secretary.

To my colleagues, sitting to the Secretary's right is Mr. George Opfer. He is the VA's IG, and it was on purpose that he was not sworn in.

I will also you ask unanimous consent that Thelma Drake and Jim Walsh be permitted to sit at the dais of the Veterans' Affairs Committee.

[No response.]

Hearing no objections, so ordered.

I want to thank Chairman Walsh for being present today. He also wanted to hold his own hearing on this, and given the time con-

straints was not able to, and it's impressive that he is taking equal concern on this.

What we have here, Mr. Secretary, is this Committee working cooperatively with Mr. Walsh and Mr. Chet Edwards on IT. And before you took this job, we had been working hard on IT. And when we couldn't get the VA to listen, we worked cooperatively with not only setting forth our budget, taking out $400 million to get somebody's attention, but the appropriators also followed suit.

I am going to yield so other members can ask questions. The only thing I would like for you to take away from this, Mr. Secretary, is that we intend to have follow-on hearings. I would ask this of you: would you consider offering a reward, say, a million-dollar reward for information that would lead to the arrest or recovery of this device? I want you to think about that. I want you to work with the Department of Justice on whether or not that could be helpful to us. That million dollars is nothing compared to what we are about to expend. You have already sent us a reprogramming notice for $25 million. So I don't know where this could end. But I want you to consider that.

SECRETARY NICHOLSON. We will.

THE CHAIRMAN. At this point, let me yield to Mr. Bilirakis for two minutes.

MR. BILIRAKIS. Thanks, Mr. Chairman. Mr. Secretary, welcome, I guess. Mr. Secretary, in Vietnam you were a true, most courageous hero, a true hero. You received many awards. I doubt that the difficulties you found there are as bad as they are with the VA.

Foundationally this is a problem in the VA. And it is foundational. Others will ask questions regarding this particular instance, and I am as concerned about it as anybody else is. Mr. Chairman, I would like to ask unanimous consent that a two-page document, a written statement by a Dr. Leon A. Kappelman be made a part of the record.

THE CHAIRMAN. Hearing no objection, so ordered.

[The information appears on p. 125]

MR. BILIRAKIS. And I would like to quote from that, Mr. Secretary, very quickly here: "VA has tens of thousands of dedicated, hard-working employees committed to the important mission of serving our nation's veterans and their families. But there is a dark side to the VA. Its bureaucratic culture is unprincipled, profligate, and intransigent. I have seen them ignore Congress, GAO, OMB, and one executive appointee after another. Oh, they know how to play the game to get the executive in Congress to open the budget floodgates, but VA doesn't really care how the dollars are actually spent, as long as it doesn't interfere with business as usual at the VA. I have personally seen VA personnel sabotage and subvert hundreds of millions of dollars' worth of IT projects, and read about billions more wasted on other failures. I have seen a total disregard for one cyber security effort after an-

other. These are only the tip of the iceberg. And why do such things happen at the VA? Largely, because these systems and efforts would make the utilization of budget and personnel more transparent and thereby make accountability possible."

Mr. Secretary, without going into the merits of these statements and that sort of thing, the gentleman is not here for us to cross-examine or whatever. But I think we all agree that there is a problem, a basic bureaucratic type of a problem—at least I hope we all agree. And I ask you, if that is the case, and let's go on the premise that that is the case, can't you do something about it? What is preventing you from—I guess this task force reviewing the entire VA and basically saying, "Hey, we are going to chop here, we are going to change here, we are going to do this, we are going to do that." Is it civil service? Does anything prevent you from doing these things? Are we sort of stuck with this kind of an image, on the premise now again that this is basically true? And I frankly think that it is, based on my experience of over 24 years on this Committee.

SECRETARY NICHOLSON. I would say absolutely—

MR. BILIRAKIS. Your mike, I guess, sir.

SECRETARY NICHOLSON. No. I mean, I am aware of the history of these problems that the Chairman and the Ranking Member have recited. There are others. I am trying to ascertain exactly how many people telecommute. Yesterday, I was talking to an employee on this subject, who was a data expert, who asked somebody to burn some records, some health records for him onto a CD that he needed for a project. It was done, they were mailed to him very timely, tidy. Wrote an e-mail back to them and he said "That was great. It was prompt. I ready appreciate it. Where do you work here? At the VA Central office? Maybe I'll run into you and we can have a cup of coffee."

And the guy says, "I don't work here. I work in South Dakota." And so we have people telecommuting all over this country, and we need to get our arms around who these people are, and what they are like? And they have enormous amounts of data with enormous amounts of potential. Not necessarily because they may be up to mischief, but they may be like the current case where they are negligent. And this is an enormous, troubling situation. But I will say to you that you cannot default to it. We have to fix it. And we can.

MR. BILIRAKIS. Do you have the authority? Do you have the power to fix it?

SECRETARY NICHOLSON. Well, if we don't have it, we will come and seek it. But you raise a good point, Mr. Chairman, because there are things that are called guidelines, which some employees think do not apply because they say "guidelines," and they don't say "directives." And that has a history to it as well, about how expeditious you can get out a guideline versus the time it takes to do a directive.

I will say that the thing needs to be reviewed from tip to stern. We

have queued up I think a very strong leader to come in and replace the person that has left, as the chief information officer who I told you about, who I think did a very good job in forcing us into the transformation that we are now in on centralizing, you know, a portion of IT for business purposes and so forth. But in the information security area, there is a lot needed, and—but it can be done. These things can be fixed.

[The statement of Mr. Bilirakis appears on p. 70]

THE CHAIRMAN. I thank the gentleman. I am going to hit this and go right to Mr. Filner. What assurance can you, Mr. Secretary, give veterans that if indeed these records end up in the hands of identity thieves, that veterans will not suffer financially or otherwise for these illegal attacks on their credit?

SECRETARY NICHOLSON. Well, I think before I could give you that assurance, I'm going to have to work with, the Congress to—and see if it could be funded. If they suffer a loss from this. We are working at a fever pitch with several proprietary companies that are in this business of trying to help monitor consumers, people's credit records for them, and we are meeting with them, reviewing their proposals. With the enormous amount of people involved, there's going to be a substantial cost to that. But that would give—that would give a lot of peace of mind to our veterans, if they suffer a loss, the system of—then compensating that, which I think is something that is owed to a veteran, we'll have to figure out.

THE CHAIRMAN. Mr. Filner, you are recognized for two minutes.

MR. FILNER. Thank you, Mr. Chairman. Who is the highest level official who didn't tell you for 13 days about this?

SECRETARY NICHOLSON. That knew it during that time before, the deputy chief of—the deputy secretary.

MR. FILNER. Is he going to be fired?

SECRETARY NICHOLSON. I'm reviewing all of these issues, Mr. Filner, with a view towards what actions that I'm gonna take, and I'm going to take—but the IG is continuing to do some work on this, and I want to—

MR. FILNER. You know, your responses are incredibly bureaucratic. I don't see, as I have told you, I do not see any passion. I don't see you saying, "I take responsibility." Well, the most dramatic thing you could do to take responsibility is resign. In last years budget, you didn't know there was a war going on, so you couldn't take care of the veterans. Now, your own people do not tell you about the theft of the data of 26 million veterans, and you go through all this bureaucratic rigamarole. You issue something to veterans, "Frequently Asked Questions," and you tell them, "if you have any problem, call your credit bureau, call your bank."

Where is your responsibility in all this? You tell your veterans, "Go

call a number"—which you gave the wrong number, by the way, in your testimony. At least it is different than your press release.

So you are not taking any responsibility. Not only financially but for this management debacle. And you have said time and again as from your press release, there is no medical data here. Is that what you have said?

SECRETARY NICHOLSON. Yes, I said none of the medical records—

MR. FILNER. But you are being very bureaucratic. Isn't there a diagnostic code on here that indicates a specific injury, disability, or medical condition, that is part of the record here?

SECRETARY NICHOLSON. For disability recipients, yes.

MR. FILNER. Well, why not state that clearly and bluntly? Every specific code relates to a specific health condition, and the disability codes are linked to specific individuals by their name and date of birth, and they reveal each disabled veteran's medical problems and conditions; correct?

SECRETARY NICHOLSON. Yes, I—I think it is—that would be correct, yes.

MR. FILNER. So we have medical knowledge floating around here on 26 million people. You should resign, Mr. Secretary.

SECRETARY NICHOLSON. No, sir. It's—I mean that it happens to be those that are getting disability, which is not a small number—

MR. FILNER. How many is that?

SECRETARY NICHOLSON. It's about 2.6 million.

MR. FILNER. Oh, I'm sorry. So only 3 million people suffer from that.

THE CHAIRMAN. Thank you, Mr. Filner.

MR. FILNER. Okay, you should resign one eighth of the time.

THE CHAIRMAN. Thank you, Mr. Filner.

Mr. Stearns, you are recognized for two minutes.

MR. STEARNS. Thank you, Mr. Chairman. I would say to Mr. Filner that Mr. Nicholson has indicated he takes full responsibility. I mean, he said that personally and I understand with his record how upset he is.

But Mr. Secretary, have you fired the employee who lost this information, and why not?

SECRETARY NICHOLSON. He has been put on administrative leave pending further action. There are other people, to go back to Mr. Filner's comment, who are also in my sights as a result of this.

MR. STEARNS. Do you have internal controls? For example, why wasn't this information encrypted? In commercial corporations, they encrypt all this information as a standard operating procedure. How in the world could a person take this outside and not be encrypted?

SECRETARY NICHOLSON. He was—one, he wasn't authorized take it home at all. That we have a standing regulation, standing policy, that anyone who he is authorized to take sensitive information out-

side of their workstation has to have it encrypted.

MR. STEARNS. Okay, do you have in place an internal security operation, with a security chief, with internal audits, and occasionally an outside audit, to confirm that this information is secure, in the Veterans Administration? Just yes or no.

SECRETARY NICHOLSON. Yes.

MR. STEARNS. What is this going to cost the Veterans Administration? Your first diagnosis of this, what do you think this is going to cost and you're going to need from this Committee?

SECRETARY NICHOLSON. That's a tough call, because it's going to depend on what, you know, what level we decide you—

MR. STEARNS. You're talking about 20 million, 5 million, 2 billion?

SECRETARY NICHOLSON. No, we're talking—

MR. STEARNS. I mean, you must have a figure.

SECRETARY NICHOLSON. We're talking—I would say we're talking way north of 100 million.

MR. STEARNS. So you might be talking about half 500 million?

SECRETARY NICHOLSON. It could be.

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

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

SECRETARY NICHOLSON. Yes, sir.

THE CHAIRMAN. Thank you. Mr. Gutierrez?

MR. GUTIERREZ. Yes, I yield to Corinne Brown.

SECRETARY NICHOLSON. Mr. Chairman, I'm sorry but I'm going have to—I'm committed to go to the Senate—

THE CHAIRMAN. Well, I know. We are going to do Mr. Gutierrez, Miller, and then you are gone. So you have four minutes.

MR. GUTIERREZ. Thank you very much. I yield to Corinne Brown.

[The statement of Mr. Gutierrez appears on p. 74]

MS. BROWN OF FLORIDA. Thank you very much. Mr. Secretary, can you see me in my nice pretty red suit? This Monday all of us will be facing our veterans in the Memorial celebration. And I do not know what we are supposed to say. They are going to paint us with the same brush. What assurances will we be able to give about the 26 million veterans' records, how have we notified them? How have we assured the veterans that we are going to work with them throughout the process? And I also want to know, you know, some of our veterans say this could have been an inside job. Have we done lie detector tests with everybody involved?

SECRETARY NICHOLSON. Well, as I said, Congresswoman, I hate this I'm sure more than you do. And I'll take responsibility for it. It happened to my organization, and I think what we are doing is everything we can in the time that we've had so far to try to get the word out to the vets. We're gonna send them each a letter, but we can't send 26

million letters instantaneously. We've found out we can't right now even get 26 million envelopes, but we're underway in getting them. And they will each get a letter. You can help inform us with the 1-800 number, and the Website, the media. Because we want each of them to know what to do, and to know that right now there is no reason to panic. There's nothing, there's no sign that any of this is being used at this time.

MS. BROWN OF FLORIDA. Mr. Secretary, I asked a question. What assurances do we have? Because this identity theft is a very profitable thing. How do you know it wasn't an inside job?

SECRETARY NICHOLSON. Because the local law enforcement authorities that investigated the scene of the crime—that's the first question I asked, by the way—are convinced that it—that it was a real break-in.

[The statement of Corrine Brown of Florida appears on p. 78]

THE CHAIRMAN. Ms. Brown, I thank you.

MS. BROWN OF FLORIDA. Well, are we going to be able to give these questions in writing to the Secretary.

THE CHAIRMAN. Yes. If anybody has questions in writing, please, you can submit them and we will get them to the Secretary.

The last questioner, Mr. Miller, is recognized for two minutes and then the Secretary has to leave. Thank you, Ms. Brown.

MR. MILLER. Thank you very much, Mr. Chairman. I did hear the Secretary in his opening remarks refer to the fact that there were codes that was in this information, so I do think he brought it to this Committee's attention, contrary to my colleague's question.

Two things: number one, why would an employee take this information home?

SECRETARY NICHOLSON. Congressman Miller, he took it home to work with it. He was working on a project where he was trying to streamline a telephonic polling that we do of veterans periodically, and it's done randomly, that they're called and asked a series of questions, which is, you know, benign. We're trying to find out what's going on in their life, how we're doing with them, how they're doing, and so forth, and he thought he had a way that he could make this more efficient in the selection of the veterans that we were calling, and he took this data home to work it.

MR. MILLER. And my second question and as of course, we are all concerned about the financial implications to the veterans, but I also want to know, you know, the financial institutions, banks, credit unions, retailers, anybody that may get caught up in this; who is going to be responsible for the cost that may be incurred for private entities out there?

SECRETARY NICHOLSON. Well, you know, I suppose the ultimate answer to that question is going to be up to you all that make the laws.

I mean, we're—it happened because of—it happened because of us.

MR. MILLER. Well, let me ask it this way: what would your recommendation be?

SECRETARY NICHOLSON. Well, my recommendation would be that we'd be responsible for it. We caused it.

MR. MILLER. Thank you. That is what I wanted to hear.

[The statement of Mr. Miller appears on p. 83]

THE CHAIRMAN. All right. Mr. Secretary, thank you very much. You and Mr. McClain are excused. Thank you.

I would now like the other witnesses to please come to the table to replace the Secretary and the General Counsel. If staff could help them. What we may have to do is bring your chairs to the front.

To all of my colleagues, while all this administrative shuffle is occurring, the team that the Secretary is leaving behind is the team that is responsible for cyber security and in charge of plans and policy.

There is a hearing on the Senate side that starts at 10:00 a.m., and that is the purpose of the Secretary's and General Counsel's exit. But what I wanted to insure for all of my colleagues is that as the secretary leaves, these are the individuals who are in the responsible positions.

Ms. Berkley?

MS. BERKLEY. Thank you, Mr. Chairman. With all due respect, and I am sure these are the men and women that do the nuts and bolts on this issue, but I was hoping to talk to the Secretary, and have an opportunity to question him. Will he be available to us? It seems that something this important, one hour in front of this Committee simply is not enough. Oh, I'm sorry, 45 minutes.

THE CHAIRMAN. 45 minutes. We will entertain that. WWe are going to have follow-on hearings. If the Secretary is necessary we will bring the Secretary back before the full Committee. We can do briefings to members. I will seek your counsel.

MS. BERKLEY. I would appreciate that. Thank you, Mr. Chairman, and I am going to the IR Committee markup.

THE CHAIRMAN. All right, thank you.

All right. Mr. Michaud, you are now recognized. The Committee will come to order, please. People can take seats and please close the door. If somebody can help out and make sure all the nameplates can be read by the members, please.

I'm sorry, Mr. Michaud. I just wanted to say good morning to you.

MR. MICHAUD. Good morning, Mr. Chairman.

THE CHAIRMAN. Good morning. Prerogative of the chair, I would ask unanimous consent to rescind the former unanimous consent to yield to members for two minutes, and now go back to regular order.

[No response.]

Hearing no objection, so ordered. Mr. Strickland, you are now recognized for five minutes.

MR. STRICKLAND. Thank you, Mr. Chairman. Mr. Chairman, I also am sorry that the Secretary is not here. I wrote down verbatim what he said to us, "I am the person ultimately responsible for our veterans, and therefore, the responsibility for what has happened rests with me." I am not sure what it means to take responsibility. I think it ought to mean more than just uttering those words. I think it should imply some decisive action. And quite frankly, if this was the first concern I had about the Secretary, I may be a little more charitable in my response. But quite frankly, I don't think the Secretary is up to this job, and I do hope he takes this opportunity to reconsider whether or not he should remain in that position. I quite frankly have serious questions about whether or not he should.

I have a question regarding the fact that many states have enacted privacy laws that in some cases certainly supersede the requirements that may be currently in place under the VA's system. Thirty-five states have introduced data security legislation. Twenty-two states have actually enacted such security laws, one of those states being my home state of Ohio. Can someone at the table inform me as to whether or not the VA takes seriously the states that may exist at the state level, and makes efforts to comply with those state security laws, if they are more stringent than those currently embraced by the VA?

GENERAL HOWARD. Sir, Bob Howard. I have not seen any evidence that we have addressed that for the states. One of the efforts that the Office of Information and Technology has been undergoing, you know, throughout this incident is trying to determine what guidelines and policies exist. I have not seen that, unless any of my other colleagues have.

MR. STRICKLAND. Can someone give a definitive answer as to whether or not there was a difference in requirements between State and Federal law? Or there was a conflict there; would it be likely that the VA would attempt to comply with those more stringent state laws, within the state?

MR. DUFFY. Congressman, it's my understanding that Federal law supersedes state law. I believe however that the department makes every effort to meet state law where it's consistent with our own rules and standards of practice.

MR. STRICKLAND. Okay, thank you. I am curious as to why an employee would take this kind of material home. I mean perhaps he is just a very dedicated employee that is willing to work above and beyond what may be required of him at his official worksite. Why was he not doing this work during regular work hours? Can someone speak to me about the staffing needs that may be inadequate, that would result in an employee taking such action, in terms of taking

this kind of data to work on it at home rather than doing it at the facility, or at the worksite?

MR. DUFFY. Congressman, I think in this particular instance we have an individual who believed that with—on his own time, and without the din of daily work; telephones and meetings and the like, he would be able to apply his own time and talent to resolving what to him was a basic problem of reducing substantially the size of a survey instrument that we were attempting to create.

I would say to you that he fully understood that it was inconsistent with departmental policy to take that information home with him, that he had no right to remove the materials from his worksite. He did it with all of the best intentions, at least that's my personal opinion. There was no malice a forethought. I don't believe that there was any sinister intent here. He did it because he wanted to be more productive and to come back with a problem solved. And in all candor, I think we attempt to promote individual initiative on the part of our employee workforce. However in this instance, it was contrary to what the rules and regulations require regarding safeguarding sensitive personal identifier data.

MR. STRICKLAND. Thank you. Just sitting here listening to Secretary estimate the potential cost, I think he said it could be over $100 million. And if, as the Chairman has suggested, we have the responsibility to make whole any veterans who have been harmed, I can see where that number could go much, much higher. Just sitting here thinking, the latest I have heard the cost of the Capitol Visitor Center was I think something over $500 million, and the work has been going on for years and years, and we know what a massive undertaking that has been. So just kind of putting this in perspective, if the lower cost estimates of $100 million hold forth, we can see what an incredible cost this is going to be to the taxpayer, to the Federal Government, and ultimately to the VA administration, and that means ultimately to the individual veteran, in terms of how they are served. So you know, I don't think this is a little thing, and I don't imply that any of you believe it is a little thing. I think this is just incredibly serious. It is going to be very very costly, even if the best case scenario it is that there is no use of this data for, you know, for nefarious purposes. It is still in to be incredibly, incredibly costly. And it is just such an unfortunate incident.

Mr. Chairman, I thank you for the hearing. I do hope that we could have the Secretary back at some point in the future, and I yield back my time.

THE CHAIRMAN. I thank you, Mr. Strickland. I thank you for your leadership. Mr. Strickland and Mr. Bilirakis, Mr. Filner and I want to work with both of you because at some point, where do we retain this at Committee; where do we do a handoff to the O&I Subcommittee? We want to work with you with regard to our jurisdictions.

I have asked Mr. Opfer to remain with us, as he is not going over to the Senate. This is the VA IG.

And at this point, I am going to yield to Mr. Bilirakis, who has asked for his three minutes.

MR. BILIRAKIS. Thank you again, Mr. Chairman. Mr. Opfer, who do you work for?

MR. OPFER. Sir, I work for the President and—

THE CHAIRMAN. Scoot up to a microphone.

MR. OPFER. Sir, I am a presidential appointee, Senate-confirmed, which means I can only be removed by the president.

MR. BILIRAKIS. Okay. Very good, that is what I wanted to hear. Mr. Opfer, you know, these things happen and they have been happening. The same sort of thing has been happening over a period of years. I know we have had secretary after secretary after secretary here. And you know, when the media is here, particularly, we speak very brusquely and that sort of thing in order to make the media and whatnot. But you know, in my opinion, as I indicated during my two minutes, two minutes-plus, it is culture. It is a culture at the VA. Maybe it is a bureaucratic culture of all the agencies and departments. I don't know, but certainly at the VA.

Let me ask you, sir, when were you made aware of the theft of the data?

MR. OPFER. The Office of Inspector General and I particularly were never notified by the Department of theft of the data.

MR. BILIRAKIS. You never were?

MR. OPFER. Never were.

MR. BILIRAKIS. Never were. How about that? Yeah, how did you learn? You read about it in the newspaper?

MR. OPFER. What happened was on May 10th, the information security officer of the Office of Inspector General was attending a normal monthly meeting in the department. And at that meeting, one of the ISOs mentioned that an employee of VA had lost data which was stolen from their residence. That information security officer, who is not an agent, not an investigator, came back, reported to his supervisor, and the next day it was reported into our office of investigations. We had no information other than an employee had lost data that was stolen in a burglary in their residence.

MR. BILIRAKIS. And what was your reaction—

THE CHAIRMAN. Can you pull that microphone closer to you. We can barely hear you.

MR. BILIRAKIS. Yeah. What was your reaction to that?

MR. OPFER. I was not notified then because the information was very sketchy. Our Office of Investigations dispatched agents on Friday, May 12th, to try and locate the information security officer who had the information, and also to locate and start the interview process of the employee who had had their residence burglarized.

The information security officer that had the information was not working. The agents attempted to locate him at his residence and left messages there, as well as at work. It wasn't until Monday, May 15th, that the Office of Investigations located the subject employee that had the burglary, and we conducted the interview.

[The statement of Mr. Opfer appears on p. 101]

MR. BILIRAKIS. Wow. Well, there you go. Yeah, I guess the Chairman is suggesting I do this. Misters Duffy and McClendon, why did you not notify the IG?

MR. DUFFY. I'll begin first. Let me begin by noting that the first I was notified of it was on Friday morning, May 5th. And my notification was in hallway conversation with the IT specialist who serves as both our security and privacy—

MR. BILIRAKIS. In a hallway conversation?

MR. DUFFY. Yes, sir. He indicated to me at that time that there had been the burglary of one of our data analysts, that some sensitive data and information may have been burglarized. At that time, I asked him to do two things: first, attempt to identify and document for me all of the data sets and personal identifier elements that may have been compromised. The second thing I asked him to do was to confirm for me of what the formal process for notification is in the department regarding a matter such as this; that is, where information or data has been compromised.

He agreed to prepare for me a memorandum that would identify for me, to the best of his knowledge, the information that might have been compromised. With respect to notification, what he told me was that the process was to notify the cyber security systems operations center, and that they have an incident management process in place for responding to these types of issues.

Later that afternoon, sometime around 3:30 in the afternoon, I received the first initial memorandum from my IT specialist that identified in rather generic terms the data and the information that appeared to have been stolen. I talked at that time with Mr. McLendon, who is the deputy assistant secretary for policy. He asked for an opportunity to have a member of his staff, who has dramatically more familiarity with the data sets, take a look at it, and review and validate that information, and indeed he did that.

Monday morning, the eighth, we had a new, more detailed memorandum on the nature of the information that was contained on the hard drive that was stolen.

On Tuesday the ninth, early afternoon, I had a meeting with the department's chief of staff, Tom Bowman, and informed him at that time for there had apparently been a burglary, and that some significant personal data may have been compromised, and indicated to him at that time that I thought it important that senior leader-

ship get together and identify exactly what our responsibilities were regarding notification to the beneficiaries whose information might have been compromised.

MR. BILIRAKIS. Did you ever take in consideration when you should notify the IG?

MR. DUFFY. Sir, with all due respect, my understanding was that all that would have been processed through the incident management reporting system in cyber security, in the SOC.

THE CHAIRMAN. Oh, so you are blaming who?

MR. DUFFY. I'm not blaming anybody. What I'm telling you is what was in my mind. And what was in my mind was two things: one is that we had made formal notification through our IT systems specialist to cyber security, that they have that responsibility. The other point that I would make to you is that when I had information in hand, it was provided up the chain to those above me regarding the fact that the information may have been compromised, and our need to take some affirmative action.

THE CHAIRMAN. Mr. Bilirakis, may I?

MR. BILIRAKIS. Well, my time as long up. Yes, sir, by all means.

THE CHAIRMAN. Mr. Cadenas, you are sitting right there. What do you think about what Mr. Duffy just said?

MR. CADENAS. Well, sir, because we get a number of reports on a regular basis, the SOC, the Security Operations Center, did receive this notification. But before it's escalated, it must be confirmed that a—because the original message that came in says "possible compromise." So part of the process is we contact the information security officer to validate if in fact it has been compromised.

A number of days had lapsed. We started beginning our own investigation, asking additional questions, and the information was not forthcoming, as well. Still had no valid confirmation that the information was lost or stolen or anything to that effect. We're still dealing with the compromise, potential compromise, of information.

During the course of the process, we asked the information security officer to also contact the privacy officer based on the information that you identified that was on there. We later found out—I don't know if it was my office or the individual himself, there was a privacy office ticket violation opened up on that.

I found out about this incident on the 16th, as well, and my team, they were trying to conduct their due diligence to validate that this in fact had happened.

THE CHAIRMAN. Do you work with the IG? Do you ever report these incidents to the IG?

MR. CADENAS. Well, yes, sir. We have understood rules of engagement. Once it reaches a certain level, any incident reaches a certain level, we back off because now it could be a potential criminal investigation, and then we hand off.

THE CHAIRMAN. But the IG has testified that he has never even received this yet. So when does this rise to the level of concern?

MR. CADENAS. Well, in looking at the entire incident, sir, because this does not fall—and I don't mean to sound like the bureaucracy here—but because it does not fall under cyber security, this was not a cyber security attack or hack, we tried to follow up with the privacy office, and we ran it up the chain. This is a privacy issue.

THE CHAIRMAN. Okay. It is not your problem, I guess now it is not yours. Now it is not the privacy guy. We don't have the privacy guy at the table?

GENERAL HOWARD. It is a bureaucracy, Mr. Chairman, and it is culture—

THE CHAIRMAN. All right, let me just pause a moment.

GENERAL HOWARD. Mr. Chairman—

THE CHAIRMAN. Ms. Brown, you are now recognized. Hold on, I know you want to say something. But Ms. Brown wants her three minutes. I need to yield to her.

Ms. Brown, you are recognized for three minutes.

MS. BROWN OF FLORIDA. Well, I hate to break the chain. I am going to let you answer your question, and then I will go to mine. Just finish what you were saying.

GENERAL HOWARD. I just wanted to comment that—that there's the constant refrain of "it's just a large bureaucracy." It is indeed a large and complex structure, but it is not so large that we don't talk to each other. And the truth is that a number of days passed where the information was being reviewed and validated. The burglary took place on the third. On the fourth, the employee did not report for work. He was told by—as I understand it, the home had been ransacked, and he had been told by police to secure his premises and the like. So he was not in. He did not come in until the morning of the fifth, on that Friday. That's the day when Mr. McLendon and a senior data analyst sat down with the individual and talked specifically about the nature of the data that may have been compromised. And it was only after a full day of discussions with somebody who quite candidly appeared to be fairly distraught about the whole incident.

MS. BROWN OF FLORIDA. Well, do you know this is a meltdown? And the secretary said he didn't find out about it until the 16th? When did the secretary find out?

GENERAL HOWARD. He indicated the 16th.

MS. BROWN OF FLORIDA. It is a complete failure. Since 2001, has your office requested changes that would limit anyone's ability to remove VA data to a personal computer or storage device?

MR. CADENAS. Yes. Yes, ma'am, the office of—

MS. BROWN OF FLORIDA. Yes, what was the result of that action?

MR. CADENAS. We do not have the authority to enforce any such request.

THE CHAIRMAN. Ms. Brown?

MS. BROWN OF FLORIDA. Yes, sir?

THE CHAIRMAN. If you pay really close attention to the response that he just gave, what I just learned from last night, and I want to make sure I get to all the members, I have a March 16th, 2004 document from Tony Principi, when he was the Secretary. And he instructed that the chief information officer be the individual that is responsible. We need somebody in charge of all this. Then we have the General Counsel. He writes an opinion. And in his opinion, he says that the CIO does not have that authority. And matter of fact, Mr. Cadenas here with cyber security can only do compliance. He does not have the authority to demand anybody to do anything. He can only say whether somebody has complied or not.

I yield back.

MS. BROWN OF FLORIDA. It is a complete meltdown. The system is not working for the veterans.

To your best knowledge, does anyone other than VA employees take home or store veterans' personal information; names, Social Security, date of birth, financial, medical, anywhere in VA? Is there a statute, regulation, or policy, that allows that action?

GENERAL HOWARD. Ma'am, we have procedures in place to permit telework, virtual connections, you know, through laptops and what have you. The only clear guideline that I have personally seen on the rules of the game, regarding taking information away from a VA facility, is contained in the guideline that the secretary mentioned during his testimony. And there are two specific items in that guideline: one is to take information such as what we are talking about away from a VA's facility, the individual has to have permission. And the second key part of it, it must be encrypted. Clearly, both of those elements were not followed. But that guide—it's in a guideline. It's not a directive.

MS. BROWN OF FLORIDA. Oh. God, we need help. This is unbelievable. I am going to yield my time, but I can tell you that this system is a failure. I mean, we are not talking to each other, we are not communicating. You can't tell me how many other people have this information, that could have this data at home. It is not illegal to do it. It is a regulation, it is not—do you hear what he is saying?

[Laughter.]

MR. BILIRAKIS. What the gentle lady yield?

MS. BROWN OF FLORIDA. Yes.

MR. BILIRAKIS. Yeah. The VA Inspector General in his November '05 report entitled "Major Management Challenges; Fiscal Year 2005," stated that, quotes, "VA has not been able to effectively address its significant information security vulnerabilities and reverse the impact of its historically decentralized management approach,"

end quotes. And there you are.

That is why I keep going back to this culture business, this environment business, because that is where the problem stems from. Mistakes are made. I mean, we are all human beings. But continually, continually, and the frustrations of IT, and the lack of security. Thank you, Mr. Chairman, thank you for—

MS. BROWN OF FLORIDA. I think it has to go back with whose responsibility it is. I think the ultimate responsibility is with us. As a co-equal branch of government, we have not done our job.

THE CHAIRMAN. Well, we passed the CIO Bill, ma'am. When I look at this for the members, I would ask unanimous consent that the documents which I referred to in my discussions with Corrine Brown be submitted for the record. And in particular, the memorandum from Secretary Principi dated March 16th, 2004 be entered into the record.

[No response.]

Hearing no objection, so ordered.

[The attachment appears on p. 135]

THE CHAIRMAN. I would ask that the General Counsel's memorandum dated April 7th, 2004, be entered into the record.

[No response.]

Hearing no objection, so ordered.

[The attachment appears on p. 136]

THE CHAIRMAN. The Secretary Principi, this is what he says:

"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, the CIO, Bob McFarland, with responsibility to devise and implement a department-wide cyber security program under the Federal Information Security Management Act."

We passed that act.

"I expect all employees to fully support and cooperate with the implementation of the department's cyber security policies. It is my intention to ensure that the 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, personnel regulations, are being drafted to effectuate my intentions."

We have the acting CIO in front of us, former Major General Howard. Now the problem is the General Counsel comes along and does

an interpretation and says they CIO does not have these authorities. And that is what we now end up, we have got a mess in that bureaucracy.

MS. BROWN OF FLORIDA. Mr. Chairman, could I—30 seconds?

THE CHAIRMAN. Yes ma'am.

MS. BROWN OF FLORIDA. Mr. Chairman, we often passed bills, and then the agency will come up with regulations that's just opposite of what we pass.

THE CHAIRMAN. Well, that is why we have been working on this Committee in a bipartisan fashion, ma'am, to bore through this, but we have a bureaucracy that is recalcitrant. We have individuals sitting at this table.

Yes, Mr. Duffy, I just saw your reaction. You and I have a complete disagreement with regard to centralization versus decentralization. You fought us all along. You go, "Oh, this is my business. Stay out of my world."

Well, now that the problems we have got. We said, "Okay, we are going to leave it to you, we are going to leave it to Mr. McLendon," and look what we have got in a decentralization.

MR. DUFFY. Mr. Chairman, with all due respect, I have never taken a position on centralization or decentralization of IT. It has nothing—

THE CHAIRMAN. Thank you for your views, Mr. Duffy.

MR. DUFFY. —it affects me only on the margins. And trust me, I have not entered that—

THE CHAIRMAN. Well, that's one hell of a margin for a veteran.

MR. DUFFY. Well.

THE CHAIRMAN. I yield to Mr. Miller.

MR. MILLER. Thank you, Mr. Chairman. I have already asked my questions. I will yield back my time.

THE CHAIRMAN. All right. I have been asked to meet with the Speaker.

MR. BILIRAKIS. [Presiding]. Okay, where are we here? Mr. Boozman?

MR. BOOZMAN. Yes.

MR. BILIRAKIS. Mr. Boozman is recognized for five minutes.

MR. BOOZMAN. Yeah, I would like to know a little bit about what happened. So the place was broken into, and not just the computer was stolen, but the whole place was ransacked? I think somebody alluded to that earlier.

MR. MCLENDON. I'll be glad to answer that, Mr. Boozman. The employee had left to go home from work. His wife is also a government employee. She arrived home to find the home having been broken into and ransacked. She called her husband and reached him on the cell phone when he was I guess in the parking lot fixing to get in his car to drive home. As best I understand it, she arrived home some-

where around maybe 3:30, 4:00 o'clock in the afternoon. So they did the notification to the police. When he finally kind of got a handle on what was going on, he called the office. The secretary got ahold of me, and I called him just a few minutes later, probably somewhere around 5:30, quarter of six that afternoon.

He was very distraught, as you can imagine. He was also concerned because his wife had found a break-in, and he was kind of after-the-fact concerned that maybe somebody was still in the house. He described that the house had been ransacked, that they had gone through drawers upstairs, and drawers all over the house, and that things like change that we would normally put in a glass jar or something was missing out of drawers. He described kind of the state of the house, and how they had broken into a back window. And then he said that, you know, that they had taken—he was surprised at things that they had passed up in the house, you know, like silver and those kind of things, but it appeared that they had grabbed his personal laptop and external hard drive when he had—when they had left.

And it was at that point that just straightforwardly, and I have to give the individual credit for this, that he said he believed that there was some veterans' data on his hard drive. And I have to say that to this day, that that individual does not understand that there are many people who would not have self-reported that information. But he did, and he acknowledged on the phone that he knew that he was not supposed to have done that, and he just had no explanation as to why. And clearly, he was just very distraught at the incident.

So he was—the police were still there. He said he needed to work with them. He had already notified VA security office about the incident. He was not at work the next day because the police had asked him to secure his home and be available for questions and whatever.

Early the morning on Thursday morning—and also I have to say, after I talked to the gentleman that afternoon, I contacted the individual in our office who is the most technically knowledgeable about the details of the data and systems, to also called the individual to try to elicit more information from him. And so then he reported back to me, so that early Thursday morning, that individual, Dat Tran and I sat down with the information security officer for the office of policy planning to relate everything we knew up to that point, and to say, "Okay, now you tell us what the process is and what additional information that is gonna be required."

And he very matter-of-factly laid out what he said he knew the procedures were, just like Dennis acknowledged, about what was gonna happen, who he would be generally talking to, and he says if I need any more information, or when I do, I will come back and tell you.

MR. BOOZMAN. So if he hadn't self-reported it, then we really would have had no way of knowing that the data ever left the office, or whatever.

MR. MCLENDON. No, sir, we wouldn't have. And I think it's important to remember that this is not a case in which information was put up on the Internet for wide public access. It was, he had taken some disk from work that he was using, to use on his external hard drive at home, to continue to do work. He's a Ph.D. analyst—

MR. BOOZMAN. What are the police saying? I mean this happens all the time, you know, sadly, in the sense that places are broken into. What is the customary stuff, when you steal electronics—first of all, who are they saying are the likely thieves? What kind of profile do they have? What do they customarily do with this stuff when they get it?

MR. MCLENDON. Depends upon—I'll just say from my personal experience, I have been through this, it could be anywhere from kids to more professional individuals who are looking for easy prey and things they can quickly turn a dollar on. I don't believe that the police report or the FBI has completed their investigation yet, so we will just have to wait and see what they say.

MR. BOOZMAN. Thank you.

MR. BILIRAKIS. The gentleman's time has expired.

MR. BOOZMAN. Mr. Chairman, also, could I have a statement put in the record, please?

MR. BILIRAKIS. Oh, yes. That, you see, took place before you came in.

MR. BOOZMAN. Okay, thank you.

[The statement of Mr. Boozman is found on p. 89]

MR. BILIRAKIS. Mr. Salazar to inquire.

MR. SALAZAR. Thank you, Mr. Chairman. We do appreciate this.

As I hear more about what happened and the items that were taken during this burglary, it seems like you were talking, Mr. McLendon, that silver was passed up, and other things. It almost seems to actually send up a red flag because it seems like the computer was targeted.

We introduced legislation a couple days ago. It is HR-5455, the Veteran's Identity Protection Act, which will actually provide free credit reports for veterans who might have been affected by this for a period of one year. Could someone in this panel maybe address that? And do you think this is something that should be done?

MR. HENKE. Sir, I am not familiar with the particular legislation you cite, but obviously our first concern is to protect veterans. And as the Secretary has indicated, he would be more than happy to work with the Congress to find ways to do that and take those steps that are necessary.

MR. SALAZAR. Well, what this particular legislation will actually do, is provide free credit reports for veterans for a period of a year to make sure that in case some of their credit information has been

breached, that it would not necessarily have to come out of their pockets. Of course, you know, the first credit report is free for any time that you apply. But after that, you have to pay for it.

Of course this will cost taxpayers, and VA maybe, an incredible amount. I think the price tag is 1.5 billion for the first year. Would you be supportive of that?

MR. MCLENDON. Let me just make a general comment. I think it's very fair to say that the department certainly takes it seriously. There have been a lot of discussions over the last week about exactly how could we do something like that, what the mechanics would be, what the logistics are associated with doing that, how that would occur. And the department is actively looking at how to bring that about, those kind of things, right now.

MR. SALAZAR. Thank you. Mr. Chairman, there are a lot of people here that want to ask questions, so I would like to submit my full statement for the record.

MR. BILIRAKIS. The chair appreciates that.

[The statement of Mr. Salazar is found on p. 93]

MR. BILIRAKIS. Mr. Moran, to inquire.

MR. MORAN. Mr. Chairman, thank you very much. Perhaps what is most troublesome to me about this scenario is the failure to communicate to the Secretary in what I would consider a timely fashion. And I understand Mr. Filner asked the question earlier about what level this information reached, as far as the hierarchy of the Department of Veterans Affairs. And you know, I am interested in knowing, you know, why the Secretary was not notified immediately. I would at least like to think in my own professional life that something dramatic happened that I would be at the top of the list of people who would know. And I don't know whether it is a concern with the attitude, I should have a concern with the attitude of VA officials as, "This is something we don't want to tell our superiors." Or it is a distance by the Secretary; he is not there, interested, available.

I cannot imagine that is the case, but there is something—again, Mr. Bilirakis's word, the "culture"—that is troublesome to me, that we wouldn't immediately go to the top leadership, the leader of the Department of Veterans' Affairs with this kind of information. So I am interested in any thoughts that you all have as to what the problem would be that this would not be seen at the VA as an incident that would be immediately reported to the leader of the department. I am curious just to know whether in the course of time you have observed other departments, studied what their security measures are, how this is prevented. I am interested in knowing if there are other departments out there within the Federal Government that are role models that the Department of Veterans Affairs should have been following. Or other disasters waiting to happen at other cabinet-level

positions, other departments within our Federal Government, that we as members of Congress should be aware of.

And finally, a more practical question: my constituents, my veterans are calling, asking, "you think that information about me or my spouse are in these records?" Example, a Vietnam veteran discharged in 1972 who has now deceased, his spouse, his wife is calling to say, "Is there any chance that there is information there about my husband or me?"

And so if there is information that you can provide as to how we can answer the calls we are receiving as to who is included in this 26.5 million veterans whose records are released.

I thank the Chairman. Anyone, respond to any or all of those.

GENERAL HOWARD. Sir, you ask a number of questions. I would like to recommend we answer all of them for the record. But let me address a couple of them. You mentioned the other government agencies. One government agency that is a role model is Social Security. You know, they constantly get very high grades with protection of information. I know that for a fact.

There are others besides VA that don't get high grades, I know that also. It is a very real problem in other government agencies, I don't recall the scores. When you say the Veterans' Affairs is fairly low, you're exactly right. You know, our grades have not been high. But as I say, there are role models. There are definitely things that we can do to improve things.

MR. MORAN. What you are telling me is that what has occurred at the Department of Veterans' Affairs may not be an anomaly, but something we could to see repeated elsewhere?

GENERAL HOWARD. Sir, with respect to the magnitude it may be an anomaly. You know, what's significant—obviously, the loss of any data is a serious problem, but it's the magnitude of this one that is so troublesome. I suppose it could occur in other government agencies, but you know, I really can't comment on that.

MR. MORAN. Any explanation of the nature of the VA that the Secretary would not know this immediately?

MR. DUFFY. Congressman, I'll make an effort to answer it. And that is that in all candor, I don't believe anybody had a true appreciation originally of the magnitude, the size of the data set that was lost. When I first heard that there was a BIRL's extract, while I knew from my own experience that the BIRL's record is a large data set with millions of records, my own thought was, "Well, he probably extracted some very small subset of that record." And once notified, I think what we did was we attempted to do due diligence. And that is, we first of all attempted to get the facts. And once we had the facts in hand, we provided them to the chief of staff, who in turn said, "Well, let's work with the general counsel to assess what our obligations or responsibilities are here."

And it was that process that took some time. Now, should the Secretary—in hindsight, obviously the Secretary should have been notified earlier. But again, I think originally there was no sense of the size or magnitude of the data loss.

MR. MORAN. Can you assure us that there was no cover-up involved?

MR. DUFFY. I can certainly assure you of that from my personal vantage point and from dealing with the individuals that I have dealt with. There absolutely was no effort, no attempt at all. We made every effort to do what we thought was the right and prudent thing.

MR. BILIRAKIS. The gentleman's time has expired.

MR. MORAN. Thank you Mr. Chairman.

MR. BILIRAKIS. Ms. Hooley to inquire.

MS. HOOLEY. Thank you, Mr. Chair. This is really frustrating, and there are so many troubling things about this incident. This is one of a string of data breaches that have happened in all kinds of other industries, and is why I think we need some kind of data security legislation, which I have championed in the Financial Services Committee. I have also introduced legislation that would require VA administration to provide veterans six months' of free credit reporting, that there would be authorized funding, and that you would also have negotiating powers so that you can get the best price for the monitoring services. There has been a lot of estimates about what this would cost. We have gotten estimates anywhere from 25 million to $1.2 billion, so it is a wide range. And hopefully, we can narrow that piece down.

My question is, if this legislation passes, could you implement that in a very timely manner to help our veterans? And are you prepared to negotiate the best price for credit monitoring services? You can answer that now or wait until I am finished.

And I guess the third question would be, could you start that process right now? Do you have to wait for legislation to pass? Can you start the process right now?

Fourth, right now you are giving I think some good advice, but it is very reactive. You're saying, you know, "Please monitor this, call your bank," you know, all of those things. But why aren't you more proactive? For example, you could say to every veteran, "You could put a fraud alert on your credit report" If they put a fraud alert they automatically get a free credit report. Right now, even without having their information taken, or stolen, or breached, they can get a free credit report every year. I mean, that is the law, currently. And if they get one from each credit bureau, they can do one credit bureau, and then another credit bureau, and another credit bureau, they can get a free report every four months.

So it seems to me there are some very proactive things you can tell all of the veterans that have had their, security breached, you can

give them that proactive information today. And my question is, are you doing that; and if not, why not? Then—

MR. BILIRAKIS. Wouldn't you not like to get some answers to those?

MS. HOOLEY. Yeah, I am ready to get answers any time they are ready to give them to me.

MR. BILIRAKIS. Yeah.

MS. HOOLEY. And then I have one last question.

MR. BILIRAKIS. Good.

GENERAL HOWARD. Some of that information is on one of the Websites that the veterans are referred to.

MS. HOOLEY. Some of the information. I know what is on your Website, and it is very reactive, saying "Monitor this," but it is not proactive, and there are some very specific things they can do that will make a difference on whether or not they have their identity stolen, which is a huge problem if that happens.

GENERAL HOWARD. That's what I meant. Some of that—things that they can take, what they are authorized, is available.

With respect to additional items like credit monitoring and things like that that Veterans' Affairs could pay for, I'll defer to Bob Henke. We get into budget issues and authorities to pay for that sort of thing. Obviously, we're prepared to do anything that we need to do, but I'd let Bob comment on the financial aspect of it.

MR. HENKE. Ma'am, I went to the Websites that we have set up for this particular incident, and it does link you to the opportunity to get a free credit report, and for every member to put a 90 day fraud alert on their individual accounts, so that information is out there, through both the VA Websites and firstgov.gov.

MS. HOOLEY. Is that your recommendation? I mean, do you recommend that happen, that they do that?

MR. HENKE. That members—

MS. HOOLEY. I mean, it is on there. When they go onto the Website, what are the things that you tell them that they can do, the first things they can do?

GENERAL HOWARD. Monitor their information.

MS. HOOLEY. Monitor their information. Which is good advice. But there are some proactive things they can do immediately. You say, you know, Put a fraud alert on. What does that mean if they do that? How long does that last? It lasts 90 days. They get a free credit report. I mean, I think that is the kind of proactive information you should be giving your veterans.

MR. MILLER. Congresswoman, I think it's fair to say that the Secretary and this task force is indeed looking at a whole host of different affirmative steps that the department can take, all the way to perhaps providing credit monitoring. What we need to do is lay out what those potential options are, what the costs are that are associated with them, and what authorities we have. I think the secretary made

clear that we were going to do everything in our power to mitigate whatever adverse impact this may have on the veterans whose data was compromised—

MR. BILIRAKIS. The gentle lady's time has expired. But Mr. Duffy, with all due respect, you know, meetings, consultations, "we are looking at it, we are trying to decide what authority we have." In the meantime, a lot of bad things can be happening. I think that's what the gentle lady is saying, sure.

MS. HOOLEY. I just want you to take some leadership. That's what I want you to do. I want you to take some leadership.

MR. BILIRAKIS. Yeah, well.

MS. HOOLEY. Excuse me, Mr. Chair.

MR. SALAZAR. Especially for people who don't have computers.

MR. BILIRAKIS. Well, that is another point. There are many veterans out there who don't have computers. So you can't just look at that one particular way to do it. There are public service announcements that all the television stations as broadcasters are required to make available.

GENERAL HOWARD. And the department is taking steps now to send individualized letters to every veteran that we can indeed identify, to notify them personally. You are absolutely right about not everybody having a home computer.

MR. BILIRAKIS. Well again, as Ms. Hooley said, take some leadership here. Let us not just sit back and, "we will let these bad things happen"—then the cow has already left the barn, or whatever the proper terminology is.

Let us see, Mr. Bradley to inquire.

MR. BRADLEY. Thank you very much, Chairman Bilirakis. I would just like to start out by thanking you, and Mr. Filner, and Chairman Buyer, for your leadership in making sure we have this hearing in an expeditious fashion.

Not to beat a dead horse, but my concern I think with some of the other more recent questioners is the 27 million people that have potentially had their data stolen, and it may well be used. Let me try to encapsulate what I think you have said today in terms of procedures that are in place, or about to be in place:

You are going to write a letter to all 26.5 million, but you don't have envelopes, so we don't know when that is going to happen. There is a Website. The question that Ms. Hooley asked is why is there no fraud alert on it? There is a call center with an 800 number. Are there enough operators, and is the information clear? There are expedited procedures at credit bureaus. How helpful that is, that would be a question I would have. Equifax has a toll-free number.

We don't know that there are any problems yet, which I guess is good news. Secretary Nicholson I think made a pretty clear statement. The VA is responsible. Let us admit the reality. That means

we are responsible, and we are going to have to deal with this, in terms of responsibility.

So, in terms of questions, do you have authority right now under your existing authorizations and budget, authority to pay for any credit checks, counseling, or any other expenses such as that? And number two, do you have statutory authority to make people whole if they do have identity theft problems? Or if you don't have that authority, are you prepared to work with us immediately so that we can take the legislative steps necessary to give you that authority?

GENERAL HOWARD. We are clearly prepared to do anything we need to do, sir. We do not believe we have the authority to do that right now.

MR. BRADLEY. Either authorities I asked? You don't believe you have the authority to compensate for counseling, for credit checks, or any other expenses that are preventative in nature?

GENERAL HOWARD. I don't believe so. No.

MR. BRADLEY. And if you don't have that authority, you probably don't have the authority to make people whole in the event that problems do manifest themselves.

GENERAL HOWARD. I don't believe so, sir. We would need some additional authority.

MR. BILIRAKIS. I understand that Mr. McLean left with the Secretary to go over to the Senate. But his assistant is here? Can you answer that question, sir? Mr. Thompson, Mr. Jack Thompson?

MR. THOMPSON. Yes, sir, I am Jack Thompson.

MR. BILIRAKIS. Yeah, why don't you pick up that mic, and maybe you can respond to that.

MR. THOMPSON. Yes, sir. We have determined that VA does in fact, incident to its authority to administer these benefit programs, have the inherent authority to provide, to fund credit checks for individuals. What we lack is clear authority if any individual suffers economic damage as a result of identity theft. Those sorts of losses perhaps could be compensated through an action under the Federal Tort Claims Act, based on Federal negligence. But quite frankly, there would be a number of legal obstacles in the path of anybody who needed to go that route.

MR. BILIRAKIS. Well, now, sir, would your department, your office, furnish this Committee your opinions regarding what additional authority might be needed so that we can do whatever is necessary I guess through legislation if you don't think they have the authority?

MR. THOMPSON. Yes, sir—

MR. BILIRAKIS. Let us not wait until it happens I guess is what I am saying.

MR. THOMPSON. Yes, Congressman. We would be glad to.

MR. BILIRAKIS. Many of furnish that to us as soon as you possibly can? Good, all right.

Mr. Bradley, I am sorry to take up your time.

MR. BRADLEY. Not a problem. Glad to accommodate you, Mr. Chairman.

So having answered the first question about authority, that you do in fact have the authority, it would seem incumbent upon all of you to make sure that in the widest possible venues, whether it is the letter, the call centers, the Website, public service announcements, on and on and on, that you disseminate the information that in fact veterans will be compensated for, if they have expenses to do with credit counseling checks or any other expenses, on that first authority I asked you.

And I look forward to working on a bipartisan fashion with all the members on this Committee on the second authority, which we need to do, it would seem to me, as soon as possible.

MR. BILIRAKIS. I thank you, Mr. Bradley. I thank you, Mr. Thompson.

Mr. Udall to inquire.

MR. UDALL. Thank you, Mr. Chairman, and let me say this in listening to all of you and listening to the Secretary, it seems to be like a comedy of errors, and I think you can probably understand why so many members of this Committee have expressed on both sides of the aisle a great deal of displeasure with what has gone on here. We do not have to tell you, these are men and women who have served this country, and potentially we have put them in a situation violating their privacy, and costing them a significant amount of money.

And Mr. Chairman, I would like to echo what others have said. I think we have many questions that were unanswered from the Secretary. He is the one in charge of this department. We should bring him back here and get those answers. I mean, the thing that he said that was shocking to me, to hear this happened on May the third, and he did not learn until the 16th of May, and he is the guy running the department. Theoretically within the Veterans' arena, the buck stops at his desk, and all of you that work for him, it did not get to his desk for 13 days.

And I guess my first question is why is that the case? Why did none of you that are here, or anybody else, report to him for 13 days what had gone on? We heard from you, Mr. McLendon, we heard that you interviewed and had the information. You knew there was a breach on the 5th. It would seem to me that that would be the date that someone would report to the Secretary that we have had a very serious problem here. Can anybody answer that?

MR. FILNER. Tom, can I just add half a sentence?

MR. UDALL. Yeah, sure. Please, yeah.

MR. FILNER. Mr. McLendon testified earlier that on the fifth you called the secretary. I do not know who you meant.

MR. UDALL. Because the Secretary in his testimony here said he did

not learn until May the 16th is what—

MR. MCLENDON. I was referring to our administrative secretary in our office when I said "the secretary." She's the one that first get the call. If I could just add from my point of view, is we have a process in place that says, and we are trained do this, that you notify your security and information privacy officer, and there is a protocol that they follow as to what they do. And that's what we did. And I think General Howard would probably say the same—we were both trained by the same building—that when you have a protocol and process in place, you pass that information along, you do the due diligence that's required, and you give them the information. And you wait for them to tell you what it is that they need to move this process forward.

MR. UDALL. But Mr. McLendon, Mr. McLendon—after you did your interview, you knew on the fifth that 26 million veterans' information was out there and had been stolen. And you had a process clearly—you had a process clearly to follow—

MR. MCLENDON. No, sir—no sir, we did not know that on the fifth—

MR. UDALL. When did you know that, then?

MR. MCLENDON. We began doing due diligence when [Stricken from the record upon request of the Presiding Chairman] was able—came back to work on Friday. And talking to him about what he thinks that he had done. And that's when a memo was prepared on the eighth, that as Mr. Duffy shared with you what happened with that, that—

MR. UDALL. But when did we know that 26 million veterans had information that was in that disk, was in that hard drive that was taken? When did we know that?

MR. MCLENDON. I don't think we completely knew that until somewhere around the 16th. And let me—

MR. UDALL. Why did it take so long to figure that out? I mean, you had the employee in your office. He told you what he was taking home.

MR. MCLENDON. Well, by this point the employee had already been placed on administrative leave, and—

MR. UDALL. You did not do a thorough interview of him before? Before—

MR. MCLENDON. Yes, we did a thorough interview. The IG did several interviews with the individual. But you have to sit down and go through a fairly painstaking process of looking at all of the records that are in a file. And let me just make a comment about Burrels—

MR. UDALL. Well, let me ask you one question here because I wanted to ask the secretary this, but the VA has an internal system to rate the sensitivity of veterans' data, from a one to a nine, with a level nine reserved for VIPs like the president of United States, or a member of Congress, or a cabinet member. In 2001, the VA stated that only 43

people had VA-wide, were authorized access to those records. Was this GS 14 individual specifically authorized access to all sensitivity levels, including Cabinet member records, prior to the incident?

MR. MCLENDON. Not as far as I know, sir.

MR. UDALL. So there was no authorization.

MR. MCLENDON. Sensitivity levels are established in a very strict way within VA in terms of access. I would not even have access to that information.

MR. UDALL. Thank you, Mr. Chairman.

[The statement of Mr. Udall appears on p. 91]

MR. BILIRAKIS. Talking about insensitivity: without objection, the name that was uttered by Mr. McLendon will be struck from the record.

MR. MCLENDON. Excuse me, Mr. Chairman. I didn't understand that.

MR. BILIRAKIS. Well, there was a name mentioned of the employee. That will be struck from the record.

MR. MCLENDON. Oh, oh, oh, yeah. Okay. Yeah. Yeah, yeah, yeah, yeah.

MR. BILIRAKIS. Without objection. Ms. Brown-Waite to inquire.

MS. BROWN-WAITE. Thank you very much, Mr. Chairman.

Any member of Congress whose district office is helping constituents, including veterans, if one of our employees took this information home and the same thing happened, we would immediately fire that employee for putting the constituents at risk. General Howard, you referred to the "rules of the game." The problem is this is not a game. It was not a game. You know, the guidelines, that the VA had put down were kind of like suggestions. We often
hear that people believe the Ten Commandments are suggestions. So obviously, you all put this down as suggestions.

The VA has had problems that the IG has reported: information, security, material weaknesses, every year since the 1997 audit. This is 2006, and this has happened? I am sorry, what are you all doing over there?

Back in our individual districts, the medical care that is being given is excellent. But I will tell you, our constituents believe that Washington DC is La-la land, and I have sat here from the beginning listening to everybody, and I am starting to absolutely agree that this is La-la land, because you all are in denial.

Is the employee on paid administrative leave, or unpaid administrative leave for taking this material which he was not authorized to take? Mr. Pittman, can you answer that?

MR. PITTMAN. Paid.

MS. BROWN-WAITE. Would you please stay by the microphone. He is on paid leave? Is there a reason why if he was not authorized to take

this why he was not fired?

MR. PITTMAN. Yes, ma'am. From the very beginning we were under the instructions that we have to investigate this process to determine the severity of the action to be taken, and that's what we've done.

MS. BROWN-WAITE. Is the employee a civil service employee, or is he a political appointee?

MR. PITTMAN. Civil service.

MS. BROWN-WAITE. If the Secretary does not know how many employees telecommute, do you?

MR. PITTMAN. Yes, ma'am, 1600.

MS. BROWN-WAITE. You have 1600 telecommuters?

MR. PITTMAN. Yes, ma'am.

MS. BROWN-WAITE. From all over the country? Or just here in the DC area?

MR. PITTMAN. All over the country. We have 40,000 occupation—employees that are eligible to telecommunicate, but only 1600 take advantage of that category.

MS. BROWN-WAITE. And do you know—it has been 22 days since the burglary took place—does the department have a copy of the police report, or are they relying entirely on the individual's report of this incident? Now obviously, the police report would not be completed because an investigation is ongoing. But do you all have a copy of the initial report?

MR. PITTMAN. I'm told that the answer is yes.

MS. BROWN-WAITE. Could you confirm that?

MR. DUFFY. I can confirm that for you.

MS. BROWN-WAITE. Okay, so you do have a copy of that.

MR. BILIRAKIS. Can we get a copy?

MS. BROWN-WAITE. Yes, we would like a copy.

The other thing is, did the department do a risk assessment on this breach?

MR. PITTMAN. I cannot answer that question.

MS. BROWN-WAITE. So no one here knows if a risk assessment was done on this breach?

MR. PITTMAN. No ma'am, I don't.

GENERAL HOWARD. Don't believe it has.

MS. BROWN-WAITE. Well, inasmuch as it happened on the third, the Secretary did not find out until the 16th, but the deputy secretary found out somewhere in between that time. Don't you think that it was appropriate to do some sort of a risk assessment?

GENERAL HOWARD. There are actions going on as to what conditions do exist, but that's an ongoing effort to find out how much data is out there in an uncontrolled environment. We don't know the answer to that right now.

MS. BROWN-WAITE. The other question is, why isn't all of this information encrypted?

GENERAL HOWARD. It should be. I believe I mentioned earlier, the guideline—and you're correct, ma'am, I should not have referred to it as "rules of the game," you're exactly right. In that guideline, there were two key requirements. One is that the information should not have been removed. And two, it should have been encrypted, so—and it was not.

MS. BROWN-WAITE. What steps is the Department taking to ensure that information is quickly encrypted?

MR. BILIRAKIS. Would you furnish that information to us in some detail, please?

GENERAL HOWARD. You mean the guideline, sir?

MR. BILIRAKIS. Well, what steps are being taken—

GENERAL HOWARD. Yes, sir.

MR. BILIRAKIS. —responding to the question.

MS. BROWN-WAITE. Mr. Chairman, I would also inquire as to why these are just guidelines, and that they are not in your regulations?

MR. BILIRAKIS. Well, even going further than that, the Inspector General's report that I referred to earlier of November of 2005 indicated that there were some problems potentially, security problems. And you know, that was a half a year ago, and this has taken place.

General Howard, I am not going to get into that with you now, but come on, you are a general officer, and there is no way that when you were on active duty, that you would allow this to happen, and would not have taken care of the problem when you were notified by the Inspector General. It is something, again, that goes back into the culture kind of thing.

I am going to recognize Ms. Herseth, and I am going to excuse the Inspector General. But Sir, I am very much concerned what can be done. Because again, I have said this, what, for the third time, over 24 years that I have been here, similar things have arisen, and it seems like an awful lot of it has come from—you don't like the word "bureaucracy." I don't know whether you like the word "culture." But it is culture, and an environment there, and whatnot. And Mr. IG, I would hope you can help us solve that. I know we have got civil service, those particular problems.

Can you respond very quickly? Do you mind very much, Stephanie? Go ahead, sir.

MR. OPFER. Mr. Chairman, let me just say from the IG's perspective what we are doing. Once this came to our attention that we had a serious breach of security, I initiated a criminal, investigation and an administrative investigation, and tried to gather all the rules and policies and procedures in the department.

There are three prongs to our approach. One is looking at the theft of the data. Two which may answer some of the questions that were posed by the Committee members—we are looking at the incident: what happened when the employee reported it? Who did he report

it in to? What did they do with the information? All the way up to the top levels of the department. That is part of our administrative investigation.

I have the Counsel to the Inspector General looking at all the policies and procedures, and we intend to review all those policies and procedures, we are looking not only at the policies and procedures for the department—are they only geared towards someone in IT, when there is hacking into the system, or attacking the system? But also, what policies procedures What do we have regarding employees and their access to data? And what are the authority? Who is supervising it? Who is reviewing the need to have access to that material? We hope to conclude that in our Inspector General review.

MR. BILIRAKIS. When do you anticipate that being completed?

MR. OPFER. We are going to try to—separating the ongoing criminal investigation and working with the Federal Bureau of Investigation and Montgomery County police, and the Department of Justice, keeping that separate because as you know, ongoing criminal investigations limit my ability to discuss and provide information.

MR. BILIRAKIS. Sure.

MR. OPFER. I have separate teams working on all of the other ones. My goal is to try to have that out in 45 days.

MR. BILIRAKIS. Forty-five days. Would you share all that information with this Committee directly?

MR. OPFER. Yes, sir. Right now, my thought would be that we would have a number of recommendations, and a report would be addressed from myself as the Inspector General to the Secretary, and it would be provided to the Committee, and the members of the Committee.

MR. BILIRAKIS. Would you be able to also share with us suggestions? I mean, I don't know if you agree with me. I keep throwing this word "culture" around. I don't know if you agree with me or not, but I think it is there, I think it is a problem, and otherwise a lot of these things would not be taking place. Could you share with us maybe your suggestions on how that can be improved?

MR. OPFER. Yes, I think there is a good opportunity now, with the Congress enabling the agency, to centralize the IT function and give the authority and the responsibility to one individual to coordinate that. That was one of the recommendations for years from the Office of the Inspector General.

MR. BILIRAKIS. Okay.

MR. OPFER. So we continue to be pleased with that—

MR. PITTMAN. Will you share that with us within that 45 day period of time, too? Any suggestions—

MR. OPFER. —we expect that in the FSM audits that we will continue to have those material weaknesses until they are corrected within the agency.

MR. BILIRAKIS. Exactly. Exactly. Thank you, sir, and you are excused, and we appreciate very, very much your hanging around.

Ms. Herseth to inquire.

MS. HERSETH. Well, thank you, Mr. Chairman. I appreciate the questions you posed to Mr. Opfer, because I think that review will answer some of the questions that had been posed previously and that I have as well. But let me make a couple of initial observations, and then get to a couple of the questions about the IT system now, and how it's working.

First, I think we do need some clarification from the Secretary, because I specifically wrote down during his testimony that he indicated that the VA Inspector General became aware of this on May 10th. He may have misspoken and meant the information security officer, or perhaps he was under the impression that this information had been communicated to the IG, which it hasn't, but we need some clarification on the issue.

Also, it's my understanding based on your testimony and the questions posed in your responses that the reason that the VA has not formally notified the IG even as of this date is because it is not a cyber security issue in your opinion, it is a privacy issue; and therefore, it is being handled by an office, a division not currently represented today.

Secondly, I shared Ms. Brown-Waite's concern that we have to address this issue of something being a guideline versus a directive, as it relates to any employee in the VA being permitted to take this information outside the workplace, getting the permission, having encryption, because I think someone made a note in particular that that is a guideline, not a directive.

So let me ask two questions. The first is very straightforward. If one of my constituents who is concerned that his or her information is among the 26.5 million records within what was stolen and he or she calls the 800-number, will the person answering that number be able to tell him or her whether or not his or her records were among the 26.5 million records were stolen?

MR. MCLENDON. To do that would be to provide this people access to the Burles system and other databases, for which they may not be authorized to be accessed. So the short answer to your question is no, they would not have access to that.

MS. HERSETH. So they won't know until they receive the letter of notification from the VA?

MR. MCLENDON. That's why we are sending the letters. And let me also add, people keep talking about 25 million records. 19 of those—million of those records have Social Security numbers. 6 million do not have any identifying Social Security numbers.

MS. HERSETH. Okay.

MR. MCLENDON. And of the 19 million we believe that there are a

number of those veterans are deceased, because when we look at the birth dates of a number of them. So there is effort going underway to try to understand of that 19 million—

MS. HERSETH. I appreciate that. I appreciate that. So what the information that one of my constituents would get by calling 800 number is just the recommendation to monitor their credit?

MR. MCLENDON. Yes, they are getting direction on what they need to do.

MS. HERSETH. Okay. And we do not have a time frame yet as to when those letters would go out, or did you mention that earlier and I missed it?

GENERAL HOWARD. No, I don't think—yeah, I don't—

MS. HERSETH. Because you still have to analyze all of this data? Okay. Let me move to—

GENERAL HOWARD. To elaborate, though—

MS. HERSETH. I am going to let you elaborate. I just want to make sure I get to this third question. And if there is time, the Chairman permitting, please elaborate. I mean, there is so much information that we do want here. We are just under these time constraints.

Five, six years ago, I was practicing law at a very large firm here in Washington, a firm that has a global presence, number of offices across the country. I could not save a document, any client identification numbers on a disk. We didn't even have hard drives in our desk. But what we did have if we were going to do any work outside of the office was a secure ID that changed, as you know, every few seconds so that when you are home, or on your laptop, that you have that ID number that you type in that is only available—you know what I am talking about.

GENERAL HOWARD. Yes, ma'am.

MS. HERSETH. Do you have that? Is that a process that you are utilizing, that you are integrating over time? I just don't understand why any employee would be able to save anything onto a desk or an external hard drive, and maybe that is part of where we are heading with a centralized IT system, but it just seems that a five or six years ago, and I note it is a difference between a private sector and a public sector and different resources, but are we moving in that direction, to have a system like that in place?

GENERAL HOWARD. We definitely need to improve on the procedures that you just described. The specific drive that this information was stored on, the folder is protected. In fact, I physically tried to get into it myself, and I could not do it. Dennis, you can probably comment on—

MS. HERSETH. Okay, I appreciate knowing that there is a firewall or two that the thieves would have to get through here. But do you have—

GENERAL HOWARD. Ma'am, not the information that was on his

drive. I am talking about where he originally took it. The drive that was stolen, as far as we know the information was not encrypted.

MS. HERSETH. All right, okay. Okay, thank you for the clarification. Of the 1600 telecommuters, are they access saying the system remotely in the way that I just described? With a secure ID, into the centralized system?

MR. PITTMAN. No, ma'am. The only thing that they are doing is they are accessing the computer by logging onto the system via a security access password.

MS. HERSETH. Okay. I have more questions, but I will submit them for the record. Thank you, Mr. Chairman.

[The statement of Ms. Herseth appears on p. 87]

MR. BILIRAKIS. Thank you, gentle lady. Mr. Michaud.

MR. MICHAUD. Thank you very much, Mr. Chairman. I also want to thank you for having this hearing.

Most of the questions have been asked, but I just want to follow up on a few of them. As we read and heard the IG state, that this condition has been going on for a number of years as far as the security deficiencies and in his testimony, he says in the 141 of the 181 VHA facilities, they identified security deficiencies, as well as in 37 of the 55 VBA facilities. You heard the Chairman talk earlier about former secretary Principi giving the directive, then the legal counsel saying they did not have the authority to do that.

Whether they have the authority or not, I guess this question would be for Mr. Duffy, wasn't that a good idea, what the IG had talked about, on these deficiencies? Regardless of whether, they had the authority or not? If it is a good idea, why not implement it?

MR. DUFFY. Absolutely, Congressman. And we thought we were indeed implementing them. In this particular instance, it was an individual who violated policies and procedures, who clearly understood that what he was doing was inconsistent with established policies and procedures, someone who had in recent months completed cyber security awareness training and privacy act training. So there are indeed policies and procedures in place. There is heightened awareness through standard annual training for all employees who are involved in this kind of work. In this instance, we had an individual who simply chose to use poor judgment and violated those policies and procedures.

MR. MICHAUD. As you heard the Secretary mention earlier this morning, someone has to be responsible if something happens in this situation as far as identity theft; has there been—and clearly this is a severe case—has VA heard of identity theft in past from veterans? And if so, how many of those cases that are out there on a yearly basis?

MR. MCLENDON. Not personally aware of any, Congressman.

MR. MICHAUD. Okay, thank you. My next question, we heard a lot from different individuals here on, you know, what did you know, when did you know it, and could you give the details? Actually, I haven't heard Mr. McLendon, when actually did you know it? What did you know, when did you know it, and can you give, some details of that timing?

MR. MCLENDON. Well, I knew before 6:00 o'clock on Wednesday that there had been a break-in at the individual's home, that he had reported that he had lost his personal computer and an external drive. At that time, the way he communicated, it also sounded like he had lost a little external USB drive, that we would call a memory stick, and some CDs. He was quite upset at the time, so that's one of the reasons why I called the guy who's our technical expert on data and systems to see if he could talk more in a technical terminology to try to pull out of him a little bit more.

So we knew on Thursday that something indeed had happened. We did not know the scope of it, or any of the details of it. And so when we began meeting with him on Friday morning, and then our information security manager met with him, we began to get I would say a broader outline, but yet not the details out exactly what was on those disks.

It's fair to say that it wasn't until Monday that those of us who had been talking together and talking with him could kind of look at each other and say, "Okay, we believe we've got kind of the initial look at what we think may be there." And that's when a memo was prepared that, as Mr. Duffy explained, where it went and what had happened after that. Then the information security officer had further discussions with him. I don't believe that we all understood the details, in terms of 25 million records, some of these other things, until we understood that his disk had not been stolen and his memory stick was not gone. There was some confusion about that right after he started talking about it, which is understandable.

And then we started painstakingly going through those of files to understand what files there were, what data variables there were, related to each one of those files. That's what led to again preparing a memo on the 16th, which went to the general counsel on the 17th, which laid that out.

Sometimes it takes a finite period of time to do the due diligence to find out exactly what is on those files and where could they have possibly come from.

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

[The statement of Mr. Michaud appears on p. 82]

THE CHAIRMAN. [PRESIDING] Has everyone asked all the questions?

MR. FILNER. If I could just follow up for a couple minutes?

THE CHAIRMAN. Sure, Mr. Filner.

MR. FILNER. Thank you, Mr. Chairman. Just to follow up on Mr. Michaud's questions, in the time line you provided to us, you said there was a memo on May 5th that says "possibly lost veterans' data." We don't have a copy of that, but what did you think, then, that was lost?

MR. MCLENDON. That may have been an original memo that the information security officer prepared. I don't have that in front of me. I'll have to go get that but I—

MR. FILNER. I was just wondering what you knew at that moment.

MR. MCLENDON. Well, what we knew at the afternoon of the fifth was that there had been a break-in at the individual's home, that he had self-reported that his personal laptop and personal external drive had been stolen, that he believed that he had loaded some veterans' data, if I remember the words right, onto that. But he didn't know for sure, and couldn't say in any detail what may or may not have been on there.

MR. FILNER. Mr. Duffy, is that your understanding of that, this memo that you provided Mr. Bowman? I'm just reading from your time line.

MR. DUFFY. Yeah, let me back up a little bit. And I apologize because there is just a little bit of confusion regarding memos. There was an original memo prepared by the IT specialist, our security and privacy officer, late in the afternoon of May 5th.

THE CHAIRMAN. His name?

MR. DUFFY. I'm sorry, his name? Mr. Mark Whitney. Mr Whitney prepared, at my instruction, a memo that attempted to lay out what he understood to be the data sets and elements. And indeed, I think he did a pretty good job. Mr. McLendon and I, upon reviewing it, Mr. Mclendon asked for the opportunity to review and validate the information. Again, while Mr. Whitney is our IT support person, he does not necessarily have detailed understanding or information on the data sets or data elements. So Mr McLendon and Mr. Tran indeed did that, modified slightly the May 5th memo. It was finalized over the weekend and provided to me on May 8th. The unfortunate thing is that the date of the memo was never changed. So we've got two May 5th memos; one more expansive than the other, simply clarifying the nature of the extracts, the type of programming language that they were contained in, and further detail than the previous memo. So it was that memo that was—an original memo on the fifth, modified on the eighth, provided to the chief of staff on the—discussed with the chief of staff on the ninth, and given to him on the tenth.

MR. FILNER. And the chief of staff is directly under the secretary?

MR. DUFFY. Yes, sir.

MR. FILNER. But everybody took the weekend off on the sixth and seventh, it looks like. Normal weekend in your life, 25 million things gone, what the hell?

MR. MCLENDON. Congressman, I can assure you that there has been a deep sense of urgency about—concern about this issue, and working on this issue.

MR. FILNER. Except that Friday you did something and then you waited till Monday to do it more, you know, Saturday and Sunday, nothing done, according to what—I am just going by what you provided us.

MR. MCLENDON. Well, that was just the date that was put on it was Monday, that was the first working day back.

MR. FILNER. You can detect the frustration and the outrage in all of our voices. And again, I mean I don't think you took it seriously enough at the beginning, this chief of staff and the deputy secretary knew a week before they decided to tell the Secretary. In addition, even given all that, the so-called outreach to our veterans, you know, you say, "Well, if you have a Website, look us up. Notify your bank, notify your credit bureau. Don't tell us, we don't need to know if you guys have a breach of security."

I mean, there is no outreach in the letter that is going to go out. As somebody said, you don't even have 26 million envelopes. I mean this is ridiculous. I mean, I think you all should be fired. To take this as un-seriously as you have, to take the amount of time that you took, and then still, even at this late date, you don't have a system where anybody even knows that their name was there. There is no outreach for people who—the normal person who may not know how to get your Website. Nothing is being done on television, radio.

I mean, you are just waiting, you know, to get this information—these guys are scared to death. And you sit there—you don't seem to want to understand that. And you give these bureaucratic answers that don't mean anything to the people we are trying to serve here. As one of the Congresspeople said, if this happened in our staffs, I mean, they would be fired right away. And I think the Secretary, as the last act before he resigns, ought to fire the whole bunch of you.

THE CHAIRMAN. I think what would be helpful to us is Mr. Duffy, if you could submit to the Committee, I would like the draft—I don't know if we ought to call it the draft—the original memo from Mr. Whitney—

MR. MCLENDON. The May 5th?

THE CHAIRMAN. The original memo, I want to see what that one says. I want to then see whatever changes that were made.

MR. MCLENDON. Right.

THE CHAIRMAN. I want to compare the two documents.

MR. MCLENDON. Reflected on the eighth. Happy to.

THE CHAIRMAN. Yes. And then that ends up to the Secretary's Chief of Staff on May 10th. At some point, the Chief of Staff notifies the deputy secretary, but almost another six days go by before anybody even alerts the Secretary. You know, what we have here is a chro-

nology, but the Secretary, because it has got a lot of other personal identifying information in it, has asked us not to have this put in the record. But I think what we are going to need to do here is, with my indulgence, is let me take and ask these witnesses to put a time line on the record in their testimony. Is that all right, my colleagues?

So Mr. Duffy, let's just begin with you. I know you did this a little bit earlier, but let us go ahead and take your time line from the first moment that your department had knowledge and Mr. McLendon, I want you to add in. And then we are going to turn to the other witnesses with regard to the time line as they know it.

Well, let me pause. I am going to seek counsel. You can do this a thousand ways. We can either do it day by day and take the testimony of them on what they knew, or we can do witnesses. Mr. Filner, what do you want to do? All right, we will turn to Mr. Duffy. Hold on.

MR. BRADLEY. Mr. Chairman, could I ask a quick question where I was not able to follow up on my time frame?

THE CHAIRMAN. Absolutely.

MR. BRADLEY. If you recall—and thank you very much, Mr. Chairman—if you recall my questions from before about the authority to reimburse veterans for credit counseling and credit checks, you indicated that you had that authority. That's correct, okay. The bulk of the phone calls and e-mails that my office has gotten have expressed a concern over the fact that it may cost fifty to sixty dollars to actually do that kind of a credit check right now. So if you have authority to do that, are you prepared to propose to us, today, that you will actually establish some mechanism for veterans who have to have expenses out of pocket to do a credit check, of a mechanism for them to be reimbursed for these expenses?

GENERAL HOWARD. Sir, in discussions this morning before we came over here, that is the intent of the Secretary, but he was concerned about to ensure that we have the authority. There are financial impacts that need to be addressed. It is actively being discussed.

MR. BRADLEY. So it is being discussed, you have the authority. When can we expect a decision on how you are going to implement that kind of reimbursement?

GENERAL HOWARD. Sir, that I'm not sure.

MR. BRADLEY. If I can ask the indulgence of the Chair. Mr. Chairman, in terms of the immediate impact on the 26.5 million veterans, which I think all of us, under your leadership and under Mr. Filner's leadership on a bipartisan basis, want to make sure that we have done everything that we possibly can to insure the safety and sanctity of their records. The most expeditious manner that these gentlemen can make that kind of reimbursement possible, to me would seem to be one of the most important first step that we can do for the 26.5 million veterans that are affected, to say nothing of all of these

security measures that have to go into place, but for those people that are worried, on an individual basis, and I would urge that we attack that head-on with obviously their assistance.

And I thank you for that.

THE CHAIRMAN. All right. Here is what we will do. To preserve time, I am going to ask you to prepare a chronology, time lines, I want each of you to prepare that, excepting personnel, unless you have something to add that we don't know about.

MR. PITTMAN. No, sir.

THE CHAIRMAN. Okay, thank you. So with the rest of the witnesses, I need to know the chronology: what did you know, when did you know it, and how it got passed along, okay? So provide that, then, to the Committee. That is the best way, I think, to do this. Can you get that to us in about 10 days?

GENERAL HOWARD. Yes, sir.

MR. BAKER. Yes, sir.

MR. DUFFY. Yes, sir.

THE CHAIRMAN. All right, thank you.

With regard to the data analyst, who is his immediate supervisor?

MR. MCLENDON. His immediate supervisor is Mr. Mike Moore.

THE CHAIRMAN. Mike Moore. And then who is his boss?

MR. MCLENDON. Me.

THE CHAIRMAN. You. I apologize, I was gone. The project which they are working on was what?

MR. MCLENDON. [Stricken upon request of the Chairman]—The individual is—

MR. BILIRAKIS. Strike the name.

THE CHAIRMAN. Pardon?

MR. BILIRAKIS. Strike the name.

THE CHAIRMAN. We are going to strike the name of the data analyst from the record.

MR. MCLENDON. The analyst is a programmer, statistician, he supports a number of different projects in the office that are ongoing. He was doing work looking at a national survey of veterans project. He was also doing some matching to support other projects he was supporting in terms of activities that other people in the office were doing during that time.

THE CHAIRMAN. Are you aware of any of your employees taking data home with them to do, quote, "homework?"

MR. MCLENDON. Not to my personal knowledge. But I would say this to be quite candid: we in government today facilitate, encourage, and reward people for working from home. We give them computers to do that, we give them access to do that. Each agency allows them to—has their own policies about how they do that and when they do that. But it is not our policy to encourage people to take work home, or to take data home.

THE CHAIRMAN. How many employees does the VA have that work from home and access your data bank?

GENERAL HOWARD. Two different numbers, Sir. Work from home is, what was it, 1600?

MR. PITTMAN. Those that are the telework employees are 1600. Then there is another group of virtual employees, which he'll address.

THE CHAIRMAN. And encryption is used?

MR. PITTMAN. It is not.

GENERAL HOWARD. Sir, if they access—

THE CHAIRMAN. I apologize. I was just told that has already been asked and answered. In the negative, shockingly. Do you, Mr. McLendon, know whether or not the data analyst's supervisor approved of the practice for this individual to take this type of data out of the office?

MR. MCLENDON. No one would have approved that.

THE CHAIRMAN. Okay. But you encourage people to do homework?

MR. MCLENDON. Don't encourage people to do homework. What I am saying is that when people are allowed to telework from home you have to be extremely careful about what people do, and what they use. And it is not my policy or anyone I know of, has a policy that allows people to take serialized, controlled information of people home, or veterans home, to do work. That's a no-no in the analytical business. You just don't do that.

THE CHAIRMAN. Let me ask General Howard, if I go back to this directive from the Secretary Principi, had the CIO been charged with this responsibility over security as the Secretary wanted, you think this would have happened?

GENERAL HOWARD. There is a memo that I saw signed by Bob McFarland. I don't recall exactly what it said. One of the—and I do know that one of the difficulties that they were trying to sort out is just what exactly the authority was. There was a lot of discussion about the word, "ensure," that's in Secretary Principi's directive—I think that's the one that it's in, sir—and if I'm not mistaken, was a keyword that the general counsel addressed.

The bottom line—again, I don't remember the exact details of the memo from the General Counsel, but it is obvious to me that the CIO has authority to set policy, to set the guidelines, but then it's up to the individual who supervises, administration heads, and assistant secretaries, to implement those policies.

THE CHAIRMAN. But see, had this been enacted, then you had the enforcement power. Now, you can't enforce cyber security. You can't do anything, all you can do is do compliance; correct?

MR. CADENAS. That is correct, sir, check for compliance.

THE CHAIRMAN. And so under a decentralized model, for which Mr. McLendon, Mr. Duffy—well, strike Mr. Duffy—for which Mr. McLendon I know has argued, that enforcement, that is where it goes, it is

decentralized.

So let me just say this gentleman, one of the first things I learned in the Army: when you take command, you want to know who the key control custodian is, because you just signed personal responsibility for all that property. Under a decentralized model, you have too many keys.

GENERAL HOWARD. Sir, I will say that the federated model that has been adopted, as you know, will give us a better capability. It won't give us the ultimate capability—

THE CHAIRMAN. Yes, that's right. You are going to get a half-baked loaf.

GENERAL HOWARD. —but it will help to some degree to get a better handle on it.

THE CHAIRMAN. So let me ask this. You are the acting CIO, and I am going to turn to cyber security. I have done hearings with you before, and those hearings dealt with the hackers from the outside, "Oh, we spent all this money," but you also came, and with the IG and GAO, you talked about all the unauthorized use of employees, you talked about that.

So to go beyond just compliance—or if you are going to say, "Steve, no, my job is only to do cyber security. That from the outside, somebody else should do that," give us your best counsel, the two of you, right now with regard to authorities and enforcement. You are a general officer. Does dissemination work very well in the Army?

GENERAL HOWARD. Very well, sir.

THE CHAIRMAN. Dissemination?

GENERAL HOWARD. We also—

THE CHAIRMAN. Somebody has got to be in charge with distinct lines and chains of command, right?

GENERAL HOWARD. Sir, there's no question about that.

THE CHAIRMAN. All right.

GENERAL HOWARD. And one thing that we do have, as you know, sir, in the Army, is very clear regulations. As I mentioned earlier, we've looked for the clear policies and directives, and with respect to what the individual actually did, the only place I can see that is in a guideline. It's not a directive or a regulation that you would think it should be. It is being turned into a regulation, or a directive. The VA uses the term, "directive." That is being accomplished without any more waiting.

But it's too late for that. I mean, the incident occurred, and it was not clear that this was a violation of a directive, because it wasn't a directive at the time. But what you described, it has to be straightened out. Clear directives do need to be put into place. As I said earlier, the federated model is helping a great—we've only been into it for a short time, as you know, but it's already helping to shed light on some activities that are going on that need to be tightened up.

THE CHAIRMAN. General, if you were to have adopted the federated model you let the individual stovepipes to do their own development, you don't own development under the federated model.

GENERAL HOWARD. That's right, sir.

THE CHAIRMAN. That is where the problem has been occurring. In software development. Wasting millions and millions of dollars. That is why we have come in and zeroed out programs. We are extremely upset. It is why we on a bipartisan basis have asked for you, your position to be empowered.

So you are correct. You can look at this and go, "Well, directives weren't violated." This is bigger than a small, little employee—

GENERAL HOWARD. They weren't violated, because they didn't exist.

THE CHAIRMAN. Well, this Committee is not going to permit an Abu Graib, whereby you prosecute the little people, and others don't have problems. We are going to work with you. We are going to work with you, on policies, and practices, and procedures, and empowerment. And we are going to also—we may use this to get a stronger hand around the development side of the house.

GENERAL HOWARD. Sir, can I comment on the term, "enforcement?" I don't think you will ever get away from the fact that individuals in charge of organizations are clearly in—responsible for implementing the policies, and enforcing the policies. We have a greater role in determining if violations may have occurred, inspections, that sort of thing. But I don't think we should ever remove the enforcement responsibility from those actually in charge of administrations and staff sections. We didn't operate that way in the Army, either. The commander was in charge.

THE CHAIRMAN. Mr. Cadenas, what do you have to add to this?

MR. CADENAS. All I can say, sir, is in the three years, six months that I've been here at the VA, it's been a little frustrating and challenging for us, and the team. We're looking forward to good things with the federated, as I said last time when I was up here, because now those systems will go under the leadership of of the CIO, and because he now owns those systems and I work directly for him, I don't need any authority to execute.

There—you know, we try the best we can. The reason why you see so many guidelines is because where we can't get policies or directives pushed through, then we go down to the next level, and then the next level, to where we are successful in getting guidelines out there.

THE CHAIRMAN. Under this federated model, will you receive the necessary delegated authority from the Secretary to do your job so an incident like this will never occur again?

MR. CADENAS. Sir, to be honest I won't need his authority because I directly report to the CIO's office. And under the federated model, the CIO is in charge of all the operations and maintenance systems,

to where he can tell me, "I got a problem out there, go fix it now with your team," or ensure or enforce compliance or execution.

THE CHAIRMAN. But on the development side of the house?

MR. CADENAS. No, sir. Not on the development.

THE CHAIRMAN. Yes, that is my point.

MR. CADENAS. But we're working—

THE CHAIRMAN. That is what I want to make clear to all the members. On the development side of the house—we can go with the federated model, but this will continue.

All right, does anyone have any follow-up questions?

[No response.]

All right, we are going to continue our hearing at a later date. I thank you for your testimony. This panel is now excused.

MR. FILNER. Mr. Buyer, I just want to thank you for your knowledge and your commitment to follow through. We will follow your lead. I appreciate it very much.

THE CHAIRMAN. The second panel will please come forward.

The second panel is three representatives from the private sector to shed light on the implications of the failure of the Department of Veterans' Affairs to control information management. Going from left to right, we have Mr. Stuart Pratt, President and Chief Executive Officer of Consumer Data Industry Association. Next, we have Mr. Dennis Hoffman, Vice President for Information Security for EMC Corporation. And finally, we have—

MS. LITAN. Avivah Litan.

THE CHAIRMAN. You say it's pronounced—

MS. LITAN. Avivah Litan.

THE CHAIRMAN. Pull it close, really close.

MS. LITAN. Oh, sorry. Avivah Litan.

THE CHAIRMAN. Avivah Litan?

MS. LITAN. Litan.

THE CHAIRMAN. Thank you. Vice President and Business Director for Gartner Incorporated. I would also like to mention that we have Joel Winston, associate director of the FTC's privacy and identity protection division, and Betsy Broder, assistant director of the same division, in the audience today. Both are members of the Identity Theft Task Force, and have been listening to the testimony. They will be available for any questions that any members may have following the hearing.

We look forward to hearing from our panelists on how we can ensure the safeguarding of sensitive information to re-earn the trust of veterans and their families.

STATEMENTS OF STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION; DENNIS HOFFMAN, VICE PRESIDENT

OF INFORMATION SECURITY, EMC CORPORATION; AND AVIVAH LITAN, VICE PRESIDENT AND DISTINGUISHED ANALYST, GARTNER, INCORPORATED

STATEMENT OF STUART PRATT

THE CHAIRMAN. Mr. Pratt, you may begin.

MR. PRATT. Mr. Chairman, thank you for this opportunity to appear before you, and thank you also—

THE CHAIRMAN. Thank you. To all the witnesses, if you have written statements—do all of you have written statements?

MR. PRATT. Yes, sir.

THE CHAIRMAN. They all acknowledge in the affirmative. It will be submitted for the record. And if you would, please summarize.

MR. PRATT. Thank you, Mr. Chairman.

This past weekend, CDIA was contacted by the Federal Trade Commission regarding this breach. We are thankful for the FTC's outreach to us which allowed CDIA to liaison with our national credit reporting company members, who had to plan for likely heavy call volumes on their toll-free numbers, and hit rates on their Websites.

Based on this contact, our members technology teams were ordered in preparation for the announcement on Monday, May 23rd. And as part of this very late stage coordination, our members also voluntarily either adjusted current toll-free number menus to include special referents for affected veterans, or implemented entirely new toll-free numbers which can be used by veterans to request the placement of a fraud alert on their credit reports.

Once a fraud alert is placed, a veteran is then by law entitled to a copy of his or her credit report, free of charge. Our members report that subsequent to the announcement by the Veterans' Administration and ensuing media coverage, the call volumes have been running at approximately 170 percent over normal volumes.

If we had a criticism of this process, it is simply the fact that our members were not consulted sooner by the Veterans' Administration. We appreciate however the fact that the FTC did contact us, and they were embargoed in terms of when they could get in touch with us to begin coordination.

Even over the weekend, the FTC was not permitted to release the name of the agency: and thus our members could not execute plans to customize toll-free number service until after 11:00 a.m. on Monday, May 23rd. We believe government agencies should be obligated to coordinate with their members well in advance where they intend to publish advice, which includes our members contact information. This is simply the right step to take so that our members can verify the accuracy of the information and ensure that our systems are prepared for the increase in contact volume. Ultimately, this obligation

helps us all serve those who are affected.

Your staff has expressed interest in hearing what steps we would recommend that a veteran take in response to the announcement, and our views on the key steps are really no different than those which the FTC has already compiled. We believe consistency in a message is very important at this stage, and that all veterans are empowered to take the steps that are appropriate to the level of risk they perceive. And these include of course placing a fraud alert.

We would only add emphasis to the FTC's point that veterans need only call one national credit reporting company to place a fraud alert, since our members exchange fraud alert requests. Further, upon placement of fraud alerts, veterans are entitled to a free copy of a credit report and will receive instructions on how to order this. Some veterans may be confused about whether or not they need to annualcreditreport.com to obtain this free report, and the answer is they do not. They will receive specific instructions once their fraud alert has been placed that will allow them to access that credit report as well.

As demonstrated by this breach—

MR. FILNER. May I just ask you a question? Sorry to interrupt you.

MR. PRATT. Yes.

MR. FILNER. Could the VA do that for every veteran right now? Would you recommend that? Why are we relying on the people who are suffering? Why don't we take a proactive step?

MR. PRATT. It is a balance sheet question, Congressman, so let me give you both sides—

MR. FILNER. It could be done though, right?

MR. PRATT. The law does permit a third party to make that request on behalf of the individual. Yes, sir.

MR. FILNER. And what are the minuses?

MR. PRATT. I am sorry, sir?

MR. FILNER. You said there are pros and cons.

MR. PRATT. The only con is that a fraud alert stops transactions, slows transactions down, and you may find there are veterans in the middle of refinancing a home, obtaining credit, and they may not appreciate the fact that it was inserted right in the middle of that process. It is a balance sheet question that we all have to wrestle with, Congressman. I think that is as good as I can do.

THE CHAIRMAN. You may proceed.

MR. PRATT. Thank you, sir.

As demonstrated by this breach, data security and the need to notify consumers, including the nation's veterans, where significant risk of harm exists, it is essential. The following statement delivered before other Committees is still our position today:

The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft,

has expanded beyond the borders of financial institutions. It is our view that a rational and effective national standard should be enacted, both for information security and consumer notification, as it applies to sensitive personal information, regardless of whether the person is a financial institution.

At this Committee knows, there are a number of House and Senate Committees that are focused on developing uniform national standards. We believe enactment of national standards will ensure that sensitive personal information is protected by all who possess it, including Federal and State government agencies. New nationwide safeguards regulations, offered by the Federal Trade Commission will compel all to deploy physical and technical safeguards strategies for this type of information. As we head into the Memorial Day weekend, we must redouble our efforts to pass strong and effective national law that will require all to secure sensitive personal information properly, and to notify consumers when there is a significant risk of identity theft. We should do no less for our veterans, who have served us all. Thank you.

[The statement of Mr. Pratt appears on p. 107]

THE CHAIRMAN. Next is Mr. Hoffman.

STATEMENT OF DENNIS HOFFMAN

MR. HOFFMAN. Mr. Chairman, members of the Committee, thank you for the opportunity to testify before the Committee on Veterans' Affairs. My name is Dennis Hoffman. I am the Vice President of Information Security for EMC Corporation. For those of you who aren't familiar with the EMC Corporation, we are the world's largest provider of storage and information management solutions. Our Fortune 1000 customers include the top 30 commercial banks, the top 40 insurance companies, 19 of the top 20 pharmaceutical companies, all of the top aerospace and defense organizations, and 14 of the top 15 health care medical facilities, and many others.

I have personally spent a great deal of time with our customers over the past year discussing issues like the one this Committee is investigating, and today I can report to you all that the veterans' administration is not alone in wrestling with what is clearly becoming a very pervasive issue, which the industry calls "data leakage."

While the identity theft problem continues to make headlines, due largely to regulation causing it to be made public, it may well be the tip of the iceberg. Relative to all confidential information that organizations and corporations have, personally identifiable information is actually a minority problem. It is however the one that is making front-page news, and is the one that of course you are investigating. My point is that there is a lot more confidential information in the

world, and it is all subject to the kinds of problems that you talked about here.

So I think it is fair to ask why do these problems exist? They exist largely, from a technical perspective—as you have heard today, this is certainly not simply a technical problem. But on the technology side, they exist due to something called perimeter-centric thinking.

In the sense that from the days of medieval Europe, the notion of security has been largely to dig moats, build walls, erect castles, erect towers inside the castles, and believe that what is inside the tower ought to be safe. That is largely the way that we have gone about doing information security, from a technical perspective. The irony is that the vast majority of products which make up the information security marketplace today don't protect information. They protect assets that are supposed to protect information.

I can almost guarantee you that the laptop we have been discussing all morning had antivirus software on it. That is the single largest-selling security product in the marketplace today. And of course, it has nothing whatsoever to do with protecting the data on the laptop. Moreover, what this has led to is it has led us to conclude, or ignore the simple fact that information lives, has a life cycle. And during that lifecycle, it moves. And when it moves, it tends to walk right out of the castle. And therein lies the big issue.

It is not simply a laptop. It could be a USB device. There have been many publicized cases of backup tapes falling off of UPS trucks. When data leaves security parameters, it becomes exposed if we haven't done something to secure the information itself. And so what we are seeing in talking to a lot of our customers is a very significant shift in thinking to something we would call information-centric security, ironically enough, where we actually begin with the notion of securing the information, and then applying security to all of the assets through which the information has to pass.

That means four basic things: we have to understand our data and our people as organizations, because at the end of the day, we don't have information until data reaches a person. So we must be able to model both of those and control those. We need to secure the information infrastructure that manages and stores the information. We need to protect the data comprehensively. To date, we have been very focused on the availability of information, and not nearly as focused on its confidentiality and integrity. And it takes all three to truly secure information. Lastly, we need to assure policy compliance.

There are no silver bullets. This is a systemic problem, and it requires a systemic solution, which you have been investigating all morning, particularly around policy and process and people. And in particular, I would like to warn that a knee-jerk reaction to encryption as the silver bullet will likely miss the point, to the extent that encryption is only one technology, and it is only as good as the

business problem it solves. If the encryption keys are not managed appropriately there are even more problems because the data has effectively been deleted when it was encrypted. If they keys cannot be shared, collaboration is slowed down.

Encrypting data makes it opaque. It makes it impossible to actually know what is inside it. So a recent regulation in the UK—or was it a regulation that existed previously, was recently enacted, to make certain that all enterprises in the United Kingdom turn over their encryption keys to the government so the government can at least look at what the data is.

There are many problems, and there is no single silver bullet solution. There are however some very significant critical enablers, and you can put these all under the very general heading of "you can't secure what you can't manage." You cannot secure information that cannot be managed. These fall under the heading of things like infrastructure consolidation. When data is spread everywhere it becomes extremely difficult to stop leaks.

Content management is a technology that has existed for years to actually manage loose content in files. On top of that, digital rights management technology allows you to do things like encrypt specific files, prohibit whether they can be re-e-mailed, sent, printed, or copied to a USB device.

Data classification is enormous in the sense that data classification helps us to understand whether the data in question on a storage device is actually the Veterans' Administration logo, or some confidential document, or Social Security number. At a certain level within the IT organization, those two pieces of data are absolutely indeterminate; you don't know.

And then finally, identity management. Securing data, ironically, begins with securing and understanding the people, which again you have been exploring all morning. I have found in speaking with most of our customers that are at the forefront of this issue that there is a relatively simple formula they are all trying to drive toward.

First, maximize access control. These are issues like authentication, the secure ID comment that was made. How do you know that the person doing the work is actually the person? Strong authentication and authorization are key.

Segmented infrastructure. If you actually understand the difference between your public Website logo and a confidential document, you might not want to put them on the same network, the same storage devices, or the same workstations. And lastly, classified data, simply being able to tell the difference between the two.

So maximize access control is the first step in the formula that a lot of our leading customers are applying. Secondly, minimize data movement. Where possible, they are trying to eradicate these use of backup tapes, the theory being if I don't put the tape on the truck

and it doesn't leave my data center, then I am less likely to be compromised by it.

Issues like the guidelines we have been discussing this morning are meant to do just that: keep data from leaving the security perimeter. But as was pointed out by the Veterans' Administration, it is very difficult to legislate against an individual deciding to go against the policy.

Thirdly, selectively encrypt whatever remains. So if we maximize the access control and minimize the movement of data, what remains should be encrypted.

And then lastly, log and monitor everything, so that we can piece together what has happened, both in real-time and after the fact.

Thank you.

[The statement of Mr. Hoffman appears on p. 113]

THE CHAIRMAN. Thank you very much. Ms. Litan?

STATEMENT OF AVIVAH LITAN

MS. LITAN. Yes, I am Avivah Litan, can you hear me now? Can you hear me now? I am Avivah Litan, I am a vice president at Gartner, and I follow identity theft and security. And thank you for inviting Gartner here to testify about the issue. Certainly I don't envy you at all. It is a big, huge task to get this out of control.

But ladies and gentlemen, you have to assume that the cat is out of the bag. At least 10 percent of US adult Social Security numbers, and all of these veteran records, could be in criminal hands. In fact, I just heard this morning that sale of Social Security numbers are way up on criminal sites, and I would have to verify that with another source, but we have to assume that that has happened.

Secondly, I think that it is impractical to ask veterans to take control of a problem that they cannot see. So there has been a lot of talk about free credit report monitoring. Sure, that is better than nothing, but there are so many crimes that can be committed by stealing data that you won't ever see with credit report monitoring. So it is not practical to ask any individual, especially a veteran, to have to take charge of this problem when they didn't create it, and they have no control over it, and they have no visibility into how their data is being misused.

So what can we do? Well, there are two practical steps that I think we can take if there is a will to execute. And of course these may sound, you know, beyond execution. But number one, stop relying on Social Security numbers as the ultimate provider of identity proof. When you have all these data elements compromised, you just can't rely on them anymore. That is the facts. So we shouldn't be worried in all this data gets in criminal hands; we need to just assume it is,

and stop relying on it.

Instead, there are things called identity scoring systems that use his Social Security number, along with many other variables to determine an individual's identity. These systems are already used by some of the best lenders and credit card issuers in the country, because they don't want to make a loan or issue a credit card to an identity thief, because they will lose money.

Those same systems should be used throughout, by other sectors including the government sector, the Veterans' Administration, the Motor Vehicle Administration, before dispersing benefits or issuing credentials, in order to protect the innocent from identity theft. You can just imagine, someone is going to get hold of this veteran data, change the address of a check, and then some criminal is going to get the benefit and then the veteran is going to have to go spend months trying to undo this. A credit report monitor would not tell the veteran anything about this.

By stealing a Social Security number, you can get into these free credit reports and sign up for them, and the crook has better access to the credit report than the veteran does, because they can answer the questions that are asked when you register.

So be realistic about this. Just assume Social Security numbers are not reliable anymore.

Number two, we do need to protect the sensitive data we have left and continue to generate, whether it is health records, financial information, telephone records, or anything else. To do so, there are several cost-effective technologies that enterprises and government agencies can deploy to protect data; including data encryption and host intrusion prevention. Of course I am not going to bore you with all the details of these technologies, but you should know that they have become much more cost-effective and easier to implement over the last two years. So these excuses among different companies out undue complexity and high implementation costs are really no longer valid, and they shouldn't be tolerated.

But as you have discussed today, you already know that many data compromises cannot be stopped with technical controls. In fact, they weren't caused by lack of technical controls. If you look at what happened in ChoicePoint, their failure was the result of not extending information security into the registration and verification process of their clients.

Other compromises such as incidences and Bank of America and Wachovia were caused by authorized insiders illegally taking fraudulent action. And of course the compromise of veterans' data at the VA was in part an example of a poor business practice that allowed an employee to bring home 26 million records. And you know, as you have said, it is not this employee's fault completely. It is the process that allowed him to take home all those records.

And in fact, fixing the business process is much harder than implementing technology. But still, security technology is important. We looked at three scenarios that are documented in our testimony that has been submitted to the Committee. We talked about data encryption, host intrusion prevention systems, and more vigorous and continuous security audits. So just those three, if you implement those three systems and processes, you can spend about six dollars just on data encryption per customer account, up to $16 per account, just on 100,000 records.

So if you are looking at 26 million records at the VA, they could do this kind of technology I'm guessing for far less than a dollar per veteran. And you compare that to the cost of a breach, and we have totaled that up to be about at least $90 per customer account, and that doesn't even include government fines and big lawsuits. So you compare a dollar or fifty cents to $90, it is a no-brainer that our data should be protected, a regardless of compliance or regulations.

So hopefully, everyone will be embarrassed enough to take action, but nobody so far—it seems to be very slow.

[The statement of Ms. Litan appears on p. 119]

THE CHAIRMAN. Thank you very much for your testimony. I am going to limit each of us to two minutes. Then we can complete this, and then we can go on. Mr. Filner, you are recognized. You pass? Mr. Michaud?

MR. MICHAUD. No, I just wanted to thank the panelists. It was very informative, and we really appreciate your time coming here. And thank you again, Mr. Chairman.

THE CHAIRMAN. Thank you. Mr. Udall?

MR. UDALL. Did most of you hear the earlier testimony?

MS. LITAN. Yeah.

MR. UDALL. And you heard the number thrown around, 100 million, 500 million, in terms of losses and things? Do you have any comment on that? I mean, do you, in terms of what you heard here, what kind of damage might be done?

MS. LITAN. In terms of the damages caused, the total aggregate, I really think that nobody has a clue. But you can't assume that the average cost of an identity theft, if it is a new account, it is about 1500. The FTC probably has better data on that than us. But if it is $1500 times 26 million, that would be probably the average worst-case.

MR. PRATT. I don't have anything—

THE CHAIRMAN. Excuse me?

MR. PRATT. I don't have anything to add. I think that using the FTC numbers as a baseline is a good approach if you are just trying to estimate general risk.

MR. UDALL. Yeah. And Mr. Hoffman, you have anything on this?

MR. HOFFMAN. Yeah, nothing major to add except that it could be zero. We don't know—obviously, there is an enormous potential liability. Significant trust damage has been done, but it is very possible that somebody just tried to rip off a laptop, and didn't know anything about it, you know, and immediately just erased and sold it, or ripped the hard drive out of it and resold it. You don't know. But the number can be enormous.

MR. UDALL. Do any of you have any critique on the way the Veterans' Administration was operating, in terms of the testimony you have heard here?

MR. HOFFMAN. I would say that there is—they represented to you what in my experience is an absolute poster child for what is going on in corporations and organizations, public and private. This is a system problem that requires people, and process, and technology, and they had issues at multiple phases of that. You know, the analogy is you can build a very safe car, and you can't somehow and necessitate a very safe driver in that car. And ultimately, security becomes a set of trade-offs around this. So I would just tell you that they are not alone, and unfortunately, they are not unique.

What does seem to differentiate them from many of the companies I have dealt with is the massive dispersion of the IT infrastructure, and the control of that infrastructure. Again, it is extremely hard to secure something you can't manage. And when it is that distributed, it becomes really hard to control.

MR. PRATT. I would only add that if I recall, one of the witnesses talked about an individual who had dual responsibilities: IT and then security. That may not be the accurate description, but good data management starts with a chief privacy officer, a chief information security officer, a set of highly trained individuals who have very specific skills in both the knowledge of the—the technical knowledge of data security. Encryption isn't the only solution, for example. It is a much wider array of strategy. But if you don't have the infrastructure that answers right up through—in the corporate world, it would be right up through the Committees of the board that would have oversight for that—you really don't have the proper infrastructure to even begin to make the decisions to address the dispersion, to oversee the proper management of the data.

MR. HOFFMAN. That is exactly right. We have been working very much with a large mutual fund company in Boston who had a very similar event two or three weeks ago: losing a laptop with information on it. There is no ambiguity about who is responsible for that. The response is lightning fast, because there is a chief information security officer reporting either to a chief information officer, or a chief risk officer. And they are empowered and accountable, and it goes right up to the board to answer the problem.

MR. PRATT. And in the private sector, it is risk-based, all of these

decisions are risk-based decisions the corporations are working into their infrastructure.

THE CHAIRMAN. In this case, the risk base is the American taxpayer.

MS. LITAN. I would also like to point out that private sector is governed in many cases by the Payment Card Industry standard, that has a definite chain of command, and penalties if there is no compliance. Here, I don't see any distinct rules that they are subject to and any reason that they have to get fined. So there is no stick.

I get a lot of calls from companies that are complying with PCI, and they are damn worried about fines from Visa and MasterCard, and that is what motivates them. I don't see the same kind of motivation at the VA.

THE CHAIRMAN. Well, nobody has any enforcement. Gartner consulting, are you still on contract with the VA, do you know?

MS. LITAN. Yes, we are.

THE CHAIRMAN. Okay. Since this incident has occurred, has anybody from the VA contacted you, Gartner consulting?

MS. LITAN. Personally, I haven't been contacted. I think—and I can't really speak for the company because there are a lot of points of contact, so—but I think the main contact was on this hearing.

THE CHAIRMAN. EMC, do you have a contract with the VA?

MR. HOFFMAN. We have sold stuff, yes, we have sold products.

THE CHAIRMAN. Sold on hardware.

MR. HOFFMAN. Yeah. And some software. And we have been in some significant conversation over the last few days on how we can help with this.

THE CHAIRMAN. Before some of these incidents had occurred, you know, I have got Secretary Cadenas still here, we had a hearing because in our disability fraud cases we individuals on the inside doing things they shouldn't be doing, and that's of he really worked on, compliance.-- He works with the IG. So those things happen.

I had a conversation with an individual CIO of one of the Fortune 20, and I asked a basic question, "So could any employee pull down the entire personnel record, or the customer list of your company, and take it home?" You know, he laughed at me. No, I'm serious, he laughed at me like that was the most ridiculous question he had ever heard, because there is no way possible they would ever let that occur.

What is your response to that? Tell me what is happening out there in the private sector? Why did he laugh at that question?

MR. HOFFMAN. Fortune 20 financial services firm?

THE CHAIRMAN. No, a Fortune 20 in the world. Sales, and sales.

MR. HOFFMAN. What industry?

THE CHAIRMAN. I am not going to tell you.

[Laughter.]

MR. HOFFMAN. The reason I ask is because we see a significant deviation in industry vertical to industry vertical. Typically, defense and intelligence get this, know what they are supposed to be doing around protection of confidential information. Financial services, particularly the large banks, get this. Healthcare organizations are beginning to, but there is a very steep falloff in the understanding and awareness of information security, issues, technology, organization structure. But if you are speaking to somebody in one of those higher-end verticals when it comes to security—

THE CHAIRMAN. It is.

MR. HOFFMAN. —it is laughable, because they have dealt with, you know—they know that they are personally liable. These are information companies. To lose the information is to lose the company. In banks, they trade in information, that is their business. And they are very aggressive about making certain things like that can't happen.

THE CHAIRMAN. Well, we already know the advice and counsel to us from Gartner Consulting with Gartner's centralized approach at this, and it was not taken seriously at the VA. The bureaucracy sort of cheered. They felt like they won. We had one of the best in our country as a CIO of VA. He didn't have to take that job. He went in and took that job, very challenging. There were a lot of career employees that had been there for a long time, they don't want to change: "Why should we do that? This model has always worked that way." And you can always come up with a list, very articulate, they sound very sensible, very reasoned.

But the challenge for our, quote, "government," for all departments is to get our arms around this. And both of you may criticize us. You called this "maximum dispersion." I guess we call it "decentralization." I like your term you have used here. And what we did here on a bipartisan basis was to get our arms around this, we needed to empower the CIO, and get hold of the architecture, and begin to then work in the systems. That was our approach.

And we tried to be good listeners to what is going on in the private sector. It has been really challenging, in the 14 years that I have done this, to get government to say it is okay to utilize some business practices and principles. It shouldn't be a radical concept, but it is really challenging, and you know that because you are consultants to, quote, "government." But we provide their budgets every year, and monies come, and they spend monies, and they don't, quote, "have to change." And it is very, very challenging.

I am glad that the acting CIO stayed here, General Howard, I appreciate that, and Secretary Cadenas, and Secretary Duffy, that you have remained here to listen to this testimony. And I would welcome you to contact them for their expertise and counsel as we proceed.

Thank you very much, you have helped your country.

This hearing is now concluded.
[Whereupon, at 12:15 p.m., the Committee was adjourned.]

APPENDIX

Statement of the Honorable Steve Buyer
House Committee on Veterans Affairs
Hearing on Failure of VA's Information Management

May 25, 2006

Ladies and gentlemen, good morning. This hearing will now come to order.
The purpose of this hearing is to learn more about the recent loss of personal data belonging to as many as 26.5 million veterans and some spouses experienced by the Department of Veterans Affairs. We have a meltdown in VA's information management. According to VA, this meltdown has resulted in a catastrophic failure to safeguard sensitive personal data.

Last Monday, the Department of Veterans Affairs released a statement acknowledging that a data analyst took home electronic data, which he was authorized to access at work, but was not authorized to bring home. The burglary of his home and the theft of his computer resulted in the loss of that data. This serious incident was not communicated to this Committee until Monday, May 22nd, 19 days after that theft.

We must answer some pressing questions, which include: how did this breach in information management happen? What will we do to protect veterans from identity theft? What policies and regulations are in place at the Department that should have stopped the mismanagement of information? And what is VA doing to eliminate the vulnerabilities associated with the security of sensitive information?

Let me be clear, we are here today to inform America's veterans and their families what the government is doing to protect them against fraud and ease their efforts to protect themselves. Our veterans and their families must be assured of how you, Mr. Secretary, will safeguard the information they place in your hands.

Whether or not any identity fraud results from the theft of *this* computer carried home by *this* VA employee, damage has been done. Speaking as one of these millions of veterans, the prospect of fraud, of theft, of the awful prospect of repairing damaged credit, that is bad enough. For that stress to be caused by our own federal government is deeply disturbing, and I know everyone here agrees is intolerable. There will unfortunately be a certain percent of the 26.5 million veterans that will have to deal with identity theft in the normal course of life, and now some of them will blame the VA. Beyond the very personal dimension, this incident has implications regarding the larger picture of control over VA information technology.

Beginning exactly 6 years ago, compelling evidence of an information security problem at VA has existed, if anyone wanted to pay attention to it. I refer to the following Committee hearings:

At the May 11, 2000 hearing, GAO stated that computer security "is critical to VA's ability to safeguard its assets, maintain the confidentiality of sensitive information, and ensure the reliability of its financial data. The VA IG acknowledged there are "Department-wide weaknesses in information system security that continue to make VA's program and financial data vulnerable to error and fraud."

At the September 21, 2000 hearing, GAO stated, "serious computer security problems persisted throughout the department and VHA because VA had not yet fully implemented an integrated security management program and VHA had not effectively managed computer security at its medical facilities."

At the April 4, 2001 hearing, the IG continued "to identify significant information security vulnerabilities that place the Department's data systems at risk of unauthorized access and disclosure." The IG testified that "many of these vulnerabilities exist in violation of VA policy."

At the March 13, 2002 hearing, the IG repeated findings on the vulnerabilities in VA's information security.

At the September 26, 2002 hearing, the IG testimony stated "penetration testing completed during the past 2 years verified that VA's information system could be exploited to gain access to sensitive veteran healthcare and benefit information.

At the March 17, 2004 hearing, VA testified that "there was a 'glide path' in place for meeting the April 2004 deadline for the beginning of VETSNET deployment." I have been told that VETSNET will not deploy in 2006, and maybe not even in 2007.

As Chairman of the Subcommittee on Oversight and Investigations and now as Chairman of the full committee, I have led a bipartisan effort to centralize VA's IT infrastructure and control over its information systems. Last November, the House voted unanimously (408-0) to centralize IT management in the department's chief information officer. Both the department and the Senate have sadly resisted such a centralization of VA's IT architecture. Even the Independent Budget VSO's oppose centralization of VA's IT infrastructure in their 2007 Independent Budget.

The VA Inspector General, in his November 2005 report entitled, *Major Management Challenges Fiscal Year 2005*, stated that "VA has not been able to effectively address its significant information security vulnerabilities and reverse the impact of its historically decentralized management approach." The report went on to state, "While VA has accelerated efforts to improve Federal information security, more needs to be done to put security improvements in place that effectively eliminate the risks and vulnerabilities of unauthorized access and misuse of sensitive information." Within that context, of damaged trust, angered veterans and families, and systemic flaws, I consider this a wake-up call that can in fact bring about some good. But only if we pay attention and take action.

Our first witness is the Secretary of Veterans Affairs, the Honorable R. James Nicholson, and we welcome the Secretary on what is sure to be a demanding day.

Secretary Nicholson is accompanied by the Honorable R. Allen Pittman, Assistant Secretary for Human Resources and Administration; the Honorable Robert J. Henke, Assistant Secretary for Management; Retired Army Major General Bob Howard, Acting Assistant Secretary for Information and Technology; Pedro Cadenas, Jr., Associate Deputy Assistant Secretary for Cyber and Information Security and Acting Deputy Assistant Secretary for Information

Statement for Mr. Strickland

Thank you Mr. Chairman.

This problem – whatever its root causes – may touch the lives of one in every eleven Americans. In a worst case scenario, this problem may be with us for decades. For those unscrupulous individuals whose career choices might embrace stealing the identity of others for their own financial gain, this data is the equivalent of winning the lottery. With over 26 million names in the data base, someone could divide it into manageable blocks of 10,000 or fewer identities and sell them off. An attempt at identity theft stemming from this incident might occur next week, next year, or even twenty years from now. Other considerations rise from the reactions of veterans with heightened anxieties to this type of threat. Many veterans' lives are touched – and none will be better off because of this situation.

Many, many questions go unanswered Mr. Secretary – I anticipate your cooperation in addressing some of these. For example, how long did this employee have the data at home? Who knew? When did they know? Did the parent information system record the downloaded information, authorization and information parameters? Were recommendations for internal improvement supported, or were they watered down because of internal resistance? Why were warnings ignored about VA's poor internal information controls and why was so little done to address the problem?

Mr. Secretary, the time for candor is now. What exactly was this project the employee was involved in? What information could that employee possibly mine from just name, social security number, and date of birth that would be of any use to VA? Even adding the overall numerical disability ratings to some individual's data fields seems to produce little of use for data mining.

Were specific disability codes included in any of the missing data? These codes are very specific -- some are very revealing about a medical condition. For example, a code of 9404 will tell you something very specific and of a medical nature. Why did so much time elapse before the situation was disclosed to Congress?

Over three weeks have passed since the alleged burglary. This story has been told and retold on most mainstream domestic media outlets. If our questions directly relate to the ongoing investigation, we may understand

your silence, and your unwillingness to answer. But if there is not a relevant link to the ongoing investigation, we expect candid answers. Twenty-six million veterans deserve nothing less.

Are you willing to address these issues?

(Note: may wish to recommend swearing in the panel)

Yield back.

The Honorable Michael Bilirakis
Committee on Veterans' Affairs
May 25, 2006

Hearing on the Data Security Breach at the Department of Veterans Affairs

Thank you, Mr. Chairman.

I wish we were here today under different circumstances. Like my colleagues, I am extremely concerned about the data security breach that occurred earlier this month when a VA employee took veterans' sensitive personal information home without permission and it was stolen when the employee's home was burglarized.

Veterans and their families are understandably upset that their personal information has been compromised, and they have good reason to be. I think everyone at one point or another has seen or read a news report depicting the time-consuming and frustrating hurdles that identity theft victims must go through in order to reclaim their lives.

According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all fifty states, and complaints regarding identity theft have grown for four consecutive years. A 2003 FTC report found that identity theft had resulted in losses to businesses and financial institutions totaling nearly $48 billion over a five year period. Over that same period, consumer victims experienced approximately $5 billion in out-of-pocket expenses. In 2005, there were approximately 17,000 identity theft complaints in my State of Florida alone.

This security breach never should have happened, and there are serious questions that need to be answered. Why was an employee able to remove such sensitive information from the VA so easily? What security protocols are in place? Were these safeguards deliberately bypassed? How many other VA employees have access to sensitive information? Under what, if any, circumstances should VA employees be allowed to remove such information from VA premises?

This Committee and the Oversight Subcommittee have focused a great deal of attention on the VA's management of its information technology infrastructure. Since 2001, the VA Office of Inspector General has reported multiple security vulnerabilities related to the VA's information and data systems. In light of this security breach, the VA clearly has not taken sufficient steps to address these vulnerabilities.

In additional to the issues I've already raised, I am particularly concerned by reports that the VA may have waited several weeks before notifying law enforcement officials of the theft. Given the enormity of the situation, I do not understand why the VA would delay notifying law enforcement officials. Did this delay impede the investigation and potential recovery of the stolen data?

Our veterans and their families deserve to know that their private information is protected. I hope that they will hear some reassuring news today that the Administration and Congress will do everything we can to protect them.

Mr. Chairman, I look forward to working with you and my Committee colleagues to ensure that steps are being taken to safeguard veterans' sensitive information.

Thank you, Mr. Chairman.

OPENING STATEMENT OF LUIS V. GUTIERREZ HOUSE COMMITTEE ON VETERANS' AFFAIRS

"Oversight hearing on the recent theft of sensitive information belonging to as many as 26.5 million veterans and spouses from a VA employee's home"

Thursday, May 25, 2006

Thank you, Mr. Chairman, for calling this hearing today. The loss of identifying information of 26.5 million veterans and their family members is one of the most serious situations the VA has confronted since I've been a Member of this Committee.

When the VA finally came clean two days ago and told us the personal information of almost every veteran had been compromised, they said the theft happened "sometime in May."

Now, we know that the VA decided to keep the theft quiet for more than two weeks. They didn't call in the FBI and they didn't tell our veterans. Instead, the VA decided to handle one of the largest losses of personal identifying information in our nation's history as an internal matter. Someone at the VA decided the Inspector General alone could handle the issue.

This is the same IG that took almost a year to explain to Illinois veterans that demographics were to blame for their low disability compensation rates compared with veterans in other areas. So, I don't think it is too unreasonable to say that the IG may not be equipped to track down and retrieve 26.5 million identities that may be in the hands of criminals.

The VA is now sending out letters to veterans in the lowest ranked states informing them how they might revisit their previous claims.

In fact, it took an act of Congress for the VA to do that outreach and it might take another act of Congress for the VA to get out of this mess.

Yesterday, I was pleased to work with my colleague, Darlene Hooley, in her effort to address the VA breach at the Financial Services Committee during a mark-up of data security legislation.

It is important to ensure federal agencies like the VA promptly notify victims when their personal information is compromised. After today's hearing, I look forward to working with my colleagues to make sure that a breach of this magnitude never happens again.

There are many questions that remain unanswered about this breach. Hopefully, today we can get to the bottom of why this happened and assure our veterans we will keep their personal information as secure as they've kept our country.

Opening Statement of the Honorable Cliff Stearns

Committee on Veterans Affairs

May 25, 2006

335 Words

Mr. Chairman, thank you for holding this hearing today on the troubling turn of events. I am deeply concerned that nearly 27 million veterans may be affected by a security breach that could compromise sensitive, personal information.

What is frightening here is that we don't know if, or when, the second shoe will drop. These veterans' most sensitive information, their Social Security numbers and dates of birth, are hanging out there for any savvy identity thief to wreak financial and psychological havoc. Or, if we are lucky, the thief does not know what he or she has, or the stolen laptop has been scrubbed, and the millions of records will never be opened and used against these veterans. But it may be weeks, months, or years before it is known. No one deserves the frightening uncertainty, least of all our dedicated military men and women, who would never have any reason to doubt the Department charged for caring for them.

I also am a little mystified of the timeline. The burglary was May 3, the FBI I understand was notified on May 16, and we were notified and briefed of the incident by Secretary of Veterans Affairs R. James Nicholson on May 22, 2006. So I look forward to learning about this.

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

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

Statement for the Record of Hon. Corrine Brown of Florida

House Committee on Veterans Affairs
Full Veterans Committee Hearing relating to
the Data Security Breach at the Department of Veterans Affairs
May 25, 2006; 9:00 am
334 Cannon HOB

Thank you Mr. Chairman and Mr. Filner, the new Acting Ranking Member on the Committee.

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

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

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

You are "outraged at the loss of this veterans' data and the fact an employee would put it at risk by taking it home in violation of our policies."

Why are you outraged? You ordered the investigation to look into the disappearance. This was your call and you blew it.

You also say that your "first priority was to take all actions necessary to protect veterans from harm and to assist in law enforcement efforts."

Your first priority should be to stop this from happening. Who has access to all these files? How many disks have been made? Why don't you know?

Written Statement for the Record
Congressman Richard H. Baker
before the
House Veterans Affairs Committee
"Failure of VA's Information Management"
May 25th, 2006

Mr. Chairman, on Monday, May 22, 2006, the Department of Veterans Affairs (VA) released a statement acknowledging that data containing identifying information to include names, Social Security numbers, and date of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings, was taken home by a VA employee, a data analyst. The employee's home was subsequently burglarized, and this information was reportedly stolen.

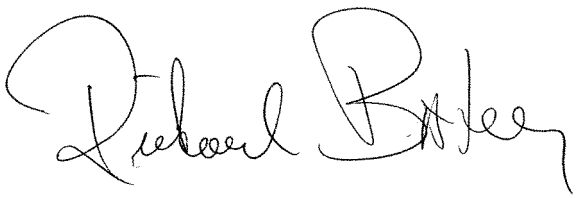
Unfortunately data security breaches have been occurring far too frequently. The breach at the VA is a prime example as to why our colleagues in the Financial Services, Energy and Commerce and Judiciary Committees have been working for months to enact common-sense legislation to address this problem.

As stated, the breach at the VA could possibly affect millions of veterans, resulting in the largest unauthorized disclosure *ever* of Social Security data and possible credit fraud.

Mr Chairman, as we move forward to resolve this issue, I believe that any data security legislation should place the burden of addressing a data breach on the entity responsible, whether it is a federal agency, data broker, financial institution, retailer, or any other party.

In other words, should an entity lose sensitive data, which then directly causes an economic loss to a third party, that entity at fault should be responsible for *all* economic costs associated with protecting consumers that have been affected by a security breach.

As this Committee begins to examine ways to ensure that this never happens again, we must remain steadfast in our obligation to protect every veteran's personal information. I look forward to working with the Committee on this endeavor.



Opening Statement of Congressman Michaud HVAC VA Data Breach
May 25, 2006

Mr. Chairman, thank you for holding this hearing to address this significant, shocking and shameful breach in the security of veterans' personal information.

We do a disservice to the men and women who have served our nation and their families if we allow VA's information security policies and practices to continue as the status quo.

This breach in the security of personal data should have been a wake up call to VA.

Unfortunately, VA did not immediately call for a stand down to do a rigorous review of its policies and practices to identify vulnerabilities in its data systems. I am also extremely concerned by reports that VA did not inform law enforcement immediately about this breach.

While it may be tempting for VA leaders and others to put the blame for this debacle at the feet of one employee, doing so misses the larger problems with VA's IT security. These larger problems rest not with a single data analyst but the leadership of the VA and its security policies.

We need to know how this dangerous breach happened so that we can hold individuals accountable, but more importantly we need to know – right now – what we can do to prevent it from ever happening again and make those changes immediately. And we need to take immediate steps to protect the potentially millions of veterans who have been put at risk by this situation.

It is a matter of public trust.

If we don't tackle the larger issues, then it is only a matter of time before another breach of data happens. We need to focus on the vulnerabilities of VA's data systems rather than focusing on just one individual act. We should not have a system that results in harm to veterans or their families when an individual error occurs.

VA's IT security system must focus both on prevention, and targeting and eliminating system vulnerabilities. The VA has been a leader in creating a culture of patient safety. The VA needs to learn from this experience and be a leader in creating a culture for data security.

Again, thank you Mr. Chairman for holding this timely hearing.

Honorable Jeff Miller
Hearing on the Failure of VA's Information Management

May 25, 2006

Mr. Chairman, I appreciate your taking the lead on this issue and holding this hearing.

We were all shocked to learn – three weeks after the fact – that sensitive information on more than 26 million veterans was not only taken from the Department of Veterans Affairs

headquarters, but was then stolen from that employees' home. Clearly, there are vast failures in the Department's security procedures, and I question when the Department actually learned of the theft and why it took so long to notify Congress.

In order to receive benefits and services from VA, veterans and survivors must provide their home address, phone number, date of birth, and social security number.

They absolutely must have faith that this highly personal information will be treated with the utmost care by the federal government. That faith is indeed being tested now, and we must hope that the person or persons in possession of this data don't use it for ill-gotten gains.

There are a myriad of questions that must be answered, and safeguards that must be taken to protect those who have honorably served our country.

I expect the Secretary, the VA's Office of Inspector General, and the Federal Bureau of Investigations to do absolutely everything in their power to address this situation now.

Mr. Chairman, I will be submitting questions for the record.

Statement of Representative Stephanie Herseth

Full Veterans' Affairs Committee Oversight Hearing Regarding the Recent Theft of Sensitive Veterans' Information

May 25, 2006

Thank you, Mr. Chairman. I would like to express my disbelief and disappointment ~~outrage~~ regarding the VA's recent announcement that the personal data of as many as 26.5 million veterans has been compromised because files containing their names, Social Security numbers, and dates of birth were stolen from the home of a VA official who improperly removed this data from the VA.

This is an outrageous, unacceptable violation of the brave men and women who have served our country. Our veterans and their families deserve better. It is the responsibility of the VA and this committee to get to the bottom of this and never let it happen again.

The loss of these personal records has placed 26.5 million Americans at great risk for identity theft and has the potential to generate a national financial disaster - if the compromised information should fall into the wrong hands. While the VA and law enforcement agencies have taken many important steps to inform the veterans of the situation and investigate the incident, many questions remain unanswered and many changes to the VA's policies, regarding the handling of sensitive information, will need to be made.

I hope that today's hearing will shed some light on these unanswered questions and lead to better safeguarded information security systems at the

VA. We must work to ensure that the personal information of our nation's veterans is protected always and without compromise ~~and this never happens again~~.

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

Honorable John Boozman
Hearing on VA's Loss of Veteran Data
May 25, 2006

Mr Chairman – I am sure every member here is angered and embarrassed by this data security fiasco. We are angry because millions of our constituents are now faced with the very real possibility of financial ruin not of their own making. We are embarrassed because the agency for which we are responsible to our veterans and their families has made a profession out of avoiding real reform in how it manages its information technology systems.

Mr. Chairman, this committee has worked in a bipartisan manner on VA information technology reform for over 10 years and passed a bill that would have put the organization in place to make real changes at VA. The House passed that bill. It is unfortunate that the Secretary convinced the other body to ignore this excellent legislation. And, the VA continues to obfuscate and prevaricate over how to manage its information systems.

I note just a couple comments made by the VA Inspector General and GAO.

"Department-wide weaknesses in information system security that continue to make VA's program and financial data vulnerable to error and fraud."

"VA has not been able to effectively address its significant information security vulnerabilities and reverse the impact of its historically decentralized management approach."

Mr. Chairman, I am normally not one given to expressing strong emotions, but I cannot tell you how much this has disturbed me and you will have my full support to make sure this does not happen again and that the appropriate people are held accountable. Thank you.

Congressman Tom Udall (NM-3)
House Veterans Affairs Subcommittee
On Disability Assistance and Memorial Affairs
Hearing on VBA Fiduciary Program
June 8, 2006

Mr. Chairman,

"Deter identity thieves by safeguarding your information." This is the very first commandment of protecting one's identity. Yet we are here today to accept testimony of how the United States Department of Veterans Affairs found themselves investigating the theft of the personal information for 26.5 million American veterans. Mr. Secretary, this is irresponsibility of the highest order.

The fact that one individual, in case a VA data analyst, has the ability to walk off of VA premises with personal information on 26.5 veterans is in and of itself a matter to be addressed immediately. There is no doubt that VA employees are hard-working individuals who may find themselves taking resources off VA premises for work purposes. But to allow the opportunity for such sensitive information, and in such a massive amount, to be transported is an absolute error. Unfortunately, this is only the beginning of the problems catalyzed by the VA's announcement on Monday.

During a briefing earlier this week, representatives from the VA were unable to answer what I believe are basic questions: What information was taken by the data analyst? For what purpose was this date taken? Was the data encrypted? Were health, disability ratings, or financial codes including in the data? Why was the analyst able to take the information out of a secure area and keep it at home? Do other employees have similar data at home, either with or without the permission of their superiors? Has this policy been changed, or has it at least been suspended pending this investigation? The VA was unable to provide answers to any of these questions.

These legitimate and necessary questions are ones that should be, and are being asked by law enforcement officials. But now, we have learned, the VA knew of the data theft for two weeks before alerting authorities, and nineteen days before making it public.

During this time, the VA considered the loss of sensitive information on every American veteran simply an "internal issue" If this is the VA's perspective on protesting veterans' information, it has lost its focus on the mission to "serve those who have served."

Again, there are obvious reasons why some questions cannot yet be publicly answered, as the FBI, VA IG and local authorities continues to investigate the theft. However, I pose all of these questions again today in hopes that those which can be answered will be answered. This is more than simply a question of security threats or personnel policy. This issue transcends bureaucratic process because it had directly and

completely placed the personal, private information of every veteran in America in jeopardy.

Every member of this committee represents thousands of veterans who are now worriedly watching their credit reports, their credit card statements and their bank records, fearing that they will become a victim of identity theft. That some of them have taken every precaution to safeguard against this situation yet still find their information vulnerable is wrong. Mr. Secretary, I would offer the strongest urging that you undertake a serious reevaluation of VA policy on these matters and that you ensure new regulations and rules within the Department that will better secure veterans' information are put into place as soon as possible. As always, this committee stands to assist the Secretary with this and all veterans' issues, and I greatly hope that in the very near future we will be hearing good news on why our veterans' no longer need worry that their personal information will not fall into the wrong hands.

Thank you, Mr. Chairman.

Office of Congressman John Salazar
Opening Statement
HVAC Full Committee Hearing – VA Data Theft
May 25, 2006

- Thank you Mr. Chairman and Acting Ranking Member Filner for holding this important hearing today.

- I am experiencing a mix of emotions as it relates to the news that 26.5 million names, Social Security Numbers, and dates of birth of our nation's veterans were stolen from the home of a career VA employee three weeks ago.

- I am still shocked by the revelation that an employee had access to this large amount of records and that this person had the ability to take them from the VA.

- I'm angered that the VA and the Administration waited for over two weeks to notify law enforcement authorities.

- Given the nature of the information that was stolen, a speedy notification to law enforcement was warranted.

- It seems as though there was a lack of respect for the gravity of this situation and, perhaps, even an attempt to cover up the theft.

- I have many questions that I would like answered in today's hearing and I look forward to hearing from our panel members.

- Our nations veterans put a great amount of trust in the VA and that trust was violated, not only with the loss of this personal information, but in the delayed response as well.

- We can only hope that we as a Congress can gain back their trust.

- With that in mind, I introduced HR 5455 – the Veterans Identity Protection Act which will grant veterans affected by this theft free credit reports for one year.

- There will be a heavy price tag on this, but I am convinced this step must be taken.

- Veterans should be able to monitor their personal credit rating to ensure they have not become the victim of an identity theft crime.

- This Congress would expect any private company to do the same thing if this happened to them.

- We as a Congress must hold the federal government to the same standard.

- Mr. Chairman, in the interest of time I will conclude my remarks, but I would like to reiterate my frustration with this entire situation.

- I hope that my fellow committee members will be tough with their questions and that we will receive candid, honest answers from the administration.

- I thank you once again for holding this important hearing.

Opening Statement of Rep. Terry Everett
Committee on Veterans' Affairs
Hearing Relating to the Data Security Breach at the Department of Veterans Affairs
May 25, 2006

Thank you for being here today Sec. Nicholson. I hope that this hearing today is only the first step that this congressional body will take to shed some light on breaches in data security at the VA. Our veterans deserve better than this. I know that because of the criminal investigation, that there is only so much you can tell us about this specific problem, but you can fill us in on other measures you are taking to secure other private information such as medical records. I have personally been involved with the VA's IT infrastructure problems, especially when I was the Chairman of the VA O & I Subcommittee. This incident is a direct result of data mismanagement that has plagued the VA for over 10 years. We must ensure that our veterans' personal information is safe, and I look forward to working with you and other VA officials to achieve this end.

Statement of the Honorable R. James Nicholson
Secretary of Veterans Affairs
Before the
Senate Committee on Veterans' Affairs
And
Committee on Homeland Security and Governmental Affairs

May 25, 2006
*

Mr. Chairman and Members of the Committee:

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

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

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

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

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

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

Appropriate law enforcement agencies, including local police, the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. It is possible that the thieves remain unaware of the information they possess or of how to make use of it. Because of that, we have attempted to describe the equipment stolen, the location from which it was stolen and other information in very general terms. We do not want to provide information to the thieves that might be informative as to the nature of what they have stolen. We still hope that this was a common theft, and that no use will be made of the VA data.

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

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

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

I have taken the following actions so far:

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

- This includes:

  - The Privacy Act;

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

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

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

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

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

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

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

Additionally, working with other government agencies, VA has set up a manned call center that veterans may use to get information about this situation and learn more about consumer-identity protections. That toll free number is 1-800-FED INFO (333-4636). The call center is operating from 8:00 am to 9:00 pm (EDT), Monday-Saturday as long as it is needed. The call center is able to handle up to 20,000 calls per hour (260,000 calls per day). Through the end of the day on Tuesday, concerned veterans had made a total of 105,753 calls to this number.

I want to acknowledge the significant efforts of numerous government agencies in assisting VA to prepare for our announcement on May 22nd.

Agencies at all levels of the federal government pitched in to ensure that our veterans had information on actions they could take to protect their credit. Hundreds of people worked around the clock writing materials to inform the veterans and setting up call centers and a website to ensure maximum dissemination of the information. I want to personally thank each of those agencies and those individuals for their selfless efforts on behalf of our veterans.

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

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

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

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

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

On Monday, following the announcement of this incident, I also issued a memorandum to all VA employees. The purpose was to remind them of the public trust we hold and to set forth the requirement that all employees

complete their annual General Privacy Training and VA Cyber Security Awareness training for the current year by June 30.

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

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

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

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

STATEMENT OF
GEORGE J. OPFER
INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
THE COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

MAY 25, 2006

INTRODUCTION

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

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

CRIMINAL INVESTIGATION

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

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

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

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

ADMINISTRATIVE INVESTIGATION

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

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

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

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

As part of our investigation, we will determine if the work the employee was performing at home was related to his official duties, and if he had appropriate authorization to take individually-

identifiable data to his residence. We will also determine if the employee complied with relevant policies and procedures in taking this information home and properly protecting it. Our report will identify what breakdowns occurred that may have hindered timely notification and follow-up of this incident. Based on our investigation, we will make recommendations for appropriate action, if warranted.

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

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

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

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

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

SUMMARY OF OIG REPORTS ADDRESSING INFORMATION SECURITY WEAKNESSES

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

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

Pursuant to the Chief Financial Officers Act of 1990, the VA consolidated financial statements are audited annually. We contract with an independent public accounting firm to perform this audit. As part of the audit, the contractor follows Government Accountability Office methodology to assess the effectiveness of computer controls. The contractor conducts audits at VA's three information technology centers and selected regional offices and medical centers.

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

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

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

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

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

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

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

In total, the FY 2004 report included 16 recommendations: (1) centralize IT security programs; (2) implement an effective patch management program; (3) address security vulnerabilities of unauthorized access and misuse of sensitive information and data throughout VA demonstrated during OIG field testing; (4) ensure position descriptions contain proper data access classification; (5) obtain timely, complete background investigations; and complete the following security initiatives on (6) intrusion detection systems, (7) infrastructure protection actions, (8) data center contingency planning, (9) certification and accreditation of systems, (10) upgrading/terminating external connections, (11) improvement of configuration management, (12) moving VACO data center, (13) improvement of application program/operating system change controls, (14) limiting physical access to computer rooms, (15) wireless devices, and (16) electronic transmission of sensitive veteran data. As of May 23, 2006, all recommendations from this report remain open.

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

needed fixes, we believe VA has a unique opportunity to successfully address all the vulnerabilities and weaknesses discussed in our reports since 2001.

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

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

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

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

CLOSING

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

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

STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Oversight Hearing: Department of Veterans Affairs Data Breach

Committee on Veterans' Affairs

United States House of Representatives

Washington, D.C.

Tuesday, May 25, 2006

Chairmen Buyer, Acting Ranking Member Filner, and members of the committee, thank you for this opportunity to appear before you today. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.[1] We appreciate this opportunity to discuss the Veterans Administration's loss of sensitive personal information on as many as 26.5 million veterans.

Planning and Coordination

This past weekend, CDIA was contacted by the Federal Trade Commission regarding this breach. We are thankful for the FTC's outreach to us, which allowed the CDIA to liaison with our national credit reporting company members who had to plan for likely heavy call volumes on their toll free numbers and hit rates on their websites. Based on this contact our members' technology teams were alerted in preparation for the announcement on Monday, May 23rd. As part of this very late-stage coordination, our members also voluntarily either adjusted current toll free number menus to include special reference for affected veterans, or implemented entirely new toll free numbers which can be used by veterans to request the placement of a fraud alert on a their credit reports. Once a fraud alert is placed a veteran is then, by law, entitled to order a copy of his or her credit report free of charge. Our members report that subsequent to the announcement by the Veterans Administration and ensuing media coverage that call volumes have been running approximately 170 percent over normal rates.

If we have a criticism of this process it is the fact that our members were not consulted sooner by

[1] CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and

the Veterans Administration (the FTC notified us as soon as they were permitted to do so), though perhaps there are extenuating circumstances of which we are not aware. Had the FTC not notified us, we would not have had any opportunity to plan for the contact volumes our members are now experiencing, which are high, but manageable. Even over the weekend, the FTC was not permitted to release the name of the agency and thus our members could not execute plans to customize toll-free number service until after 11:00 a.m. on Monday, May 23rd. Government agencies should be obligated to coordinate with our members well in advance where they intend to publish advice which includes our members' contact information. This is simply the right step to take so that our members can verify the accuracy of the information and ensure that our systems are prepared for increased in contact volumes. Ultimately this obligation helps us all serve affected consumers.

Recommended Steps for Veterans

Your staff indicated interest in hearing what steps we would recommend that a veteran take in response to the announcement. Our views on the key steps for veterans are no different than the information that the FTC has already compiled. We believe consistency in messages is important at this time to ensure that all veterans empowered to take steps that are appropriate to the risk. Following is the latest FTC advice:[2]

Things to Consider

- Because your Social Security number can be used by ID thieves to open up fraudulent accounts in your name, watch for signs that your personal information has been misused. For example, bills that don't arrive on time, receiving credit cards you didn't apply for,

---

employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services.

[2] See http://www.ftc.gov/veterans

being denied credit or receiving unfavorable terms like high interest rates for no apparent reason, or being contacted by debt collectors or businesses about merchandise or services you didn't buy.

- You can order your free annual credit report. You can order online at **annualcreditreport.com**, or by calling toll free 877-322-8228, or by writing Annual Credit Report Request Service, Box 105281, Atlanta, GA, 30384-5281.

- Once you receive your report, review it for suspicious activity like inquiries from companies you didn't contact, accounts you didn't open, and debt on accounts you cannot explain. Check that other information, like your address, date of birth or employer, is correct.

- Consider placing a fraud alert on your credit file. (Note: You may find it more difficult to obtain new credit while there is a fraud alert on your credit file.)

- To place a fraud alert, call the toll free number of any one of the three nationwide consumer reporting agencies. That agency will inform the other two. This alert can help stop someone from opening new credit accounts in your name. An initial fraud alert stays on your credit report for 90 days. After 90 days, if you want to extend the fraud alert for an additional 90 days, you may do so.

  TransUnion: 800-680-7289; **www.transunion.com**
  Equifax: 877-576-5734; **www.equifax.com**
  Experian: 888-397-3742; **www.experian.com**

- When you place a fraud alert with one of these three companies, you'll receive information about ordering one free credit report from each of the companies. Many people wait about a month from when the information was stolen to order their report because suspicious activity may not appear right away.

- If you learn that your information has been misused, file a complaint with the police, and with the Federal Trade Commission at **ftc.gov/idtheft** or 877 ID THEFT. The FTC website also has step-by-step instructions on other measures to take, including an ID Theft Affidavit that consumers can use when disputing unauthorized accounts.

For more information visit:

- Identity Theft Tips from the Federal Trade Commission
  www.ftc.gov/idtheft
- The U.S.Government's Official Web Portal
  www.FirstGov.gov/veteransinfo

- Department of Veterans Affairs
  www.va.gov

We would only add emphasis to the FTC's point that veterans need only call one national credit reporting company to place a fraud alert since our members exchange fraud alert requests. Further, upon placement of fraud alerts veterans are entitled to a free copy of their credit report and will receive instructions for how to order this. Some veterans might be confused about whether or not they need to use **www.AnnualCreditReport.com** to order their free report resulting from placement of the fraud alert, and in this case, the answer is no, they should follow the instructions provided by the national credit reporting company which will be part of a written confirmation that the fraud alert has been placed.

CDIA Position on Data Security and Notification of Consumers

As demonstrated by this breach, data security and the need to notify consumers (including our nation's veterans) where significant risk of harm exists is essential. The following statement delivered during our testimony before the Senate Banking Committee on September 22, 2005 continues to reflect our position on protecting sensitive data about consumers:

> *"The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft has expanded beyond the boundaries of financial institutions. It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a 'financial institution.'"*

As this committee knows, there are a number of House and Senate committees that are focused on developing uniform national standards for ensuring the protection of sensitive personal information. We believe that enactment of national standards will ensure that sensitive personal

information is protected by all who possess it, including federal and state governmental agencies. New nationwide safeguards regulations authored by the Federal Trade Commission will compel all to deploy physical and technical strategies for the protection of sensitive information about consumers.

Ultimately national standards for the safeguarding of sensitive personal information will address consumer concerns and perceptions, including those of veterans who rightly expect that their information will be secured. These are all good public policy results and CDIA remains committed to a constructive dialogue as various bills move through the House and Senate.

Conclusion:

As we head into a Memorial Day weekend, we must redouble our efforts to pass strong and effective national law that will require all to secure personal information properly and to notify consumers when there is a significant risk of identity theft due to a breach of such information. We should do no less for our veterans who have served us all.

Thank you for this opportunity to testify and I would be happy to answer any questions.

Testimony to the U.S. House of Representatives Committee on Veterans Affairs

---

Information Security at the Department of Veterans Affairs

Dennis Hoffman
Vice President of Information Security
EMC Corporation
May 25, 2006

Mr. Chairman, thank you for the opportunity to testify before the House Committee on Veterans Affairs. EMC is the world's leading provider of technology that allows organizations of all sizes to store, manage, protect, *and secure* their most critical asset: their information. We invest more than $1 billion annually ($1.2 billion this year) in research and development to innovate technology solutions that allow enterprises to manage, store, protect, and secure their growing volumes of information; from its creation, to its ultimate disposal, helping them efficiently, *and securely*, gain the maximum value from their information throughout its lifecycle.

I am Dennis Hoffman, Vice President of Information Security at EMC Corporation. Data breaches are happening at an alarming rate. Last year, at least 23 million—or about one in nine—Americans received notification of a data security breach.[1] The Department of Veterans Affairs is not alone. Organizations—from government entities to commercial enterprises—all face this problem. Despite the media's focus on breaches involving personal information, the problem is not limited to this type of information. Organizations create many types of sensitive or mission critical information; many government agencies' and commercial businesses' primary product is information, which they cannot afford to be compromised.

Despite massive investments in security technologies, few organizations today in the private sector feel their data are secure because the majority of today's security solutions protect networks, data centers, and resources, but not information itself. The historic threat of external hackers has driven IT professionals to take a "perimeter security" approach to securing sensitive information.

The fundamental issue with this approach is that while these are necessary investments, they are not complete and do not solve the problem. Commercial enterprises spent more than $6 billion on security software last year.[2] Despite that investment, 82 percent of commercial enterprises do not feel their data are secure or "adequately protected".[3]

Even though the nature of security threats is changing, the majority of enterprise data security spending is still "perimeter-centric"—aiming to protect the network perimeter from outside threats. Two-thirds of hardware and software spending last year was on perimeter-focused

technologies such as firewalls, virtual private networks, intrusion protection systems, antivirus, and anti-malware.[4]

The problem, however, is that *none of these technologies protects data; they protect the IT infrastructure. None would have prevented the compromise of veterans' data from this breach.* For example, if a laptop or similar device were stolen, it is likely the laptop would have some sort of antivirus software—the largest security software market today—installed. However, this software would do nothing to protect the sensitive information stored on the laptop. Technology exists today, which is used by the National Security oversight committees in The Congress that would render specific information on the laptop unusable. Erecting perimeters ignores the fact that in order to have value, information *moves* throughout or between organizations. Once your information moves (accessed, downloaded, e-mailed, printed, etc.) outside secure perimeters, it is left unprotected.

Additionally, a perimeter security approach ignores the fact that often the threat exists *inside* the perimeter. A comprehensive approach is needed that secures *the information*, as well as the IT infrastructure. Thus, information security has increasingly become an information management issue.

IT professionals are realizing that the *internal threat* is the more detrimental. 70 percent of security incidents that cause monetary loss to enterprises involve insiders.[5] The internal threat may be malicious—such as a criminal stealing credit card data, or it may very well be inadvertent—a human resources worker e-mailing sensitive employee health data outside the company by accident. Internal threats are magnified by the fact that we are an increasingly mobile workforce. Today, nearly a quarter of the world's online workforce works "remotely". Given that workers take their laptops (often containing sensitive material) to work and home again, it is only a matter of time before sensitive data become exposed.

Threats today come from both likely and unlikely sources. While it is necessary to defend against sophisticated hackers who are deft at exploiting vulnerabilities in a system, it is equally important to understand the inherent danger from traditional threats. Media accounts of the data loss at the VA state that the individual responsible was likely not part of an elaborate scheme to steal millions of Social Security numbers, but rather, was the victim of a simple burglary.

However, with no security attributable to the data on the laptop, the possibility for fraud becomes a high value alternative to just selling the device.

This event speaks to a wider information security problem. Organizations often 1) cannot distinguish whether data are sensitive or not, 2) do not know where their sensitive data reside, 3) do not enforce security policies around those sensitive data, and 4) are not able to prove compliance with those policies.

In this breach, the data in question may have been exported from a database. While the database itself was probably "locked down" with all of the appropriate access controls, once the names and Social Security numbers are exported into a file, the controls associated with the database become irrelevant. An Excel spreadsheet, for example, could be stored or moved anywhere: on an insecure file share, employee laptop, or e-mailed outside of the organization. Sensitive data such as these often propagate throughout (and beyond) a network as they are saved, replicated, accessed, e-mailed, manipulated, and resaved. *Moreover, as the file moves and is saved in various locations, the organization has no knowledge of what information is contained therein, and whether it is sensitive.*

While the VA has a security policy that forbids sensitive data from leaving the premises, the policy was unenforceable. Similarly, many commercial organizations have reams of paper-based business and security policies that rarely see the light of day. Not only are they rarely enforced in some automated fashion, but they are often not effectively communicated to an organization's employee base.

Finally, many organizations do not have a way to prove compliance with the policies they have established. This is detrimental for two reasons: 1) policy violations are not detectable in real time to enable corrective action; and 2) they are not able to demonstrate (to internal or external auditors) the effectiveness of the security in place.

Thus, how do we solve the problem of *protecting data* as opposed to protecting the IT infrastructure? The solution to this problem lies in people, processes, and technology, where technology is actually the minor piece. It is important to note that there is no single threaded solution or technology "silver bullet", and to prescribe one would be a mistake.

There must be a fundamental shift in our approach to information security. The focus—rather than being "perimeter" or "network" centric, should be "information" centric. It should aim to secure data themselves. To accomplish this, organizations must start by assessing the security of their data. They must understand and define what constitutes sensitive data, where those data reside, and how those data are being used.

Second, organizations should create policies for the storage, access, and use of those sensitive data. The organization is then able to employ the appropriate mechanisms to enforce those policies *at the data level* by leveraging technologies that enable "Data Element Rights Management," which grants or denies access and use privileges (who can see it, when it can be seen, where it can be seen, if it can be copied, printed, forwarded, and when access should be revoked or expired) based on the policy assigned to the specific data. Thus, the sensitive data are protected at the point of access, whether that is inside the office on the corporate network or on a laptop at home.

Finally, organizations should be able to enforce and prove that they are in compliance with those policies at any time by leveraging automated technologies that provide an audit trail of *authorized* data access, or *attempted unauthorized* data access. This has the dual effect of enabling organizations to detect policy violations on a real-time basis for remediation purposes, as well as to prove that the security they have in place is effective.

Information security need not be the equivalent of boiling the ocean. Within the majority of Federal agencies, the IT infrastructure that supports the enterprise is often highly decentralized and stove-piped. The VA has more than twenty-five separate data centers, which historically have operated under various levels of decentralized management and control. With this degree of decentralization and disparate IT systems, our experience indicates that any comprehensive approach to data security methodology or technology will be exceedingly difficult to effectively implement.

Mr. Chairman, you have been at the forefront of this issue for the past several years, working to empower the CIO of the VA by providing him with centralized authority over IT personnel, IT management, and IT investment across the Department. As a result of your efforts, the Office of

the CIO is finally empowered to develop, plan, and budget for a major data processing center consolidation initiative that would significantly consolidate the VA's existing decentralized IT infrastructure. This initiative should not only be maintained, it should be accelerated. Significant steps can immediately be taken to reduce the data security threat within the VA; however, given the magnitude of the VA IT enterprise, only after an aggressive consolidation initiative would the Department realistically be in position to perform a high quality information assessment, develop comprehensive security strategy and policy, as well as implement the necessary technology, methodology, and automated enforcement controls to achieve comprehensive information security across the enterprise.

An information-centric approach must be supported not only by technology, but more importantly, by people and processes. Organizations should assess the security of their information by classifying data and understanding where those data reside, document and communicate their security policies clearly, enforce the policies appropriately, remediate violations to the policies swiftly, and prove compliance quickly and easily.

This problem is big and the Department of Veterans Affairs is not alone. Today, there exist thousands of technologies that address security. We believe that the plethora of vendors and point products on the market is confusing to security buyers and implementers. Some basic principles of IT best practices – consolidation, standardization, centralized management and control, and the classification of data and systems based on their sensitivity and mission criticality – make this endeavor significantly more feasible. In short, security must become information-centric.

Mr. Chairman, thank you for the opportunity to testify before your Committee. I look forward to your questions and those of the Committee.

[1] Source – The Ponemon Institute, 2006

[2] Source – The Gartner Group, 2006

[3] Source – The Enterprise Strategy Group, 2006

[4] Source – The IDC, 2006

[5] Source – The Gartner Group, 2006

Committee on Veterans' Affairs
May 25, 2006
Testimony of Avivah Litan
Vice President & Distinguished Analyst, Gartner Inc.

"Data Protection is much less Costly than Data Breaches"

Executive Summary

A huge theft of personal data from the U.S. Department of Veterans Affairs (VA) makes it clear that the Social Security number cannot be relied on as proof of identity. Enterprises should use this data only as part of overall "identity scores." The compromise also illustrates just how unprotected some of the nation's most sensitive data is.

Event:
On 22 May, the U.S. Department of Veterans Affairs (VA) acknowledged the theft of personal information on approximately 26.5 million people, including names and addresses, dates of birth and Social Security numbers. The information was held on computer equipment stolen from the home of a VA employee, who had taken the information home without authorization.

Analysis:
Industry research suggests that most of the individuals whose information has been stolen in this incident will not fall victim to fraud or other crimes. The thieves apparently wanted the computer equipment, and likely erased the data on it to make it easier to sell. Still, the records may have been retained and could be sold in bulk to other criminals, who in turn can use the information to create synthetic identities (by combining the Social Security numbers with new names and addresses) or make withdrawals from the bank accounts of the wealthiest individuals. Individual wealth can be easily determined by visiting www.freecreditreport.com — a U.S. government Web site set up, ironically, to help prevent identity theft — and registering for a credit report using a stolen Social Security number and other personal data.

Even though only a relatively small number of individuals will likely be directly affected by it, this incident — the largest theft of Social Security numbers documented to date — should serve as yet another wake-up call for U.S. legislators, who are currently debating identity-theft-related legislation. New laws should hold enterprises accountable for damage caused by their failure to screen for identity theft when issuing new accounts, benefits, credentials, loans and other instruments, and for not employing sound security practices around the storage and handling of sensitive personal data.

This incident also shows that the Social Security number has become an extremely unreliable piece of information and cannot be trusted to be unique to an individual. As many as one in seven adult Social Security numbers in use in the U.S. may already have been compromised.

Recommendations

Enterprises that have an interest in identifying individuals accurately, including financial service providers, healthcare providers and educational institutions: Do not rely on Social Security numbers alone as proof of individual identity. Consider the Social Security number as only one of several data elements that help to create a score for an

identity.

Enterprises that must store sensitive data about customers and other individuals: Protect the data by focusing on strong access controls, data encryption, host intrusion prevention systems, regular security audits and continual vulnerability assessments.

Attachment 1:

Data Protection is less Costly than Data Breaches

Summary

Protecting customer data is much less expensive than dealing with a security breach in which records are exposed and potentially misused. The Payment Card Industry security is a good example of industry data security standards and provides enterprises that manage or store cardholder data with good justification to increase data protection.

Analysis

The recent spate of customer information compromise and data theft provides security managers with plenty of ammunition to justify putting in more-stringent security measures around sensitive information. However, the price tag for such protection can cause sticker shock, and Gartner clients frequently ask: *How can I convince management to approve the expenditure required to better protect customer and business-sensitive information?*

Gartner analyzed the publicly disclosed costs of several recently disclosed incidents and developed estimates of additional relevant costs. We made "ballpark" estimates of the cost of three typical strategies for avoiding such incidents. These strategies are not the only ways to protect data, nor are they the only solutions to all information theft problems. Every business is different, but you can use these scenarios as starting points for developing your justification for security expenditure.

The Cost of Dealing With Failure to Protect Customer Data

A number of data points provide an indicator of the cost of allowing customer information to be exposed through a compromised business process. ChoicePoint (see Gartner research note: "ChoicePoint, Bank of America Cases Should Spur Regulation") mistakenly granted record access to an illegitimate business that exposed and potentially abused 145,000 customer accounts. In the first and second quarters of 2005, the company reported $11.4 million in charges directly related to the incident. This works out to $79 per account in direct charges for legal expenses, professional fees and communications to affected customers. Adding in the embedded costs of cleanup and recovery, systems modifications to provide after-the-fact security improvements and other related indirect costs, Gartner estimates the cost of this exposure to ChoicePoint will be in the range of $90 per exposed account.

Furthermore, ChoicePoint's total market capitalization also dropped by $720 million immediately after the disclosure and remains down more than $350 million. While Gartner doesn't believe market cap fluctuations provide reliable indicators of the impact of individual events, the actions a company will take (or not take) to address the concerns of shareholders, boards of directors, regulators and other external parties can often multiply the financial impact of a large compromise.

When smaller quantities of account information are exposed, the costs per account can work out to much-higher numbers, as the legal and professional fees are amortized across a smaller base. In 2002 (see Gartner research note "FT-18-1317" ZD Settlement Shows Cost of Deficient Privacy Protection"), Gartner estimated that the cost per account — when some 5,000 accounts were

compromised — was closer to $1,500, not including market cap fluctuation. For very large compromises (greater than 1 million accounts), we estimate the direct cost per account will be closer to $50, but such large compromises raise the very real prospect of liability lawsuits, and customer and supplier desertion leading to financial failure. CardSystems (see Gartner research note "G00130308" "CardSystems Flaw Shows Deep Credit-Card Security Problems") had up to 40 million accounts compromised and is barred from accepting Visa and American Express cards, which essentially spells a death sentence for any card processor. CardSystems was eventually bought by another payment company, Pay By Touch.

New Disclosure Costs

The U.S. Congress is considering several identity-theft related bills, and if passed, could impose stiff penalties on corporations that experience data breaches but don't disclose them.

The Cost of Protecting Customer Data

The Payment Card Industry Data Security Standards (PCI DSS) serves as a good example of a private sector response to the data security problem. PCI has expanded the original "Digital Dirty Dozen" into several hundred requirements, but most of these simply codify standard practices, such as the use of firewalls, vulnerability management and antivirus systems. As Gartner noted in "G00125063" "Visa's CISP Is Mostly Reasonable but Has Some High Hurdles," the requirements for encrypting stored cardholder data (or demonstrating effective compensating controls) have been the most difficult to meet. However, as Gartner pointed out in research note "T-22-3173" "When and How to Use Enterprise Data Encryption," encrypting stored data has become more feasible and less costly over the past 18 months.

Other advances have been made in security, such as host-based intrusion prevention (see Gartner research note "G00127317" "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention") that can provide effective security when encryption is not possible — controls that are effective at stopping attacks, not just passing compliance audits. PCI compliance is a good reason for many companies to start implementing these newer technologies, because excuses of undue complexity and unreasonable costs are no longer acceptable. (Other industries and sectors, including the government sector, need to follow the lead of the card industry and adopt standards similar to PCI).

Not all data compromises have been because of the lack of technical controls, nor can all attacks be prevented by technical controls:

- ChoicePoint's failure was the result of not extending information security into the customer registration and validation process.
- Other compromises, such as incidents at Bank of America and Wachovia, have been caused by authorized insiders taking illegal or fraudulent actions.
- The compromise of veterans' data by the VA is in part, an example of a poor business practice that allowed an employee to bring home the (unencrypted) records of over 26 million veterans.

Security processes (see Gartner research note "G00130303" "Prevent Targeted Attacks") must be extended to protect against targeted attacks that may come from a variety of external and internal sources. For many businesses, the hardest and most costly step will be to improve deficient business and IT processes, which has to be done before deploying security technology.

To address the question of demonstrating the return on investment (ROI) of protecting customer data to meet (not just to pass the audit) the PCI DSS requirements, Gartner developed three straw-man protection scenarios to illustrate typical costs: encrypting data, deploying host-based intrusion prevention on all servers, and contracting for a strong security audit and continual vulnerability assessment service. These scenarios provide different levels of both protection and deployment complexity. However, all go beyond simple PCI compliance to reach strong protection of customer data.

Encrypting stored data can provide the most-robust data protection, but if that's unfeasible because of undue cost and complexity, enterprises should deploy comprehensive host-based intrusion prevention systems (HIPS). However, successfully deploying HIPS requires strong server configuration control and additional administrative cost and complexity. Another option for enterprises is strong security audits to validate that the organization has deployed satisfactory mitigating controls, reducing the need for data encryption or HIPS. None of these options are mutually exclusive, but implementing all three will still be less expensive than having to respond to a large-scale data breach.

We make some rough estimates of deploying these protections across a large processing environment that might have as many as 1,000 servers used to handle the processing of transactions involving 100,000 customers. The cost of protection for smaller systems will be less in total but higher on a per-account basis, while larger processors will see higher totals but much-lower per-account costs.

Encrypting Stored Data

Most data theft attacks would have failed if the stored information was encrypted and the encryption keys were sufficiently protected. Network-based encryption appliances can minimize the impact of encryption on existing applications but still require significant integration effort (see Gartner research note "G00129566" "Use the Three Laws of Encryption to Properly Protect Data"). For large processing systems, Gartner has seen estimates of $200,000 for encryption appliances and an equal amount for professional services. Additional fees for process and procedure development and other ancillary concerns would increase the costs to about 20 percent to 25 percent. Gartner estimates that an expenditure of $500,000 would be feasible for protecting large (100,000 or more customer records) processing systems. This level of protection would cost about $5 per customer account in the first year, with approximately $1 per account per year in recurring costs.

Host-Based Intrusion Prevention

When account data has been compromised by direct access to stored data (whether live data or on backup media), encryption may be the most-robust solution, albeit probably the most complex to implement. However, many attacks take advantage of server vulnerabilities to launch attacks against data. If all servers in the processing system (not just the servers holding the data) were protected with effective HIPS, more than half of the reported compromises could have been prevented.

The cost of deploying HIPS includes the cost of the HIPS software agents and the labor required to configure, tune and monitor activities to ensure that business operations are not affected by false blocking actions. For large processing systems, in which as many as 1,000 servers may need to be protected, negotiated annual prices of $350 to $500 per server are feasible, depending on operating system mixes. In typical environments, startup and configuration professional

services should require, at most, six person-months of contract labor or, on the order of $200,000 at the high end. An overall HIPS expenditure of about $600,000 could have prevented large-scale attacks; much less needs to be spent when fewer servers are involved. For 100,000 accounts, this works out to be about $6 per customer account, with recurring costs on the order of $2 per account per year.

More-Vigorous and More-Continuous Security Audits

The PCI DSS program requires Level 1 merchants (typically those establishments processing more than 6 million card transactions per year) and processors to undertake annual audits, and quarterly scans of their networks. Processors must use preapproved security assessors, and large enterprises may use either third-party assessors or their own internal audit departments. The costs of audits using third-party assessors for large companies are typically upward of $60,000. The cost of subscribing to an annual scan service at a large company is about $10,000 to $15,000 for more than 128 IP addresses.

For smaller companies, the audit costs of third-party assessors can range from $5,000 to $25,000, and an automated scan service can cost as little as $1,000 a year. But the business value of low-cost security audits is highly questionable, even though they can satisfy PCI DSS compliance requirements.

Businesses serious about protecting customer data (and avoiding the costs of incidents) should not stop at the minimum level mandated by the PCI. By having a more-detailed annual audit, performing vulnerability scans weekly and using a managed service provider to monitor perimeter security controls and key internal servers, enterprises would detect deficiencies (in controls and processes) more quickly and be provided with recommendations for fixes that would prevent attacks. These actions can be viable, although less-effective, data protection options when encryption and HIPS are not feasible, and they can be designed to ensure that adequate mitigating controls are in place.

For a large processor, the costs of these types of services would be about $300,000 to $400,000 per year ($150,000 audit, $50,000 weekly vulnerability scans and $150,000 managing 20 sensors), but this would include the existing cost of demonstrating PCI DSS compliance. Of course, problems pointed out by such audits would need to be fixed. However, fixing problems before the public finds out about them is invariably less expensive than solving them afterward — the fallout also could be potentially damaging. Thus, the recurring cost per year of this approach is in the range of $3 to $4 per account, independent of the fix-it costs that are spent as a result of the audit's findings.

Bottom Line

A company with at least 100,000 accounts to protect can spend, in the first year, as little as $6 per customer account for just data encryption or as much as $16 per customer account for data encryption, host-based intrusion prevention and strong security audits combined. These unit costs will be reduced drastically if these strategies are applied to protecting millions of customer accounts. This compares with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach. Likewise, these costs may escalate dramatically if proposed legislation mandating fines for each exposed and damaged customer account is imposed. Protecting your data is well worth the investment — with or without Payment Card Industry or other compliance requirements.

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
U.S. House of Representatives, Congress of the United States

Thursday, May 25, 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 for this opportunity to share my observations about the Department of Veterans' Affairs. I previously testified before this Committee in March, 2002, and I have assisted VA in their enterprise architecture, cyber security, project management, IT contingency planning, and IT workforce efforts. I have done similar work for the Executive Office of the President, as well as many other public and private enterprises.

VA has tens of thousands of dedicated, hard-working employees committed to the important mission of serving our nations veterans and their families. But there is a dark side to VA. Its bureaucratic culture is unprincipled, profligate, and intransigent. I have seen them ignore Congress, GAO, OMB, and one Executive appointee after another. Oh, they know how to play the game to get the Executive and Congress to open the budget floodgates, but VA doesn't really care how the dollars are actually spent as long as it doesn't interfere with business as usual at VA.

I have personally seen VA personnel sabotage and subvert hundreds of millions of dollars worth of IT projects and read about billions more wasted on other failures. I have seen a total disregard for one cyber security effort after another. These are only the tip of the iceberg. And why do such things happen at VA? Largely because these systems and efforts would make the utilization of budget and personnel more transparent and thereby make accountability possible.

Changing VA's culture will not be easy, or fast. Three critical ingredients are needed:

- First is accountability. Nothing can change unless and until those who refuse to follow the law or their lawful leaders, and those who waste, subvert, steal, and deceive are held accountable. Not promoted or moved to another position or another agency as is often the case, but reprimanded, demoted, and even fired or prosecuted when necessary. The lack of accountability is why the people at VA do whatever they want, whenever they want.
- The second critical success factor is courageous leadership. Nothing can change unless VA's political appointees and Congress actually hold VA accountable. At a minimum

this means communicating expectations, measuring performance, and following up. This includes rewarding right behaviors, but it also means cutting off the dollars and terminating those who refuse to be part of the solution. This requires courage.

- Thirdly, changing VA's culture will require patience and perseverance. Fully bringing about such a change will take a decade or more. It will require a clear vision of where VA should go – This has existed for years in the concept of OneVA, but that has become little more that a phrase to ignore or pronounce when useful. Change will also require good parenting – of both the nurturing and disciplined variety. It seems perhaps that this Committee is best suited for this role since, like the VA bureaucracy, it has a stronger element of continuity than the Executive and their appointees. And this Committee carries the big stick of budget, and has the GAO to provide it with independent performance measurements.

Bringing about a culture change at VA will not be easy – the forces for the status quo are powerful, apprehensive, and treacherous. But the forces for good at VA are also there to be nurtured. Positive culture change at VA can happen. We all know it should happen, for the good of the Veterans and the rest of the country. And just maybe, if we start with VA, this kind of change can happen elsewhere in Washington. Certainly it is needed elsewhere. So if you ever wondered why so many projects fail at VA, or why DOD can't pass an electronic medical record to VA when a soldier becomes a veteran, or why the parts of Homeland Security still can't share information, you now know the answer. The culture is badly broken. But it can be fixed: If we have the courage, patience, and perseverance to make it happen.

Department of Veterans Affairs

Office of Public Affairs
Media Relations

Washington, DC 20420
(202) 273-6000
www.va.gov

Statement

FOR IMMEDIATE RELEASE
May 22, 2006

A Statement from the Department of Veterans Affairs

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

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

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

notification letters to veterans to every extent possible. Veterans can also go to www.firstgov.gov to get more information on this matter. This website is being set to

-More-

handle increased web traffic. Additionally, working with other government agencies, VA has set up a manned call center that veterans may call to get information about this situation and learn more about consumer identity protections. That toll free number is 1-800-FED INFO (333-4636). The call center will be open beginning today, and will operate from 8 am to 9 pm (EDT), Monday-Saturday as long as it is needed. The call center will be able to handle up to 20,000 calls per hour (260,000 calls per day).

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

# # #

VA's Notification to Veterans

Dear Veteran:

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

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

Out of an abundance of caution, however, VA is taking all possible steps to protect and inform our veterans. While you do not need to take any action unless you are aware of suspicious activity regarding your personal information, there are many steps you may take to protect against possible identity theft and we wanted you to be aware of these. Specific information is included in the attached question and answer sheet. For additional information, VA has teamed up the Federal Trade Commission and has a website (www.firstgov.gov) with information on this matter or you may call 1-800-FED-INFO (1-800-333-4636). The call center will operate from 8 a.m. to 9 p.m. (EDT), Monday-Saturday, as long as it is needed.

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

Sincerely,
R. James Nicholson
Secretary of Veterans Affairs

Department of Veterans Affairs

Office of Public Affairs
Media Relations

Washington, DC 20420
(202) 273-6000
www.va.gov

F A Qs

FOR IMMEDIATE RELEASE
May 22, 2006

Frequently Asked Questions on VA's Letter to Veterans

1- I'm a veteran, how can I tell if my information was compromised?
At this point there is no evidence that any missing data has been used illegally. However, the Department of Veterans Affairs is asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved and contact the Federal Trade Commission for further guidance.

2- What is the earliest date at which suspicious activity might have occurred due to this data breach?
The information was stolen from an employee of the Department of Veterans Affairs during the month of May, 2006. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that veterans may notice suspicious activity during the month of May.

3- I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?
The Department of Veterans Affairs strongly recommends that veterans closely monitor their financial statements and visit the Department of Veterans Affairs special website on this, www.firstgov.gov or call 1-800-FED-INFO (1-800-333-4636).

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

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

5- ***Where should I report suspicious or unusual activity?***
The Federal Trade Commission recommends the following four steps if you detect suspicious
activity:
Step 1 – Contact the fraud department of *one* of the three major credit bureaus:
Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

-More-

Frequently Asked Questions // 2

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

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

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

6- I know the Department of Veterans Affairs maintains my health records electronically;
was this information also compromised?
No electronic medical records were compromised. The data lost is primarily limited to an
individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of
potential use to identity thieves and we recommend that all veterans be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7- What is the Department of Veterans Affairs doing to insure that this does not happen
again?
The Department of Veterans Affairs is working with the President's Identity Theft Task Force,
the Department of Justice and the Federal Trade Commission to investigate this data breach and
to develop safeguards against similar incidents. The Department of Veterans Affairs has directed all VA employees complete the "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by June 30, 2006. In addition, the Department of Veterans Affairs will immediately be conducting an inventory and review of all current positions requiring access to sensitive VA data and require all employees requiring access to sensitive VA data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the

Federal Bureau of Investigation and the Inspector General of the Department of Veterans Affairs, have launched full-scale investigations into this matter.

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

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

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

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)

Questions for the Record
Chairman, Steve Buyer
House Committee on Veterans' Affairs

May 25, 2006

Hearing on Failure of VA's Information Management

Question 1: What actions have been taken, or will be taken by the Department to protect veterans from identity theft?

Response: In May, the Department of Veterans Affairs (VA) initiated a focused program to strengthen data security procedures. The "Data Security – Assessment and Strengthening of Controls" program has two principle objectives, i.e., to reduce the risk of recurrence of data security incidents and to remedy Department material weaknesses. The program includes four phases. Phase 1 involves an "Assessment of Existing Conditions." Initial briefings with VA staff have been conducted to kick-off this phase. Phase II is the "Strengthening of Controls" with regard to sensitive data access, encryption, data storage and protection, and IT infrastructure. Phase III is "Enforcement" and will be accomplished through VA-wide inspections, certification and accreditation activities, and implementation of new Virtual Private Network procedures. Phase IV is the "Enterprise Continuous Monitoring Security Program" which will periodically review all components of technical, management, and operational security. Further, the Department has conducted a survey to determine exactly which systems contain sensitive information, which users have access to that data, and how they access the information. Analysis is ongoing to ensure that access is limited to the minimum staff necessary to perform our mission.

Question 2: What is being done to ensure that a failure of information management such as this never happens again?

Response: VA initiated a focused program to strengthen data security procedures. The "Data Security – Assessment and Strengthening of Controls" program has two principle objectives, i.e., to reduce the risk of recurrence of data security incidents and to remedy Department material weaknesses.

Question 3: How many calls to the call centers have included veterans claiming that there identity has been stolen?

Response: The call centers began operations on May 22, 2006. As part of our initial planning with General Services Administration (GSA), VA agreed that any callers who thought they had been the victim of identity theft or alleged some misuse of their account or personal information would be referred to the Federal Trade Commission's Identity Theft Hotline (1-877-ID-THEFT). In many cases, the caller wanted to provide detailed information to the telephone agent. To date, telephone agents have taken a total of 1,168 reports where the caller has alleged some misuse of their account or personal information. These reports are referred to the Federal Trade Commission for review and any appropriate action.

Question 4: What other Federal Departments and Agencies has the Department been in contact with as a way to proactively offer solutions to veterans for protection against identity theft?

Response: VA promptly held discussions with the Federal Trade Commission regarding appropriate solutions. Moreover, the matter was considered extensively by the President's Identity Theft Task Force, of which Secretary Nicholson is a member. Other members of the task force include representatives of the Departments of Justice, Treasury, Commerce, Health and Human Services, and Homeland Security, the Federal Trade Commission, Office of Management and Budget, Social Security Administration, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration Board, and the U.S. Postal System.

Question 5: What is VA proposing to do for veterans that may be victims of identify theft because of this breach?

Response: The Federal Bureau of Investigation (FBI) has recovered the stolen laptop and hard drive. After an exhaustive examination of the hard drive, they concluded with a "high degree of confidence" that the VA information on the recovered hard drive had not been accessed or copied between the date of the theft of the hard drive and the date of recovery. Further, law enforcement has arrested three individuals for the burglary of the VA employee's home during which the laptop and hard drive were stolen. Information developed after the arrests supports the conclusion of the FBI that the information on the recovered hard drive had not been accessed or copied while in the suspects' possession.

Consequently, it is extremely unlikely, that affected individuals would experience identify theft based related to this incident. Nevertheless, as an added precaution, VA has engaged the services of a company that will perform "data breach analysis" of the VA data file, on an ongoing basis, in order to detect any misuse of the information.

Question 6: What securities are in place to control the sensitive personal data of veterans?

Response: In May, VA initiated a focused program to strengthen data security procedures. The "Data Security – Assessment and Strengthening of Controls" program has two principle objectives, i.e., to reduce the risk of recurrence of data security incidents and to remedy Department material weaknesses. The program includes four phases. Phase 1 involves an "Assessment of Existing Conditions." Initial briefings with VA staff have been conducted to kick-off this phase. Phase II is the "Strengthening of Controls" with regard to sensitive data access, encryption, data storage and protection, and IT infrastructure. Phase III is "Enforcement" and will be accomplished through VA-wide inspections, certification and accreditation activities, and implementation of new Virtual Private Network procedures. Phase IV is the "Enterprise Continuous Monitoring Security Program" which will periodically review all components of technical, management, and operational security. Further, the Department has conducted a survey to determine exactly which systems contain sensitive information, which users have access to that data, and how they access the information. Analysis is ongoing to ensure that access is limited to the minimum staff necessary to perform our mission.

The Honorable Terry Everett

Question 1: Of the data that was stolen, what is the VA's plan to make sure that our veterans' personal data is secure? Is the agency working with the financial services community on this?

Response: VA is pursuing numerous means to secure personal data of veterans, including by not limited to mandating completion of Privacy Act and cyber security training by all employees, contractors, interns, and volunteers, requiring a signature of a Statement of Commitment and Understanding by all employees attesting to their understanding of their responsibilities in securing and safeguarding sensitive data, completing an assessment of each employee's access to systems and sensitive data, completing an assessment of each employees' access to systems and sensitive data, restricting the removal of sensitive data and files from the worksite, requiring data to be encrypted prior to removal from the worksite or prior to electronic transmission, documenting the required clearance levels for all VA staff, and obtaining/updating security clearances. Shortly after the data breach became known, the Office of Management initiated work on an acquisition to procure credit monitoring services fro veterans affected by the data breach. Based on similar data breaches at other agencies, the General Service Administration initiated a government-wide task order providing a vehicle for any agency to obtain like services. Office of Management also coordinated a meeting with Citibank to learn of their capabilities for credit monitoring/recovery.

The Office of Finance has fully accredited all of their systems under the NIST Information Security standards and is in full compliance with the Federal Information Security Management Act (FISMA) of 2002, and the Privacy Act of 1974. These accreditations include the payroll system and the financial management system. The Debt Management Center (DMC) is the Office of Finance organization that handles strictly veteran information. We successfully accredited the CARS/CAROLS system used there, and the DMC provides a secure platform at the Austin Automation Center where the application is hosted.

Question 2: One of my veterans called your center. He said the person simply read from a script based on your Frequently Answered Questions list. We can do better than this.

Response: We worked closely with the General Services Administration as well as private sector companies experienced in operating call centers while developing our plan for handling calls from veterans concerned about the data theft. These experts strongly recommended that VA prepare scripted responses to anticipated or frequently asked questions.

The script has been updated several times since the inception of the project based on input received via daily conference calls with call center contractors and the Veterans Benefit Administration (VBA) staff assigned to each center, as well as the changing situation. We believe the scripted answers provide clear, consistent and accurate information to veterans. Moreover, the VBA employees assigned to each call center

assist call center agents with unusual questions and speak with veterans when the callers' questions are beyond the scope of the scripted answers. They also silently monitor calls to ensure quality, and use their findings to provide training to agents, as needed.

Question 3: A constituent told me that as a result of this incident, he bought a $200/yr credit monitoring service for himself and his wife. The service notifies him within 24 hours of a suspected transfer or if any new accounts are opened with his information. Is this type of credit monitoring an option for the VA to provide these veterans?

Response: As a result of the recovery of the stolen laptop and the FBI's assertion that the data was not compromised, VA has determined that credit monitoring services are not needed. VA is hiring a company to provide data breach analysis to detect potential patterns of misuse of veterans' information.

Question 4: How will you pay for this or similar credit monitoring services? Will you reprogram funds as has been mentioned?

Response: As required, VA will use available funds through reprogramming and request additional funding via appropriation specifically earmarked for payment of credit monitoring services.

Question 5: How does your cyber security training program for VA employees teach them not to take secure data out of the building?

Response: Employee education is critical to improvements in handling and protecting sensitive information. Consequently, all employees have completed annual awareness training for both privacy and information security, and have signed a statement of commitment and understanding as a tangible indication of their pledge to enforce all Department-wide security policies. This training was completed primarily in June. To further promote awareness, accountability, and responsibility, VA has published and distributed a number of memoranda to its management and staff to remind them of their roles in protecting the information of veterans and their families.

The Honorable Jeb Bradley

Question 1: I request to review the policy document, written directive, notice or memorandum which outlines the informational technology security policy/guidelines/regulations related to the handling of electronic data of sensitive nature.

Response: VA Directive 6504, *Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities*, dated June 7, 2006, and VA Directive 6500, *Information Security Program*, dated August 4, 2006, helps to ensure that appropriate safeguards are in place to protect sensitive Department information. Other directives are currently being prepared to strengthen policies on encryption, incident management, tracking and maintaining data extracts, and other controls specified in the National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*

Copies of VA Directives 6500 and 6504 are attached.

Question 2: Specifically, I would like to review the written guidelines/regulations which protect personal information either by firewalls, protocols that were violated when the employee took a data storage device home to work on which was subsequently stolen.

Response: VA Directive and Handbook 6210, *Automated Information Systems Security*, and VA Handbook 5011/5, *Hours of Duty and Leave, (Teleworking)*, were the official policies at the time of the incident.

Attached are copies of VA Directive and Handbook 6210 and VA Handbook 5011/5.

The Honorable Ginny Brown-Waite

Question 1: What employees are eligible for telecommuting?

Response: VA Telework policy covers employees under the General Schedule, including those covered by the Performance Management and Recognition System Termination Act of 1993, members of the Senior Executive Service (SES), and employees compensated under the Federal Wage System (FWS). On a case-by-case basis, the policy also covers Veterans Health Administration (VHA) employees appointed under 38 U.S.C., chapters 73 and 74.

Question 2: Can you provide us with information on the guidelines or regulations pertaining to the use of IT resources by telecommuting employees?

Response: There are numerous citations on IT security references in VA Telework policy, below are exerts from VA Handbook 5011, Part II, Chapter 4, paragraph 6- Telework Criteria:

> VA Handbook 5011, Part II, Chapter 4, paragraph 6 – TELEWORK CRITERIA.
>
> b. **Position Suitability**
>
> (f) No classified documents may be taken to, used, or stored at an employee's home office or telecenter. The employee must return to the traditional office to access and work on such documents or materials; and
>
> (g) Privacy Act materials, evidence, or sensitive documents (hard copy or electronic) may be accessed remotely provided that the employee agrees to protect Government/VA records from unauthorized disclosure or damage and will comply with the requirements of the Privacy Act of 1974, 5 U.S.C. § 552a, and all applicable Federal law and regulations, VA Directive and Handbook 6210, and other applicable VA policies.
>
> c. **Process for Establishing a Telework Arrangement**

(4) The immediate supervisor and employee develop a telework agreement which lists all terms and conditions for the telework arrangement (Appendix II-A of this handbook), and complete the User's Remote Computer Security Agreement. The Agreement is available in the "VA Remote Access Guidelines" located at the VA intranet address http://vaww.admin.vpn.va.gov/one-va-vpn/home/VARemote AccessGuidelines.doc.

(5) The employee notifies the Information Security Officer (ISO) of the telework arrangement and obtains ISO certification approving that the appropriate security controls are in place.

d. **Minimum Participation Criteria**

(3) The telework arrangement must not adversely affect VA's mission and functions. If, at any time, it is determined that an arrangement is having an adverse impact on work operations or performance, the supervisor or the employee may terminate the arrangement with two weeks notice. Supervisor modification or termination of the arrangement requires two weeks notice except where:

(d) the employee breached information security protocol,

e. **Automated Information System Security**. Each Administration and Staff Office with a telework program will ensure that Departmental information security policies, established by the Office of Information and Technology, are strictly enforced and that telework employees are informed that periodic remote computer surveillance may be conducted to ensure information security policy compliance. Each telecommuter will be assigned a VA-owned computer or agree to have the One VA-VPN software installed on their personal computers. Technical requirements for computer connections to the VA network by telecommuters will be published and issued by the CIO. Offices sponsoring telework must also ensure that adequate technological security protections are in place on all electronic devices issued to telework participants. If Federal and VA information security policies, procedures and guidelines are not followed, telework must be terminated. Prior notice to the employee is not required for enforcement and reporting of security violations. Additional security policy information and clarification can be obtained from the VA Office of Information and Technology, Office of Cyber and Information Security (005S). (See VA Directive 6210, Automated Information Systems Security, and VA Directive 6000, VA Information Resources Management Framework.).

f. **Security and Privacy Considerations.**

(1) No classified documents (hard copy or electronic), may be taken to, used, or stored at an employee's home office or telecenter. The employee must return to the traditional office to access and work on such documents or materials. Privacy Act materials and VA data and systems may be accessed remotely provided that the employee agrees to protect Government/VA records from unauthorized disclosure or damage. The employee must also comply with all

legal requirements (for example, Privacy Act of 1974, 5 U.S.C. § 552a), policies and procedures (for example, VA Directive and Handbook 6210) identified by the Administration or Staff Office as necessary to protect the VA data and systems to which the employee will have access under the telework arrangement. Prior notice to the employee is not required to terminate telework arrangements due to security violations.

(2) If any legal requirements (for example, Privacy Act of 1974, 5 U.S.C. § 552a), departmental and office policies and procedures change (for example, VA Directive and Handbook 6210), the employee, upon proper notice, agrees to comply with the changed requirements. Failure to so agree constitutes a basis for termination of the employee's participation in the program.

Question 3: What security measures are in place to ensure that data is not vulnerable for telecommuters?

Response: In order to strengthen security policy and procedures, the Department issued VA Directive 6504, *Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities*, dated June 7, 2006. The directive establishes policy and responsibilities for VA employees and applies to all VA organizational elements. It describes required security measures for mobile or fixed computers, and other electronic and storage media used to transmit, transport, process, store, or access information or connect to VA IT systems from home, travel, or alternative work locations. It also restricts the use of VA data stored in non-electronic form outside the regular work site.

Additionally, VA employees are permitted to transport, transmit, access, and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor and where appropriate security measures are taken to ensure that VA information and services are not compromised. The privilege to use or access VA data outside VA facilities may be revoked or limited at any time by appropriate VA Administration and staff office officials.

Question 4: Did the VA conduct a risk assessment on the loss of this data? And if so, what were the results?

Response: A Department-wide assessment of risks attendant to VA-information management is currently being conducted as an initial component of the Secretary's *Data Security Assessment and Strengthening of Controls* program launched on May 24, 2006.

Question 5: If no assessment took place, can you please shed some light on why this did not occur?

Response: A Department-wide assessment of risks attendant to VA-information management is currently being conducted as an initial component of the Secretary's *Data Security Assessment and Strengthening of Controls* program launched on May 24, 2006.

Question 6: What steps is the VA taking to ensure that sensitive data is encrypted?

Response: On August 11, 2006, a contract was awarded to Systems Made Simple, a small disabled, veteran-owned business, to assist VA in implementing a comprehensive encryption protection program employing Guardian Edge and Trust Digital encryption software. As of September 20, 2006, the Department has installed encryption software on 14,577 of 15,651 total laptops in VA. The remaining laptops are required to be securely stored in a VA facility and are not to leave the premises unless they have been encrypted. The next step is to construct a plan for the subsequent phase which is to encrypt portable media (such as flash drives), desktops, personal digital assistants, and Blackberries.

Question 7: Why do guidelines govern data security? Why are they not Department regulations?

Response: Internal VA guidelines do not govern data security in VA, but are sometimes provided as supplementary information. The security of VA data is governed by Federal legislation, most notably, FISMA, 44 U.S.C. sections 3541-3549. Under FISMA, VA must protect its information and information systems from unauthorized access by complying with information security standards and guidelines required by law, the Secretary of Commerce and the National Institute of Standards and Technology (NIST) (including Federal Information Processing standards (FIPS) documents and the special publications SP-800 series), the Office of Management and Budget (OMB), and, as to national security information and information systems, the President. In addition, FISMA requires that VA develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.

In August 2006, the Department issued VA Directive 6500, Information Security Program, which requires Department-wide compliance with FISMA and related information security issuances pertaining the Security of VA information and information systems administered by VA, or otherwise under the authority, control, or on behalf of VA. VA Directive 6500 will be implemented by one or more Handbooks that will explain and transmit mandatory information security standards and guidelines issued in law, by the Secretary of Commerce and NIST, by OMB or by the President.

The Honorable John Campbell

Question 1: What is the current policy regarding employees taking materials outside the office?

Response: In order to strengthen security policy and procedures, the Department issued VA Directive 6504, *Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities*, dated June 7, 2006. The directive establishes policy and responsibilities for VA employees and applies to all VA organizational elements. It describes required security measures for mobile or fixed computers, and other electronic and storage media used to transmit, transport, process, store, or access information or connect to VA IT systems from home, travel, or

alternative work locations. It also restricts the use of VA data stored in non-electronic form outside the regular work site.

Additionally, VA employees are permitted to transport, transmit, access, and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor and where appropriate security measures are taken to ensure that VA information and services are not compromised. The privilege to use or access VA data outside VA facilities may be revoked or limited at any time by appropriate VA Administration and staff office officials.

Question 2: Was this employee aware of this policy?

Response: VA requires all employees, contractors, and volunteers to complete the mandatory Cyber Security Awareness training, annually. This training is designed to help VA employees understand the importance of protecting sensitive information and make them aware of their responsibilities to protect this information.

Question 3: How many people have been fired in response to this incident?

Response: None

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6504
Transmittal Sheet
June 7, 2006

RESTRICTIONS ON TRANSMISSION, TRANSPORTATION AND USE OF, AND ACCESS TO, VA DATA OUTSIDE VA FACILITIES

1. **REASON FOR ISSUE:** To provide Department of Veterans Affairs (VA) policy regarding transmission, transportation and use of, and access to, VA data outside VA facilities.

2. **SUMMARY OF CONTENTS:**

   a. This directive sets forth restrictions applicable to VA employees' transmission, transportation and use of, and access to, VA data while working in locations other than a VA facility. It describes required security measures for mobile or fixed computers, other electronic and storage media used to transmit, transport, process, store, or access information or connect to VA IT systems from home, on travel, or at alternative work locations. It also restricts the use of VA data stored in non-electronic form outside the regular work site.

   b. Employees have no right to transport, transmit, use or access VA data outside the regular work site except as set forth in, and in accordance with, this Directive. VA Administrations and Staff Offices will establish necessary controls to ensure that the data is handled securely and appropriately.

   c. This directive does not supersede any other applicable law or higher level Government-wide policy guidance, but does supersede any other inconsistent Department, Administration or Staff Office policy, or policy sections, that deal specifically or generally with employees' transportation, transmission, use of, or access to, VA data outside VA facilities.

3. **RESPONSIBLE OFFICE:** The Office of Cyber and Information Security (005S) in the Office of Information and Technology (005) is responsible for the material contained in this directive.

4. **RELATED HANDBOOK: None.**

5. **RESCISSION:** Office of Cyber and Information Security (005S) Security Guideline for Single-User Remote Access, Revision 3.0, dated March 10, 2006.

CERTIFIED BY:

/s/
Robert T. Howard
Senior Advisor to the Deputy Secretary
Supervisor, Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Gordon Mansfield
Deputy Secretary

RESTRICTIONS ON TRANSMISSION, TRANSPORTATION AND USE OF, AND ACCESS TO, VA DATA OUTSIDE VA FACILITIES

1. PURPOSE AND SCOPE. This Directive establishes policy and responsibilities for VA employees' transmission, transportation, and use of, and access to, VA data outside VA facilities. This Directive applies to all VA organizational elements, and all VA employees.

2. POLICY0.

a. General. VA employees are permitted to transport, transmit, access and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor and where appropriate security measures are taken to ensure that VA information and services are not compromised. The privilege to use or access VA data outside VA facilities may be revoked or limited at any time by appropriate VA Administration and Staff Office officials.

b. VAGFE and OE. Only VA-owned Government Furnished Equipment (VAGFE), including laptops and handheld computers, may be used when accessing the VA intranet remotely. VA employees may not use non-VA owned Other Equipment (OE) to access the VA intranet remotely or to process VA Protected Information (VAPI) except as specifically provided in this Directive. VAPI is sensitive information as defined in paragraph 5 titled "Definitions." Access to the VA Intranet using non-VA owned Other Equipment (OE) will be provided via approved VA Virtual Private Network (VPN) access protocols, which will offer access to a limited set of VA applications and services. Only remote access users with VAGFE will be permitted to connect to the VPN in such a way that grants full VA access provided all required security software is installed and updated.

c. Initiation and Termination of Remote Access Accounts. Employees must request and obtain supervisory approval for remote access to the VA Intranet. The employee or supervisor may apply for a remote access account through the Information Security Officer (ISO).

(1) Remote access accounts are as-needed accounts. Unused accounts must be disabled and removed if no longer needed. If a remote access account is not used for a period of ninety (90) days, the ISO will disable the account. If a remote access account remains unused after six months, the ISO will remove the account. If the account is deleted and remote access is subsequently required, the employee must request a new account.

(2) Supervisors will ensure that remote access privileges are terminated as soon as they are no longer needed, when the account owner transfers out of the supervisor's office or leaves the VA, or when an authorized official determines that remote access privileges should be revoked. Upon termination of required access privileges, supervisors will confirm and notify the ISO that the employee has returned all VAGFE related to remote access.

d. System Security. Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Employees may not share with non-VA employees or unauthorized personnel instruction or information regarding how to establish connections with VA private networks and computers. Employees may not share remote access logon IDs, passwords, and other authentication means used specifically to protect VA information or access techniques to VA private networks.

e. Operating System Controls. Employees must use only computers and electronic storage media configured to conform with **all** VA security and configuration policies to store, transport, transmit, use and access VAPI.

(1) Required for both VAGFE and OE:

(a) VA employees must use passwords that meet VA password requirements.

(b) The "save password" feature must not be used for passwords that provide access to the operating system or VA network services

(c) "Blank" and default user names and passwords must not be used

(d) User credentials including passwords are considered VA sensitive information and must be protected appropriately

(e) A shared file or drive containing VAPI must not be created on a device used for remote computing. File sharing of VAPI must only be accomplished through the use of authorized VA servers.

(f) VAPI or VA-specific software must be segregated in dedicated directories that are protected

(g) If VAPI such as Protected Health Information (PHI), privacy information, or information that could be used by unauthorized persons to gain access to VA systems is to be stored outside of the VA intranet or outside of the physical protection of VA facilities, it must be protected. (See the *Data Handling* section.)

(2) Required for VAGFE and for OE used to access or process PHI or other VAPI.

(a) Password-protected screensavers must be configured to activate after five minutes of inactivity.

(b) The screen saver must be activated manually when the workstation is unattended.

(c) Anti-virus software must be installed and operational (refer to paragraph g below).

(e) All devices must conform to operating system hardening guidelines as specified in VA Information Security guidance.

f. Protection from Viruses and Other Malicious Code. Certain protection mechanisms are required to protect systems connecting to the VA intranet and/or containing VAPI against viruses and other malicious code.

(1) VAGFE and OE that contain VAPI must be equipped with, and use, a VA-approved antivirus (AV) software and a personal ("host-based") firewall that is configured with a VA-approved configuration.

(2) In the event that the computer/device connecting remotely is simultaneously attached to a second network (such as an in-home LAN), either the secondary network computers/devices must be provided with similar AV and host-based/personal firewall protection, or all other connections must be severed.

(3) VAGFE devices attempting to access the VA intranet remotely via the One-VA VPN client must have the AV and Host-based Intrusion Prevention System (HIPS) software installed and current, including all critical updates and patches, in order to be granted access to the VA intranet. HIPS software must also be installed and current, including critical updates and patches, on non-VA OE that will connect via the One-VA SSL VPN option before such OE may be used to transport, transmit, access, process or store VAPI. For additional information regarding software required for use on VAGFE or recommended for use on OE, refer to the document titled *"Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN." (This document may be found on the Office of Cyber and Information Security intranet web site.)*

g. Antivirus Software. VAGFE and OE used to transmit, transport, access, process or store VAPI must be equipped with current, VA-approved anti-virus software. The local facility Information Resource Management (IRM) Office or local ISO will provide the software for VAGFE. Employees using non-VA OE devices to access the VA intranet remotely must comply with the policy set forth in *"Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN."* If non-VA OE is connected to a home or small office network with other workstations, all interconnected workstations must have virus protection. Anti-virus software must contain a real-time scanning feature, which must be enabled. Employees must update their antivirus software and check for viruses before use of any diskette or file they encounter that is of uncertain or unauthorized origin. Data and executables copied from removable media, the internet, or email must be scanned for viruses as soon as reasonably possible after their introduction on the computer. Executables must not be launched without first having the origin validated by the sender and verified to be free of viruses.

h. Host-based Intrusion Protection System/Personal Firewall. Employees using VAGFE to access the VA intranet remotely must use the HIPS provided as part of the One-VA VPN client solution. Employees using non-VA OE devices to access the VA intranet remotely must comply with the policy set forth in *"Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN."*

i. Enclave/Perimeter Firewalls. Any employee who uses a computer to connect to the internet outside the regular work site, whether VAGFE or non-VA OE, must ensure that the computer is protected by a firewall. The firewall may be enclave-based or host-based. The boundary between a user and the Internet is considered an enclave perimeter with the user residing in the enclave. Any firewall software and/or firmware must be maintained at the most current release and patch level and configured separately. This includes personal/home use internet routers such as those produced by Linksys/Cisco, D-Link, Netgear, etc., and those used to protect other permanent connections such as Local Area Networks (LANs) of small offices, facilities, etc.

j. Application Software Security. Users with NT, W2K, and systems administration capability must scan their system for vulnerabilities. Those dependent on third-party system administration must arrange to have their systems updated regularly.

k. Virus or Malicious Code Infection Handling. Employees must immediately stop using any computer or software suspected of malicious infection or malfunction. In all such cases, the machine must be immediately isolated from any VA network connections. Do not reboot (turn off/on) the system, as many viruses are triggered to propagate upon system reboot which can cause further damage. If it appears that a negative activity is occurring (such as the deletion of files) then the system must be shut off and left off until a clean Antivirus boot media is used to clean the system. Employees not authorized to attempt recovery and restoration must not remove the suspected software themselves, but must contact a qualified IT Specialist via their respective help desks to attempt recovery. Recovery must be attempted only by an authorized IT Specialist. If a non-VA technician is called to service non-VA OE, the employee must exercise caution to protect VA data, including information that facilitates access to VA private networks. An employee must never surrender or swap hard drives or other storage to an outside party if he or she was storing VAPI at the time of the system problem. Only VA-approved software and tools may be used to attempt recovery from virus or other malicious code infection.

l. Remote Access Configuration. Only VA-approved remote access solutions may be used. All remote connections to VA networks must be through OCIS-authorized configurations and access points. No VA employee is authorized to use VA remote access services to engage in any activity that is illegal or violates VA policies. While connected to VAGFE, do not simultaneously connect to VA and one or more non-VA networks. VPN client software must not be configured to support split or dual tunneling, which allows the user's computer to connect to the VA while simultaneously connected to another public network such as the Internet. Inactive sessions must be terminated by logging off when finished or when leaving the workstation unattended. Employees must not turn off the device or monitor without first logging off. All VAGFE are required to have a password-protected screensaver enabled.

m. Remote Access Via Non-VA Networks. Non-VA networks refer to third-party networks that are considered "untrusted" by the VA. The One-VA VPN gateway, which includes both the IPSec and SSL VPN devices, is the VA's method for securely using non-VA network services to access VA networks. Third-party, untrusted network examples include: dial-up or broadband access to an Internet Service Provider (ISP), visiting a non-VA network, and wireless connections. VA-approved VPN software and/or hardware are required to create VPN or Extranet connections to VA private networks.

n. Remote Access Using Wireless Networks Wireless routers and access points, even if not used at the enclave perimeter, must be configured in accordance with the "*VA Wireless and Handheld Device Security Guideline.*"

o. Data Handling. VA Staff Offices and Administrations must conduct risk assessments and Privacy Impact Assessments as specified in applicable VA policy, and protect VAPI in compliance with the results of the risk and Privacy Impact Assessments.

p. Protection Of Information. VA information may not reside on non-VA system or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and only where the non-VA systems or devices conform to, or exceed, applicable VA security policies or are specifically authorized by VA guidance.

(1) VAPI must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be **validated** by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See http://csrc.nist.gov/cryptval/140-1/1401val.htm for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission.

(2) Passwords or other authentication information must not be stored on remote systems unless encrypted. VA-PKI certificates must be stored in encrypted form only and must be accessible only by using a personal identification number (PIN) or password.

q. Data Stored – Encryption. Additional security controls are required to guard VAPI stored on computers used outside VA facilities. If an employee uses VAGFE or non-VA OE in a mobile environment (e.g. laptop or PDA carried out of a VA office or a PC in an alternative work site) and VAPI is stored on the computer, file or electronic storage media, approved encryption software must be used. The file or hard drive encryption software must be FIPS 140 certified, operated in FIPS 140 mode and all VAPI stored on the computer must be stored in the encrypted partition created by the encryption application. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple safe locations with the supervisor and ISO.

r. Backup. A remote or mobile computer must not contain the only copy of VA records or data. Employees must make redundant copies ("backups") of essential business data and software at regular intervals. Employees must store multiple sets of backup data in protected locations other than the location of the device containing the data. Back-ups and archives must be treated according to their VA security classification.

s. Theft, Loss, or Compromise. If an employee becomes aware of the theft, loss or compromise of any VAGFE or non-VA OE device used to transport, access or store VA information, or of the theft, loss or compromise of any VAPI, the employee must immediately report the incident to his or her supervisor and the local ISO. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements in "Responding to Security Incidents and Malfunctions."

t. Hard-Copy Documents and Physical Media. VA personnel are responsible for ensuring that VAPI, in hard-copy documents or on physical media, under their control, is protected from improper disclosure, including inadvertent disclosure. When no longer needed, VA information classified as VA sensitive must be destroyed by a method rendering it unreadable, undecipherable, and irretrievable as prescribed in the most current version of "Fixed Media Sanitization" (see paragraph 4.b.(12) below) and its attachment.

u. Physical Security. The following rules are applicable to all VAGFE and non-VA OE used to transmit, transport, access, process or store VA data:

(1) Equipment, information, or software must not be taken off-site without express authorization by the employee's supervisor.

(2) Equipment must be housed and protected to reduce the risks from environmental threats and hazards, and the opportunities for unauthorized access, use, or removal.

(3) Portable computers that have VAPI on their storage device(s) or have software that provides access to VA private networks must be secured under lock and key when not in the immediate vicinity of the responsible employee. This includes external hard drives and other storage devices. If such devices are maintained in a hotel room or residence, they must be stored out of sight and the door(s) to the room or residence must be locked when the employee is not physically present.

(4) Employees must use physical locks to secure portable computers to immovable objects when the computers must be left in a meeting room, or other semi-public area to which individuals other than the authorized employee have access.

(5) When in an uncontrolled environment, employees must follow "clear desk" [define] practices for media to reduce the risk of unauthorized access to, loss of, and damage to VAPI. No VAPI may be left on desks.

(6) When in an uncontrolled environment (for example, when traveling on an airplane or in an airport), employees must guard against disclosure of VAPI information through eavesdropping, overhearing or overlooking (shoulder surfing) by unauthorized persons. When traveling, employees must keep portable computers or storage devices in their possession, and may not check them as baggage.

(7) Data and system backups that include VA information have the same confidentiality classification as the originals. Therefore, these materials must be protected with the same or equally effective physical security as that provided to the source computer, its media, and information contained therein.

(8) Backups must be stored where they are physically secured yet accessible within a reasonable time frame when they are needed in accordance with applicable VA policy.

v. Sanitization. Any VA employee who uses OE to transmit, transport, use or access VAPI must sanitize the OE device to remove the VAPI when the employee is no longer using the device to perform VA work or when the device is not compliant with this Directive. Sanitization must be done in accordance with the most current version of "Fixed Media Sanitization" (see paragraph 4.b.(12) below) and its attachment.

w. Waiver. No waiver to any requirement of this Directive may be granted except by request of an Administration Head, Assistant Secretary or other Key Official to the CIO.

3. RESPONSIBILITIES:

a. VA OCIS. OCIS is responsible for developing appropriate technical standards and guidance for the use of computers and other devices to transport, transmit, access, process and store VA data outside the regular work site. OCIS is also responsible for identifying approved

monitoring mechanisms to confirm compliance with this policy; reviewing remote access technology standards and procedures periodically with security personnel, verifying compliance for Certification and Accreditation; supporting risk management activities associated with business and network operations; acting as the central coordination point and final approval authority for exceptions to this policy; defining or approving acceptable methods of remotely connecting to the VA systems; and providing immediate consultation to VA administrations.

b. VA Chief Information Officer (CIO). The CIO is responsible for assuring Department-wide adherence to current VA network security policies, directives and standards; developing and implementing supporting procedures to confirm conformance with VA network security and remote access policy and standards; operating in a secure manner, commensurate with their security sensitivity, common security services for use by applications and other infrastructure services; examining systems to validate remote access requirements, ensure proper systems configuration, detect unauthorized remote access connections, report violations, and confirm that appropriate security mechanisms and monitoring devices are up to date with best practices and technical standards; supporting risk assessment activities and support technical and security standards for remote access; approving individual requests for remote access based on business requirements, including restrictions and limitations that should be applied; providing operational training for remote access; preparing and providing security and awareness training for all users; defining procedures for remote administration and troubleshooting; maintaining and reviewing an inventory of all remote access users; and maintaining audit logs in accordance with certification and accreditation requirements.

c. All VA Employees. Employees who transport, transmit, access, use, process or store VAPI outside VA facilities (even once) are responsible for requesting and obtaining supervisor and ISO approval for such transport, transmission, access, use, processing or storage; reading and following the remote access security policies; accessing only information systems that use approved hardware, software, solutions, and connections;; taking appropriate measures to protect information, network access, passwords, and equipment; refraining from using automatic password saving features; using extreme caution when accessing VA information in open areas or areas where non-authorized persons may see VA information such as airport lounges and hotel lobbies; protecting VA equipment and information from loss or theft at all times, especially when traveling; exercising good judgment in the use of these resources; complying with current and future standards of acceptable use and conduct at all times; and promptly reporting any misuse of the remote access process observed or possible compromise or loss of VAPI.

d. Information Security Officer (ISOs). ISOs are responsible for coordinating and documenting all requests for remote access within their region, facility or facilities; enforcing all policies and procedures pertaining to transportation, transmission, remote access and use of VA IT equipment; monitoring remote access account usage and ensuring dormant accounts are disabled or removed per this Directive or local policy where more restrictive; ensuring that remote access accounts are immediately disabled for all persons no longer requiring remote access; ensuring that all VA IT equipment used for remote access and VA data storage is immediately retrieved and processed according to policy; and working with the VA-SOC to ensure that remote access to the VA network is done only via approved and appropriately documented methods.

4. REFERENCES

a. Federal Standards

(1) Federal Information Processing Standard (FIPS) 140-2, *Security requirements for Cryptographic Modules*

(2) Draft NIST Special Publication 800-77, *Guide to IPSec VPNs*

(3) NIST Special Publication 800-61, *Computer Incident Handling Guide*

(4) NSA/CSS Manual 130-2, Media Declassification and Destruction, Nov 2003

(5) DoD Hard Disk Sanitizing Guidance, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

b. VA Policies, Directives, and Security Configuration Guidelines

(1) You and Your Password, August 15, 2005

(2) HISD-MDHG-pcAnywhere 11.5 V2.2 (2)

(3) *VA Security Configuration Guideline For Symantec pcAnywhere Version 11.5 Draft Revision 1.1, Feb 28, 2005*

PC AnywhereConfigurationGuidelinev1.1.doc

(4) *VA Security Configuration Guideline For Danware NetOp Remote Control Version 7.6, February 17, 2004 (Contact TIS)*

(5) *VA Security Configuration Guideline For DameWare NT Utilities & DameWare Mini Remote Control, Version 2.1 (Draft), August 20, 2005 (Contact TIS)*

(6) VA Memo, Limitations of the Installation of Modems in Desktop Computers, 15 November 2004

(7) VA Directive 6212, Security of External Electronic Connections

(8) VA Memo, *Unsecure Dialin,* Oct 13, 2000

(9) VA Memo, VPN within the VA Enterprise, July 18, 2003,

(10) *Information Systems Security Incident Reporting VHA Security Policy Procedures Template, Version 1.0, Aug 2004,*

(11) *Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN, 5 May 2005,*

(12) VA Memo, Fixed Media Sanitization, April 20, 2004,

(13) VA Wireless and Handheld Device Security Guideline, Version 3.2, August 15, 2005

(14) VA Handbook 5011/5, Hours of Duty and Leave

5. DEFINITIONS

a. Alternative work location. For the purposes of information security, an "alternate work location" is any place where VA personnel are performing VA work while outside a VA managed facility, or when remote computing is the only means of access (for example, a small department office with only dial-in access). Examples include residences and hotel rooms.

b. Asset. Property of VA or another government agency such as personnel, hardware, software, data and facilities.

c. Availability – making sure that information and vital services are available to users when required.

d. Classification. The assignment of information or an information asset to categories on the basis of the information's need for confidentiality, integrity, and availability.

e. Controllable Environment. Inside VA office buildings and other VA facilities were the security risks have been recognized and control can be exerted on work guidance.

f. Confidentiality. Protecting information from unauthorized disclosure or intelligible interception.

g. Host-based/Personal Firewall. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are used frequently to prevent unauthorized Internet users from accessing private systems or networks connected to the Internet. All messages entering or leaving the remote computer or network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

h. Information Assets. Information, information systems, information services, and information processing resources owned by or entrusted to the VA. Information can exist in several forms (written, verbal, physical, and electronic) and in various states (static or transient).

i. Information Processing Resources. The collection of equipment, software, network connections, and applications and the processes they support to handle data to derive and convey information.

j. Information Security. Protection of information to ensure its Confidentiality, Integrity, and Availability.

k. Integrity – Safeguarding the accuracy and completeness of information and computer software and services.

l. Mobile Computing Device. Any transportable computing or storage device to include personal digital assistants (PDAs), notebooks, desktops, servers, and mobile telephones.

m. OE. Non-VA owned equipment, including employees' personal equipment, commercial equipment (such as hotel and internet café equipment), and equipment owned by other agencies.

n. PAI. Privacy Act Information – information covered by and protected under the Privacy Act of 1974.

o. PDA. Personal Digital Assistant. Describes a class of handheld computing devices (Palm, Pocket PC, etc.) designed to serve the mobile computing needs of individuals. Applications delivered with PDA hardware include email, calendar events, contacts, and PC synchronization.

p. PHI. Protected Health Information. Information protected by the HIPAA Privacy and Security Rules, 45 CFR Parts 160 and 164.

q. PKI. Public Key Infrastructure. PKI is an environment based on the use of digital certificates and public and private key technology to secure communication of information. A fully deployed PKI supports encryption, authentication, privacy, and non-repudiation of information.

r. Remote. An adjective used to describe the use or processing of, or access to, VA information from locations other than sites in VA facilities.

s. Security Incident. An event that has, or could have, resulted in loss or damage to VA assets, or an action that breaches VA security procedures.

t. Telecommuting or Telework. (Performing VA work at a work location other than one directly maintained by the Department, including work done at home. In the context of security, the term applies equally to work performed while traveling on VA business or when at a customer's or vendor's site.

u. Uncontrollable Environment. Locations other than in VA facilities.

v. VA Data or VA Information. All information that is obtained, developed, or produced by or for VA or its employees as part of its business activities.

w. VAPI. VA Protected Information. VA sensitive information, Privacy Act Information (PAI), PHI, or other VA information that has not been deliberately classified as public information for public distribution. VA information that VA would have to release under the Freedom of Information Act is not VA Protected Information. All VA Protected Information should be classified as one of the following: VA Proprietary, VA Restricted, or VA Highly Restricted.

x. VA Sensitive Information. VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6500
Transmittal Sheet
August 4, 2006

INFORMATION SECURITY PROGRAM

1. REASON FOR ISSUE: To replace Department of Veterans Affairs (VA) Directive 6210, Automated Information Systems Security, dated January 30, 1997 with a policy which establishes the criteria for the Department-wide information security program.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive requires Department-wide compliance with the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-3549, and related information security issuances pertaining to the security of VA information and information systems administered by VA, or otherwise under the authority, control, or on behalf of VA. This directive applies to all VA Administrations and staff offices, and pertains to the security of all VA information and information systems, at all levels of sensitivity, and at any location or facility.

3. RESPONSIBLE OFFICE: Office of Cyber and Information Security (005S), Office of the Assistant Secretary for Information and Technology (005).

4. RELATED HANDBOOK: Under development.

5. RESCISSIONS: VA Directive and Handbook 6210, Automated Information Systems Security, dated January 30, 1997.

CERTIFIED BY:

/s/
Robert T. Howard
Senior Advisor to the Deputy Secretary
Supervisor, Office Information and Technology

/s/
R. James Nicholson
Secretary of Veterans Affairs

Distribution: Electronic Only

INFORMATION SECURITY PROGRAM

1. PURPOSE. The purpose of this policy is to establish a program to provide security for VA information and information systems commensurate to the risk of harm, and to communicate the responsibilities of the Secretary, Under Secretaries, Assistant Secretaries, other key officials, the Assistant Secretary for Information and Technology, the Associate Deputy Assistant Secretary (ADAS) for Cyber and Information Security, and the Inspector General (IG) as outlined in the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-3549, which was enacted as part of the E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

2. POLICY

a. The security of VA information and information systems is vital to the success of VA's mission. To that end, VA shall establish and maintain a comprehensive Department-wide information security program to provide for development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems. The VA information security program shall include the following elements:

(1) Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Department.

(2) Policies and procedures that (a) are based on risk assessments, (b) cost-effectively reduce security risks to an acceptable level and, (c) ensure that information security is addressed throughout the life cycle of each Department information system.

(3) Selection and effective implementation of minimum, mandatory technical, operational, and management security controls, or other compensating countermeasures, to protect the confidentiality, integrity, and availability of each Department system and its information.

(4) Subordinate plans for providing adequate security for networks, facilities, systems or groups of information systems, as appropriate.

(5) Annual security awareness training for all VA employees, contractors, and all other users of sensitive VA information and VA information systems which identifies the information security risks associated with their activities and their responsibilities in complying with Department policies and procedures designed to reduce those risks.

(6) Periodic testing and evaluation of the effectiveness of security controls based on risk to include, at a minimum, triennial certification testing of all management, operational, and technical controls, and annual testing of a subset of those controls for each Department system.

(7) A process for planning, developing, implementing, evaluating, and documenting remedial actions to address deficiencies in information security policies, procedures, and practices.

(8) Procedures for detecting, immediately reporting, and responding to security incidents, to include mitigating risks before substantial damage is done as well as notifying and consulting with the US-Computer Emergency Readiness Team in the Department of Homeland Security, law enforcement agencies, the VA IG, and other offices as appropriate.

(9) Plans and procedures to ensure continuity of operations for Department systems.

b. VA shall comply with the provisions of FISMA and other related information security requirements promulgated by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) that define VA information system mandates.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** In accordance with FISMA, the Secretary is responsible for:

(1) Ensuring that VA adopts a Department-wide information security program and otherwise complies with FISMA and other related information security requirements.

(2) Ensuring that information security protections are commensurate with the risk and magnitude of the potential harm to VA information and information systems resulting from unauthorized access, use, disclosure, disruption, modification, or destruction.

(3) Ensuring that information security management processes are integrated with Department strategic and operational planning processes.

(4) Ensuring that Under Secretaries, Assistant Secretaries, and Other Key Officials provide adequate security for the information and information systems under their control.

(5) Ensuring enforcement and compliance with the requirements imposed on VA under FISMA.

(6) Ensuring that VA has trained program and staff office personnel sufficient to assist in complying with all FISMA and other related information security requirements.

(7) Ensuring that the Assistant Secretary for Information and Technology, in coordination with VA Under Secretaries, Assistant Secretaries, and other key officials reports the effectiveness of the VA information security program, including remedial actions, to Congress, OMB, and other entities as required by law and Executive Branch direction.

b. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA Chief Information Officer (CIO), is responsible for:

(1) Establishing, maintaining and monitoring Department-wide information security policies, procedures, control techniques, training and inspection requirements as elements of the VA information security program.

(2) Issuing policies and handbooks to provide direction for implementing the elements of the information security program to all Department organizations.

(3) Approving all policies and procedures that are related to information security for those areas of responsibility that are currently under the management and the oversight of other Department organizations.

(4) Ordering and enforcing Department-wide compliance with and execution of any information security policy.

(5) Establishing minimum mandatory technical, operational, and management information security control requirements for each VA system, consistent with risk, the processes identified in NIST

standards, and the CIO's responsibilities to operate and maintain all Department systems currently creating, processing, collecting, or disseminating data on behalf of VA information owners.

(6) Establishing standards for access to VA information systems by organizations and individual employees, and to deny access as appropriate.

(7) Directing that any incidents of failure to comply with established information security policies be immediately reported to the CIO.

(8) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official for appropriate disciplinary action.

(9) Reporting any compliance failure or policy violation directly to the appropriate Under Secretary, Assistant Secretary, or other key official along with taking the appropriate corrective action.

(10) Requiring any key official who is so notified to report back to the CIO regarding what action is to be taken in response to any compliance failure or policy violation reported by the CIO.

(11) Ensuring VA's facility CIOs and Information Security Officers (ISO) comply with all cyber security directives and mandates, and ensuring that these staff members have all necessary authority and means to direct full compliance with such directives and mandates relating to the acquisition, operation, maintenance, or use of information technology (IT) resources from all facility staff.

(12) Establishing the VA National Rules of Behavior for appropriate use and protection of the information which is used to support VA missions and functions.

(13) Establishing and providing supervision over an effective incident reporting system.

c. **The ADAS for Cyber and Information Security.** In accordance with FISMA, the ADAS for Cyber and Information Security, as VA's Senior ISO, is responsible for carrying out the responsibilities of the Assistant Secretary for Information and Technology under FISMA, as described above.

d. **VA Information Owners**. In accordance with the criteria of the Federated IT Management System, these officials are responsible for:

(1) Providing assistance to the VA CIO regarding the security requirements and appropriate level of security controls for the information system(s) where their information is currently created, collected, processed, disseminated, or subject to disposal.

(2) Determining who has access to the system(s) containing their information, to include types of privileges and access rights.

(3) Ensuring the VA National Rules of Behavior is signed on an annual basis and enforced by all system users to ensure appropriate use and protection of the information which is used to support VA missions and functions.

(4) Assisting the VA CIO in the identification and assessment of the common security controls for systems where their information resides.

(5) Providing assistance to Administration and staff office personnel involved in the development of new systems regarding the appropriate level of security controls for their information.

e. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** In accordance with FISMA, these officials are responsible for:

(1) Implementing the policies, procedures, practices, and other countermeasures identified in the VA information security program that comprise activities that are under their day-to-day operational control or supervision.

(2) Periodically testing and evaluating information security controls that comprise activities that are under their day-to-day operational control or supervision to ensure effective implementation.

(3) Providing a Plan of Action and Milestones (POA&M) to the VA CIO on at least a quarterly basis detailing the status of actions being taken to correct any security compliance failure or policy violation.

(4) Complying with FISMA and other related information security laws and requirements in accordance with the VA CIO orders to execute the appropriate security controls commensurate to responding to a VA Security Operations Center (SOC) security bulletin. Such orders of the VA CIO shall supersede and take priority over all operational tasks and assignments, and shall be complied with immediately.

(5) Ensuring that all employees within their organizations take immediate action to comply with orders from the VA CIO to (a) mitigate the impact of any potential security vulnerability, (b) respond to a security incident, or (c) implement the provisions of a SOC Bulletin or Alert. They shall ensure that their organizational managers have all necessary authority and means to direct full compliance with such orders from the VA CIO.

(6) Ensuring the VA National Rules of Behavior is signed and enforced by all system users to ensure appropriate use and protection of the information which is used to support VA missions and functions on an annual basis.

f. **Users of VA information and information systems.** These individuals are responsible for:

(1) Complying with all Department information security program policies, procedures, and practices.

(2) Attending security awareness training on at least an annual basis.

(3) Reporting all security incidents immediately to the system or facility ISO and their immediate supervisor.

(4) Complying with orders from the VA CIO directing specific activities when a security incident occurs.

(5) Signing an acknowledgement that they have read, understand, and agree to abide by the VA National Rules of Behavior on an annual basis.

g. **The Inspector General**. In accordance with FISMA, the VA IG is responsible for:

(1) Conducting an annual audit of the VA information security program.

(2) Submitting an independent annual report to OMB on the status of VA's information security program, based on the results of the annual audit.

(3) Conducting investigations of complaints and referrals of violations as deemed appropriate by the Inspector General.

4. REFERENCES

a. E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002); to include Title III, the Federal Information Security Management Act (FISMA).

b. Executive Order 12958 – Classified National Security Information, as amended, 68 Fed. Reg. 15315 (Mar. 28, 2003).

c. Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191 through 45 CFR Parts 160, 162 and 164 (2006), the unofficial version.

d. Memorandum from the Secretary of Veterans Affairs: Delegation of Authority and Power to VA CIO for the Establishment and Maintenance of Cyber Security Program, (June 28, 2006).

e. National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a).

f. National Institute of Standards and Technology Computer Security Special Publication Series 800.

g. National Institute of Standards and Technology Federal Information Processing Standards (FIPS).

h. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

i. Request for Advice Relating to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549, VAOPGADV 5-2004 (Apr. 7, 2004).

j. Responsibilities Regarding National Security and Non-National Security Information and Information Systems, VAOPGADV 12-2003 (Aug. 1, 2003).

k. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 17, 2001.

5. DEFINITIONS

a. **Availability.** Ensuring timely and reliable access to and use of information.

b. **Confidentiality.** Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

c. **Control Techniques.** Methods for guiding and controlling the operations of information systems to ensure adherence to FISMA and other related information security requirements.

d. **Federated IT Management System.** The organizational realignment of information technology operational and maintenance functions under the Assistant Secretary for Information and Technology approved by the Secretary of the Department of Veterans Affairs on March 22, 2006.

e. **Information Owner.** An information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal. Information owner responsibilities extend to interconnected systems or groups of interconnected systems.

f. **Information Resources.** Information in any medium or form and its related resources, such as personnel, equipment, funds, and information technology.

g. **Information Security.** Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

h. **Information Security Requirements.** Information security requirements promulgated in accordance with law, or directed by the Secretary of Commerce and NIST, OMB, and, as to national security systems, the President.

i. **Information System.** Discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

j. **Integrity.** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

k. **National Security System.** An information system that is protected at all times by policies and procedures established for the processing, maintenance, use, sharing, dissemination or disposition of information that has been specifically authorized under criteria established by an Act of Congress or Executive Order to be kept classified in the interest of national defense or foreign policy.

l. **Plan of Action and Milestones (POA&M).** A POA&M, which is used as a basis for OMB quarterly reporting requirements, includes the following minimum information: (1) description of the security weakness; (2) identity of the office or organization responsible for resolving the weakness; (3) estimate of resources required to resolve the weakness by fiscal year; (4) scheduled completion date; (5) key milestones with estimated completion dates; (6) any changes to the original key milestone dates; (7) the source which identified the weakness (e.g., CIO audit, OIG audit); and (8) the status of efforts to correct the weakness (e.g., started, ongoing, completed).

m. **Security Incident.** An event that has, or could have, resulted in loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures.

n. **Subordinate Plan.** Also referred to as a system security plan, a subordinate plan defines the security controls that are either planned or implemented for networks, facilities, systems, or groups of systems, as appropriate, within a specific accreditation boundary.

o. **Training.** A learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge.

p. **VA National Rules of Behavior.** A set of Departmental rules that describes the responsibilities and expected behavior of personnel with regard to information system usage.

q. **VA Sensitive Data.** All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation, such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law, harm, or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6210
Transmittal Sheet
January 30, 1997

AUTOMATED INFORMATION SYSTEMS SECURITY

1. **REASON FOR ISSUE:** To revise Department of Veterans Affairs (VA) automated information systems (AIS) security policy, formerly contained in VA Manual MP-6, Part I, Chapter 2. This directive implements recommendations of VA's Security Working Group (SWG).

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive sets forth policies and responsibilities for protecting AIS and telecommunications resources from unauthorized access, disclosure, modification, destruction or misuse. The directive contains:

a. Identification of eight primary elements applicable throughout the Department and to the security of all automated information collected, transmitted, used, processed, stored, or disposed of, by or under the direction of VA or its contractors, or other government agencies under computer matching.

b. Responsibilities for implementing and managing the AIS security program.

c. References related to AIS security.

3. **RESPONSIBLE OFFICE:** The Associate Deputy Assistant Secretary for Information Resources Management Policy & Program Assistance (045A), Office of the Deputy Assistant Secretary for Information Resources Management.

4. **RELATED HANDBOOK:** VA Handbook 6210, Automated Information Systems Security Procedures.

5. **RESCISSIONS:** MP-6, Part I, Chapter 2, Change 18, dated February 24, 1992.

CERTIFIED BY:

Nada D. Harris
Deputy Assistant Secretary for
Information Resources Management

BY DIRECTION OF THE SECRETARY
OF VETERANS AFFAIRS:

Dr. Mark Catlett
Assistant Secretary for
Management

Distribution: RPC: 6500
FD

AUTOMATED INFORMATION SYSTEMS SECURITY

1. PURPOSE

a. This directive establishes policy and responsibilities for the security of automated information systems (AIS) within the Department of Veterans Affairs (VA). The Department-wide program is designed to protect all AIS and telecommunications resources from unauthorized access, disclosure, modification, destruction, or misuse. These provisions comply with Federal AIS security laws and regulations, including the Computer Security Act of 1987 (PL 100-235), and the requirements of Office of Management and Budget (OMB) Circular A-130 and its appendices.

b. The provisions of this directive are applicable throughout the Department, and to the security of all automated information collected, transmitted, used, processed, stored, or disposed of, by or under the direction of VA or its contractors, or other government agencies under computer matching. Computer matching is defined in 5 U.S.C. Section 552a (a) (8).

2. POLICY

a. VA shall establish, maintain, and enforce a comprehensive security program to assure an adequate level of security protection for all AIS, whether maintained in-house or by a contractor on behalf of, or for the benefit of the Department. Specifically, VA shall assure that AIS operate effectively and accurately, using appropriate technical, personnel, administrative, environmental, and telecommunications safeguards. VA will maintain the continuity of operations of AIS supporting critical Department functions.

b. Administration heads, Assistant Secretaries, and other key officials shall develop, implement, maintain, and enforce a structured program to safeguard all AIS assets for which they are responsible. The AIS security program will be designed to ensure the continued operation of mission-critical activities and will implement measures to prevent unauthorized access to and use of automation and telecommunications resources.

c. Responsible program offices will perform reviews and certifications of AIS at least every three years. They shall evaluate the adequacy and proper functioning of security safeguards and shall identify vulnerabilities that could heighten threats to sensitive data or valuable resources. Security or other control weaknesses shall be included in the Federal Managers Financial Integrity Act Report, an annual internal control report, required by OMB Circular A-123.

d. The VA AIS security program shall, at a minimum, include the following components:

(1) Computer Systems Security

(a) A management control process shall be established to assure that appropriate safeguards are incorporated into new or redesigned AIS applications. Principal users of AIS applications shall evaluate and determine the data protection requirements for new applications and for existing AIS applications that are undergoing substantial modifications. For those applications considered sensitive, the management control process shall, at a minimum, include sensitive systems security plans, security specifications, design reviews, and systems tests. These requirements are detailed in OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, and in OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. The life cycle documentation requirements of the sensitive system shall be consistent with the requirements outlined in the document "Model Framework for Management Control over AIS."

(b) Department components shall comply with VA Directive 0710, Security, for the determination of position sensitivity designations, risk levels and necessary screening of both Federal and contractor personnel.

(c) Responsibility for the security of each office or facility and its computer systems (personal computers, local area networks, mini and mainframe computers, associated equipment, and the automated information) shall be assigned. The responsible official shall assign information security duties to personnel who do not have management or operational responsibility for the AIS, but who do possess expertise in information resources management and security matters.

(d) Sensitivity analysis of the data in VA records and information systems is the responsibility of the organizational element that develops the data, system of records, or other information to accomplish its mission or purpose. The information owner determines the sensitivity of information and the appropriate protection to be afforded, as well as who is authorized access and what functions persons granted access are permitted to perform. The owner of information requiring protection authorizes its release to users, establishes requirements for protection, and endorses the level of protection provided by information custodians. In determining the appropriate level of sensitivity and the degree of protection required, information owners should consider the specific criteria presented below and the systems of which the information is a part. Some information is not sensitive by itself, but becomes sensitive when combined with other information. Therefore, sensitivity determinations should be made on the basis of judgment that weighs various factors including, but not limited to, the following:

1. The nature of the information being processed or transmitted.

2. The degree of access control and physical protection in effect.

3. The degree to which information IS accessible by remote terminals, other systems or networks.

4. The extent to which violations or attempted violations are detectable.

5. The extent to which backup is available.

(e) Each responsible security official shall oversee the general assessment of risks and take actions to manage them to ensure that safeguards are incorporated into existing facilities, new facilities and their computer systems. These analyses should be risk-based and take into account the size and sensitivity of the system or facility. The results of these analyses shall be maintained in a report at the facility. The assessment results will be considered when certifying applications processed at the facility and on these systems according to the standards recommended in FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, and when evaluating controls over facility and system management in accordance with OMB Circular A-123, Internal Control Systems. The major factors in this risk management determination are: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Risk assessments should be performed:

1. Prior to the approval of design specifications for new facilities or the acquisition of new computer systems.

2. Whenever there is a significant change to the facility or its computer systems.

2. A minimum frequency of once every three years

(f) Disaster recovery and continuity of operations plans shall be maintained for each facility and computer system. These plans are required to be documented for

computer systems which support essential Department functions and must be fully documented and operationally tested periodically.

(g) Appropriate technical, administrative, physical, and personnel security requirements shall be included in all specifications for the acquisition, operation or maintenance of facilities, equipment, software, and related services, whether procured through VA, General Services Administration (GSA), or another agency. The management official responsible for security at the facility making the acquisition will review and approve these security requirements.

(h) Removal of sensitive information on automatic data processing equipment (ADPE) storage media shall be conducted prior to disposal of the equipment. VA shall ensure that all offices and facilities include policy and procedures in their computer security programs for the protection of sensitive information during the disposal of ADPE storage media. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 6.

(i) Computer virus and malicious computer program code prevention, detection and elimination policies and procedures shall be developed and implemented by VA program and staff offices. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 4.

(j) Electronic mail and information messaging applications and systems shall only be used for authorized government purposes and shall contain only non-sensitive information unless the data, and accompanying passwords or other authentication mechanisms, are protected with an approved encryption algorithm. Electronic mail systems provide the means for communicating information (excluding voice) by sending, storing, processing, and retrieving the information. This allows users to communicate under specified conditions. Electronic message systems (e.g., Personal Computer Telecommunications System)are electronic mail systems that incorporate the additional feature where the central facility assumes active responsibility for delivering the message to the intended addressee rather than the passive role an electronic mail system, which delivers messages in response to a request by an addressee. This policy does not cover privacy and confidentiality issues of records in automated information systems; refer to Records and Information Management Handbook 6300.1 for records management policy and procedures. VA Directive 6301, Electronic Mail Records, establishes the policies and responsibilities for managing the creation, maintenance, use, and disposition of federal records created or received in electronic mail applications.

(2) Network Security. Proper safeguards shall be implemented on VA communication networks that transport or provide acclass to sensitive information. VA security requirements must be satisfied before full access to the Internet system is granted through VA ADPE. VA Directive 6102, VA Internet Policy, and Appendix A, governs VA access to the Internet system and specifies the minimum security requirements for establishing Internet gateway connectisons. Sensitive information transported over VA wide area data communications networks shall be protected by a NIST-approved (National Institute of Standards and Technology) encryption method. Procedures necessary to comply with the policies in this section, including mandatory features to be implemented in VA networks or interfaces to VA networks, are found in VA Directive 6100, Telecommunications and related handbook. Required security procedures for establishing, operating, or connecting to a local area network (LAN) are found in VA Handbook 6210, Chapter 7.

(3) Security Awareness and Training. A program shall be established to assure that Department and contractor personnel are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnsrabilities of such systems and trained in techniques to enhance security. Each employee shall attend an initial AIS security awareness training before accessing VA systems and receive other AIS security training on an annual basis; this attendance shall be documented and placed in their official personnel file. As part of an initial security training course or instruction, rules of behavior for systems shall be included that specify limits on interconnections to other systems, consequences of behavior not consistent with

system rules and basic computer security principles. Specific security training as prescribed in FPM Bulletin No. 410-131, Training Requirement for the Computer Security Act, dated January 1, 1992 shall be conducted for all VA employees and contractors as described in VA Handbook 6210, Chapter 2. The Department Information Resources Security Officer (IRSO) shall develop and issue basic computer security principles to each VA organization to include in their security awareness and training.

(4) Security Incident Reporting. VA shall establish, maintain, and enforce an AIS security incident reporting and response capability to ensure that computer security incidents are detected, reported, and corrected at the earliest possible time. The incident reporting and response process shall be designed to detect and respond to AIS security incidents as they occur, assist in preventing future incidents from occurring through awareness, contain necessary response mechanisms to deal with incidents, and support security controls and procedures. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 3.

(5) Copyright. All VA employees shall ensure that government-acquired commercial software is used only in accordance with licensing agreements. It is the responsibility of management and individual employees to ensure that proprietary software is properly licensed before being installed on VA equipment. VA facilities and organizations should consider acquiring special purpose software to perform software audits on each PC in the facility or organization. This policy does not apply to software developed by or specifically for the use of the Department. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 5.

(6) Contingency Planning. AIS contingency plans shall be the responsibility of end users, where applications computing is performed or directly used by the users. The plans shall be developed and maintained by the end user or a designated vendor or contractor approved by the end user This responsibility extends to individual personal computer (PC) usage by or on behalf of VA. Contingency plans are an integral part of business resumption planning which is the facility's or organization's plan to resume business or services. Contingency plans for applications and systems, when maintained at a VA automation center, are the joint responsibility of the VA program office responsible for the system, or a designated group within the responsible program office, and the VA facility. Such plans shall be consistent with disaster recovery and continuity of operations plans maintained by the facility at which the application is processed. Procedures for implementing the policies in this directive are found in VA Handbook 6210, Chapter 1.

(7) Physical Security. Policies and procedures shall be developed and implemented by VA program and staff offices which require the application of physical devices and control measures to safeguard information assets and sensitive information. Federal Information Processing Standards (FIPS) Publication 31, establishes guidelines for automated data processing physical security and risk management.

(8) Access Control to Employee Records. Employee records, in hard copy or automated forms, are sensitive records and must be afforded the same protection as veterans' records. VA employees are entitled to review the information contained in their own medical, benefits, or other records maintained in VA automated systems. In accordance with the Privacy Act of 11974, this access request must be authorized and follow a "reasonable" procedure for disclosure of employee record information. This process shall include a requirement that the employee seeking access to his/her record notify, in writing, the organizational official responsible for release of Privacy Act-covered information prior to accessing the record. This authorization process shall be supplemented by the requirement for the creation of an audit trail of access to sensitive records. This prior notification requirement does not pertain to applications such as IFCAP, Leave Balance and Service Record Screen options, where the record owner (an employee) is the primary source of input to the

application. Except for these "self-service" input systems, employees shall be granted "read-only" access.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** Yhe Secretary has designated the Chief Information Officer (CIO) as the senior agency official responsible for the Department's IRM program.

b. **Chief Information Officer.** The VA CIO will, through the Deputy Assistant Secretary for Information Resources Management (DAS/IRM):

(1) Implement the Computer Security Act of 1987, OMB Bulletins related to that Act, OMB Circulars A-123 and A-130, and their appendices, and other directives issued by the National Institute of Standards and Technology, General Services Administration, or the National Telecommunications and Information Security Committee.

(2) Develop and issue VA AIS security policies and regulations.

(3) Ensure that appropriate criticality and sensitivity levels and controls for selection and protection of information processed or handled by the Department are identified.

(4) Periodically review new and ongoing IRM projects and computer information systems throughout the Department to assess their compliance with the provisions of this directive, and ensure that AIS security requirements are incorporated in VA-developed or acquired hardware, system:; and applications software, and VA-wide telecommunications networks.

(5) Designate an Information Resources Security Officer (IRSO) for the Department.

c. **The Inspector General.** This Office is responsible for:

(1) Conducting and supervising information security audits and providing follow-up regarding progress in implementing security enhancement and corrective actions.

(2) Conducting or providing oversight for criminal investigations as appropriate.

(3) Developing composite analyses of risk assessments conducted as part of the Department security program, identifying patterns of weaknesses, and recommending preventive measures and improvements.

d. **The Deputy Assistant Secretary for Security and Law Enforcement.** This Office is responsible for:

(1) Developing and implementing Department-wide policy regarding position sensitivity and its applicability to all national security/public trust positions

(2) Processing requests for security clearances for personnel designated to national security/public trust positions.

(3) Implementing the Department Personnel Security Program.

(4) Providing/issuing policy, operating procedures, and technical standards for the protection of classified national security information.

(5) VA Emergency Preparedness Program as it involves VA's Information Security Programs.

(6) Developing and implementing Department-wide policy regarding physical security at all VA facilities.

e. The General Counsel. This Office is responsible for:

(1) Interpreting laws, regulations, and directives applicable to VA AIS security activities.

(2) Rendering legal advice and services in the area of AIS security upon request of Administration Heads, Assistant Secretaries, and other key officials.

f. Deputy Assistant Secretary for Human Resources Management. This Office is responsible for:

(1) Developing and recommending VA-wide policy related to personnel suitability.

(2) Interpreting Federal suitability policy.

(3) Recommending and advising on retention, reassignment, adverse or other actions against individuals for violation of security policies, including coordination with the Office of the Inspector General.

g. Administration Heads, Assistant Secretaries, and Other Key Officials. These Offices are responsible for:

(1) Safeguarding AIS assets under their control, including those shared with or operated by other VA organizations, other Federal agencies, contractors, or State or local governments.

(2) Appointing an Information Security Officer (ISO) and alternate for their organization.

(3) Allocating sufficient funds, personnel, and management support to implement the provisions of this directive, and assure compliance with Federal and VA AIS security requirements.

(4) Ensuring that the designated ISO reports major violations of AIS security policies, procedures, and practices to the VA IRSO.

(5) Ensuring that personnel within their organizations attend AIS security orientation and functional training, in accordance with Department policy and OPM regulation. Ensuring that all personnel within their organizations attend initial security training before they are granted access to VA systems, and at least once each year thereafter.

(6) Implementing security plans for general support systems and major applications as required by OMB Circulrir A-130, Appendix III.

(7) Ensuring that AIS security policies and procedures are developed and periodically updated, and that contingency plans are developed, tested, and periodically certified as accurate and current.

(8) Ensuring that a security certification review is made of operational sensitive systems, or those under development to determine adequacy of controls and security safeguards. The review should follow provisions of OMB Circular A-130, Appendix III.

(9) Ensuring that risk analyses are performed and security plans developed for projects involving development of new systems, acquisitions of equipment or services, and preparation of Requests for Proposals (RFPs) and other procurement documents which must specify AIS security requirements, activities and related deliverables.

4. **REFERENCES**

a. Computer Security Act of 1987, EL 100-235, 101 Stat. 1724.

b. Electronic Communications Privacy Act of 1986, Public Law 99-08. 100 Stat. 1848.

c. Executive Order 10450 Security Requirements for Government Employment.

d. FIPS PUB (Federal Information Processing Standards Publication) 1-1-3 Guideline: American National Dictionary For Information Systems.

e. FIPS PUB 31, Guidelines for Automated Data Processing Physical Security and Risk Management.

f. FIPS PUB 39, Glossary for Computer Systems Security.

FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 197::

h. FIPS PUB 46-1. Data Encryption Standard (DES).

1. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification

j. FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis.

k. FIPS PUB 73, Guidelines for Security of Computer Applications, dated June 30, 1980.

1. FIPS PUB 81, DES Modes of Operation.

m. FIPS PUB 83, Guidelines on User Authentication Techniques for Computer Network Access Control, dated September 29, 1980.

n. FIPS PUB 87, Guidelines for ADP Contingency Planning.

o. FIPS PUB 88, Guidelines on Integrity Assurance and Control in Database Administration, dated August 4, 1981.

p. FIPS PUB 102, Guidelines for Computer Security Certification and Accreditation, dated September 27, 1983.

9. FIPS PUB 112, Password Usage, dated May 30, 1985.

r. FIPS PUB 113, Computer Data Authentication, dated May 30, 1985.

s. Model Framework for Management Control over Automated Information Systems, January 1988; President's Council on Integrity and Efficiency and President's Council on Management Improvement.

t. MP-I, Part II, Chapter 13, Emergency Preparedness Planning (VA Directive 0320).

u. NISTIR 4659, Glossary of Computer Security Technology.

v. NISTIR 5153, Minimum Security Requirements for Multi-User Operating Systems.

w. OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain ljensitive Information, July 9, 1990.

x. OMB Circular A-130, Management of Federal Information Resources, particularly Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

y. OMB Circular A-123 Revised, Internal Control Systems, August 4, 1986.

z. OMB Privacy Act Implementation Guidelines, and Responsibilities published at Federal Register Vol. 40, Pages 28948-28978, July 9, 1975.

aa. OMB 1975 Privacy Act Supplementary Guidance published at Federal Register Vol. 40, pages 56741-56743, December 4, 1975.

bb. VA Directive and Handbook 0710, Security.

cc. VA Directive 6301, Electronic Mail Records.

dd. 5 CFR Parts 731, 732, and 736.

ee. 36 CFR Part 1234, Electronic Records Management, 60 Fed. Reg. 44634 (1995).

ff. 41 CFR (Code of Federal Regulations) Chapter 201, Federal Information Resources Management Regulation (FIRMR).

gg. 5 U.S.C. 552, Freedom of Information Act.

hh. 5 U.S.C. 552a, Privacy Act of 1974.

ii. 18 U.S.C. 1029-1030, Fraud and Related Activity in Connection with Access Devices and Computers.

jj. 38 U.S.C. 5701, Confidential Nature of Claims.

kk. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records.

ll. 38 U.S.C. 7332, Confidentiality of Certain Medical Records.

Department of Veterans Affairs

VA Handbook 6210

Washington, DC 20420

Transmittal Sheet

JANUARY 30, 1997

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PROCEDURES

1. REASON FOR ISSUE: This handbook establishes procedures and practices for AIS security programs at all organizational levels of the Department of Veterans Affairs. It implements the policies contained in VA Directive 6210, Automated Information Systems Security.

2. SUMMARY OF CONTENT/MAJOR CHANGES

a. The Automated Information Systems (AIS) Security Procedures Handbook provides the general procedures and guidelines to implement the policies contained in VA Directive 6210, Automated Information Systems Security.

b. Provides guidance on key AIS security topics, such as business resumption and contingency planning, computer security training, security incident reporting, viruses, copyright, information stored on automatic data processing equipment during disposal, and local area network security.

c. Provides a comprehensive reference document addressing the minimum security standards required to guide the conduct of VA Administrations' and Staff Offices' activities directed toward their AIS program.

d. Consistent with the requirements of OMB Circular No. A-130, Appendix III, dated February 8, 1996, the Amendments to the Computer Security Act of 1987, (PL 100-235) and OMB Bulletin No. 90-08, dated July 9, 1990.

3. RESPONSIBLE OFFICE: The Office of the Associate Deputy Assistant Secretary for Policy and Program Assistance (045A), Office of the Deputy Assistant Secretary for Information Resources Management.

4. RELATED DIRECTIVE: VA Directive 6210, Automated Information Systems Security.

5. RESCISSION: MP-6, Part I, Chapter 2, Change 18, dated February 24, 1992.

CERTIFIED BY: BY DIRECTION OF THE SECRETARY

OF VETERANS AFFAIRS:

Nada D. Harris D. Mark Catlett

Deputy Assistant Secretary for Assistant Secretary for Management

Information Resources Management

Distribution: RPC: 6500

FD

CONTENTS

CHAPTER 4. VIRUS CONTROL PROCEDURES

PARAGRAPH

CHAPTER 5. COPYRIGHT SECURITY PROCEDURES

PARAGRAPH PAGE

CHAPTER 6. PROCEDURES FOR SAFEGUARDING SENSITIVE INFORMATION STORED ON AUTOMATIC DATA PROCESSING EQUIPMENT DURING DISPOSAL

PARAGRAPH

CHAPTER 7. LOCAL AREA NETWORK SECURITY PROCEDURES

PARAGRAPH

AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PROCEDURES

CHAPTER 1. BUSINESS RESUMPTION AND CONTINGENCY PLANNING PROCEDURES

1. PURPOSE and SCOPE. This chapter establishes mandatory operational requirements for business resumption and contingency planning within the Department of Veterans Affairs. It is designed to provide Department-wide guidance to VA Administrations and Staff Offices in responding to catastrophic events involving VA facilities and information technology service interruptions.

2. BACKGROUND. Traditionally, contingency planning has focused on restoring information technology services for an automation center, wide area network or similar service. While remote sites are still accessed for processing and storing information, most VA facilities including: VACO, regional offices, and medical centers, have their own local area networks which link the various personal computers and share various resources. If a catastrophic event occurs that makes it impossible for VA employees to use that site, the re-establishment of information systems and network functions is only one part of the resumption of services for a facility. The critical functions of that facility must be restored and an interim process must be put into action. "Hot sites" (a reserved space already equipped with processing capability and other services), reciprocal agreements, and other arrangements to provide restored services to their end users should be considered. Critical files that were processed previously on Local Area Network servers need to be restored so they can be used in processing during the contingency period. In summary, both the information technology and the general office environment have to be restored.

3. RESPONSIBILITIES

a. The VA Chief Information Officer (CIO) is charged with ensuring that a business resumption plan is developed at all VACO locations. This includes the necessary contingency plans for critical automated information systems. The CIO is also responsible for monitoring, reviewing, and evaluating compliance with this automated information system (AIS) security program directive. These responsibilities are redelegated to the VA Information Resources Security Officer (IRSO) for execution.

b. Administration heads, Assistant Secretaries, Deputy Assistant Secretaries and other key officials are responsible for ensuring that offices and facilities under their control can operate despite disruptions. These offices and facilities must include business resumption and contingency planning as vital considerations in their

computer security programs in protecting sensitive information in VA automated information systems.

c. The director of each VA field station is responsible for the development, periodic testing and updating of a business resumption plan for that field station and contingency plans for all general support systems located at that field station.

1. **PROCEDURES.** The following procedures outline the steps to be followed in the

development and implementation of an effective business resumption and contingency plan for VA organizations and facilities. A recommended resource to use in the organizing, developing, testing, and implementing a contingency plan is VHA's "VA Medical Center Contingency Planning Boilerplate." This document provides a blueprint for the creation of contingency plan policies and procedures; it also includes sample forms used to document each step. Additional information concerning this contingency planning outline may be obtained by contacting the Medical

Information Security Service at the National Center for Information Security, at VAMC Martinsburg, WV.

a. **Identify Mission Critical Functions**. The first step of business resumption planning is to identify mission critical functions and determine their priorities. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set and approved by senior management, it will be easier for the organization to recover from the disaster and resume normal operations. Contingency plans shall be consistent with other site and building emergency plans. All plans designed to continue essential VA missions and functions must be coordinated with each other and recognize the dependent nature of this process.

b. **Identify the Resources that Support Critical Functions**. After mission critical functions are identified, the resources to support the critical functions must be identified, determine the time frames in which each resource is used (some are needed daily and others are used only once a month), and to determine the effect on the mission if the resource is not available. One method used to identify mission-critical functions and their impact is called Business Impact Analysis. It includes a review of the site's functions to understand the impact if they are not performed. A review is done of each function regarding its impact on operations, end users, interrelationships with other critical functions, as well as time lines and considering workload peaks and valleys. Also considered are additional expenses caused by overtime, the need for temporary employees and other costs associated with recovery. Finally, the effect of not performing a mission critical function needs to be examined and considered with regard to its impact within the organization, externally, and in the media.

c. **Anticipating Potential Contingencies or Disasters**. All resources associated with critical functions should be examined with likely problem scenarios. Various types and sizes of contingencies should be considered. To better understand resource needs and their support of

critical functions, a contingency planning team should be formed. Team members should include representatives from three main areas: functional/business groups, facilities management, and technology management. Legal advisors and other specialty groups can be assigned as needed to the team. This assignment should not preclude members of these groups from serving in other planning roles. Members from these areas may include financial management, personnel, computer security, and physical security. The team should identify likely problems by using analytical tools, such as existing risk assessment methodologies (e.g., qualitative and quantitative, outlined in FIPS Publication 65), and risk assessment software packages. A Department reference on the assessment of risk is found in VHA Manual, M-11, Information Resources Management, Chapter 16.

d. **Selecting Business Resumption and Contingency Planning Strategies.** The primary purpose of this step is to plan how to recover needed resources. Alternative strategies should be evaluated to consider what controls are in place to prevent and minimize contingencies.

(1) A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. Emergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps that are taken to continue support for critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode.

(2) The selection of a strategy needs to be based on practical considerations as feasibility and cost Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. Questions to be asked are: Is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of loosing electrical power for various lengths of time? Are the consequences of loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is not clear which strategy is the best. In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions. The different categories of resources should each be considered. Some of these factors include: human resources, processing capability, automated applications and data, computer-based services, physical infrastructure, documents and papers.

(a) **Implementation**

(1) Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be re-negotiated to add contingency services. Another preparation may be to purchase equipment, to support a redundant capability.

(2) Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used to restore files after a personal computer virus corrupts the data or after a hurricane destroys an automation center. System backups must be tested on a regular basis to ensure that data can be read from the disks in the event they are needed in an emergency.

(3) It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and backup services and redundant equipment should also be kept current. Contracts and agreements also need to reflect any changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or obsolete to an organization's architecture.

(4) Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were also members of the contingency planning team.

(5) There are many important implementation issues for an organization to consider. Two of the most important are 1) how many plans should be developed and 2) who will prepare each plan. The answer will depend on the organization's overall strategy for contingency planning, and should be documented in the organization's policy and procedures document.

(6) For small or less complex systems, the contingency plan may be a part of the computer security plan. For larger complex systems, the computer security plan could contain a brief synopsis of the contingency plan, which should be a separate document. The purpose of the computer security plan is to provide a basic overview of the security and privacy requirements for a computer system and the responsible VA component's plan for meeting those requirements. It also serves as documentation of the process of planning adequate, cost-effective security protection for a system. The purpose of the contingency plan is to document the specific methodology, structure, discipline, and procedures to be used for emergency response, backup operations, and post-disaster recovery maintained by the responsible VA office as part of its AIS security program. This planning will help ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

(7) Some organizations have one plan for the entire organization; others have a plan for each distinct computer system, application, or other resource. Other approaches recommend a plan for each business or mission function, with separate plans, as needed, for critical resources.

(8) The number of actual plans needed depends upon the unique circumstances for each organization. Coordination and cooperation between resource managers and functional managers responsible for the mission or business is critical to the success of any plan.

(b) **Documentation**. The contingency plan needs to be: documented, kept up-to-date as the personnel responsible for implementation of the contingency plan and other factors change. A written plan is essential

to have during a contingency situation. It should clearly state in simple language sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge can immediately begin to execute the plan. It is important to store, in a secure environment, up-to-date copies, including one in electronic format, of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities. Each member of the contingency plan response team should have copies of the plan.

(c) **Training**. All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization. Refresher training may be needed and personnel need to practice their skills. Training is particularly important for effective employee response during emergencies. Depending on the nature of the emergency, there may be inadequate time to check a manual to determine correct procedures to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.

e. **Testing and Revising**

(1) A contingency plan should be tested periodically to identify and correct any problems in implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organizations and among systems. There are several types of testing, including reviews, analyses, and simulations of disasters.

(a) A review can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organization and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organizational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

(b) An analysis may be performed on the entire plan or portions of it, such as emergency response procedures. It is more beneficial if the analysis is performed by a member of the facility staff who did not participate in the development of the contingency plan, but has a sound knowledge of the critical functions and supporting resources. This person may also interview functional managers, resource managers, and their staff to uncover missing or unworkable sections of the plan.

(c) Organizations may also arrange disaster simulations. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.

(2) The results of a "test" often imply a grade assigned for a specific level of performance, or simply pass or fail. However, in the case of contingency planning, a test should be used to improve the plan. If organizations do not use this approach, flaws in the plan may remain undetected and not corrected.

f. **Interdependencies**. Controls can prevent or reduce the effects of a disaster at the facility. Ideally, controls mutually support and compliment each other. In combination, they eliminate or lessen the damage occurring as a result of the destruction, disclosure, or denial of service to critical resources.

(1) Risk assessment provides a tool (process) for analyzing the security costs and benefits of various contingency planning options. In addition, a risk assessment effort can be used to help identify critical resources needed to support the organization and the likely threat to those resources. It is not necessary, however, to perform a risk assessment prior to contingency planning, since the identification of critical resources can be performed during the contingency planning process itself.

(2) Physical and environmental controls help prevent the destruction of automated information systems, although many of the other controls, such as logical access controls, also prevent damage. The main threats that a contingency plan address are physical such as: fires; loss of power; plumbing breaks; and natural disasters.

(3) Incident handling can be viewed as a subset of contingency planning. It is the emergency response capability for various technical threats. Incident handling can also help an organization prevent future incidents by recording the incident and educating personnel about the incident, the circumstances, and the corrective action taken.

(4) Support and operations in most organizations include the periodic backing up of critical files. It also includes the prevention and recovery from more common contingencies, such as a disk failure or corrupted data files.

(5) Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities.

g. **Cost Considerations**. The cost of developing and implementing contingency planning strategies should be taken into account and, when included in the strategy, additional expenses for contracting backup services or duplicate equipment. One contingency cost that is often overlooked is the cost of testing a plan. Testing provides many benefits and should be performed, although some of the less expensive methods (such as a review) may be sufficient for less critical resources.

5. REFERENCES

a. National Institute of Standards and Technology, Guidelines for ADP Contingency Planning, FIPS Pub 87; 1981.

b. VA Directive 0320, Emergency Preparedness Planning.

CHAPTER 2. COMPUTER SECURITY TRAINING PROCEDURES

1. PURPOSE. Computer security training requirements shall be developed and conducted for all VA employees involved with the management, use or operation of each VA computer system which contains sensitive data. The procedures and responsibilities described in this handbook apply to all VA elements and to non-VA organizations that use VA computer systems, including contractors performing work for VA. Each organization is responsible for conducting annual AIS security training to raise the level of AIS security in VA. This Chapter focuses on the provision for development and implementation of a security awareness and training program for VA.

2. BACKGROUND. The Computer Security Act of 1987 was signed and became Public Law 100-235 on January 8, 1988. The Act strengthens the role and responsibility of the National Institute of Standards and Technology for the development and promulgation of computer security. The Act places emphasis on three major provisions:

(1) Identifying computer systems containing sensitive information;

(2) Developing security plans for those sensitive systems;

(3) Mandating computer security training for all users of sensitive Federal computer systems.

3. RESPONSIBILITIES

a. The Secretary of Veterans Affairs is responsible for AIS security in VA.

b. The VA CIO is responsible for implementing the Computer Security Act of 1987 and related OPM regulations through the VA's automated information systems security program. The CIO will ensure that computer security training and awareness are basic elements of the VA's AIS security program.

c. The Information Resources Security officer (IRSO) for VA, is responsible for:

(1) Ensuring that appropriate Department policy complies with the computer security training requirements of the Computer Security Act of 1987 and related implementing regulations.

(2) Developing and issuing procedures for VA components' use to organize and conduct computer security and awareness training for all employees.

d. Administration Heads, Assistant Secretaries, and other key officials are responsible for establishing an automated information systems security program that includes security training and awareness for all employees in accordance with VA policy and OPM regulations.

e. Facility directors are responsible for establishing AIS security and awareness training in their AIS security program as prescribed in VA Directive 6210 and VA organizational directives and procedures.

f. Managers and immediate supervisors are responsible for ensuring that all facility personnel attend formal AIS security and awareness training according to facility policy and procedures.

g. All VA employees, contractors, and other individuals using AIS resources are responsible for attending specifically assigned AIS security and awareness training.

4. PROCEDURES

a. Presented in this Chapter are training guidelines and requirements for computer security. Each organization should develop and issue specific guidelines for all users to effectively implement policy with regard to AIS security awareness and training within VA. The training should be designed to enhance employees' awareness of the threats to and vulnerability of computer systems and encourage the use of improved security practices. Due to the sensitive nature of certain positions, VA organizations should ensure that personnel in positions designated as "security officer, system administrator and in contractor positions" receive the appropriate AIS security training.

b. The VA standard for developing and conducting AIS security awareness and training for VA employees shall be the National Institute of Standards and Technology's (NIST) Special Publication 500-172, Computer Security Training Guidelines, and OMB Circular A-130, Appendix III, dated Feb. 8, 1996.

c. Personnel making use of automated information systems shall be aware of the vulnerabilities of such systems and trained in techniques to enhance security. Employees shall complete an initial AIS security training session prior to gaining access to a VA automated information system. This training may be held as part of orientation that new employees normally attend. Attendance shall be documented and placed in their official personnel file. Each administration and staff office is responsible for developing, implementing and maintaining a structured security program to include application security, personnel security, facility security and security awareness and training.

d. In compliance with 5 CFR, Part 930, Training Requirement for the Computer Security Act, all VA employees, including contractors, are to receive initial security training at orientation, and shall receive annual training in the following five content areas:

(1) **Computer Security Basics**. An introduction to the basic concepts of computer security practices and the importance of the need to protect the information from vulnerabilities to known threats.

(2) **Security Planning and Management**. Training which focuses on the policy level issues of AIS security and involves decision-making on the organization of the security program, security planning, and risk management process.

(3) **Computer Security Policy and Procedures**. Training which examines government-wide and Department specific security practices in the areas of physical, personnel, software, communications, data, and administrative security.

(4) **Contingency Planning**. Training covers the concepts of all aspects of contingency planning, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all employees involved.

(5) **System Life Cycle Management**. Training explains how security is addressed during each phase of a systems life cycle, which consists of system design, development, test and evaluation, implementation and maintenance. It also addresses procurement, certification, and accreditation.

e. VA employee training is divided into the following categories:

(1) **Executives**. Those senior managers who are responsible for setting Department computer security policy, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the resources and support for the computer security program.

(2) **Program/Functional Managers**. Those managers and supervisors who have a program or functional responsibility (not in computer security) within the Department. They have primary responsibility for the security of their data and are responsible for designating the sensitivity and criticality of data and processes, assessing the risks to the data, and identifying security requirements to the supporting data processing organization, physical security staff, physical facilities personnel, and users of their data. Functional managers are responsible for assuring the adequacy of all contingency plans relating to the safety and availability of their data.

(3) **IRM, Security and Audit Personnel**. Personnel involved with the day-to-day management of the Department's information resources, including the accuracy, availability, and safety of these resources. Each organization assigns responsibility differently, but as a group these persons issue procedures, guidelines, and standards to implement the Departmental or component policy for information security to monitor its effectiveness and efficiency. They provide technical assistance to

users, functional managers, and to the data processing organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

(4) **AIS Management, Operations and Programming Staff**. Personnel involved with the daily management and operations of the automated data processing services. They provide for the protection of data in their custody and identify to the data owners what those security measures are. The group includes: computer operators, schedulers, tape librarians, database administrators, and systems and applications developers. They provide the technical expertise for implementing security-related controls within the automated environment, and have primary responsibility for all aspects of contingency planning.

(5) **(End) Users**. Any employee or other customer who has access to a Department computer system that processes sensitive or non-sensitive information. This is the largest and most heterogeneous group of employees. It consists of everyone from the data entry clerk who has a personal computer with sensitive information to the executive.

f. These groupings are based on the need for employees within a given category to know or be able to perform the same or similar types of tasks. Each organization will determine specific training needs and categories to ensure that each employee within their organization receives the appropriate training.

g. Required Levels of Training. The level of training required in each training or subject matter area will vary from general awareness training to specific courses in such areas as contingency planning, depending upon the training objectives established by the Departmental components.

(1) **Awareness Training**. Awareness training should create the sensitivity to threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them. Initial security training shall cover rules of the system(s) to which the employee or contractor has access to; is consistent with guidance issued by NIST and OMB. Each VA employee or contractor shall receive initial AIS security training and thereafter receive "refresher" training on an annual basis.

(2) **Performance Training**. Employees develop skills to design, execute, or evaluate Department computer security procedures and practices. The purpose of this training is to enable employees to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

(3) **Policy-level Training**. Training provided for executives to enable them to understand computer security principles so that they can make informed policy decisions about the computer security program.

(4) **Implementation Training**. Training which provides program/functional managers with the ability to recognize and assess threats and

vulnerabilities to automated information resources. These managers then are able to set security requirements which implement VA security policy.

1. **REFERENCES**

a. FPM Bulletin No. 410-131, 5 CFR Part 930 "Training Requirement for the Computer Security Act."

b. NIST Computer Security Training Guidelines, Special Publication 500-172 (Nov. 1989).

CHAPTER 3. SECURITY INCIDENT REPORTING PROCEDURES

1. PURPOSE and SCOPE

a. This Chapter establishes mandatory procedures for Automated Information Systems (AIS) security incident reporting within the Department of Veterans Affairs (VA). It is designed to provide Department-wide guidance to VA Administrations, staff offices, and other key officials on the proper response to and efficient and timely reporting of computer security related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of VA data. These procedures are intended to meet required mandates of the Department and to assist in the protection of VA AIS resources from unauthorized access, disclosure, modification, destruction, or misuse.

b. An AIS security incident reporting system is necessary to identify a violation or incident, assess damage as a consequence of a violation, record the violation or incident, report the incident, and to use information to prevent the occurrence or violations. The reporting process outlined in these procedures are intended to discover and respond to AIS security incidents as they occur, will assist in preventing future incidents through awareness and, when combined with existing AIS security procedures, will augment VA AIS security controls.

c. These procedures apply throughout the Department and to the security of VA resources, including AIS, data stored and processed on those AIS, data communication transmission media, and personnel who use VA AIS.

2. RESPONSIBILITIES

a. The Secretary of Veterans Affairs is responsible for administering VA security and ensuring a VA AIS security program is implemented.

b. The VA CIO, as delegated by the Secretary of Veterans Affairs, is responsible for ensuring that AIS security incident reporting is included in VA's AIS security program.

c. Deputy Assistant Secretary for Information Resources Management is responsible for:

(1) Overseeing and ensuring that VA AIS Security Program requirements and practices are implemented for all VA automated information resources through the Information Resources Security Officer (IRSO) for VA.

(2) Ensuring that VA AIS Security Incident Reporting policy is developed and issued.

(3) Reporting to and advising the Secretary and Deputy Secretary on major AIS security incidents affecting VA.

d. The Information Resources Security Officer for VA is responsible for:

(1) Ensuring that appropriate Department procedures conform to the requirements of the Computer Security Act of 1987 and yearly OMB bulletins regarding its implementation, OMB Circular A-130 and its appendices, other Federal laws and regulations, and promulgating such additional regulations and guidance as necessary.

(2) Serving as primary point-of-contact for VA and Government-wide AIS security matters affecting VA, and specifically, major AIS security incidents.

(3) Developing and issuing Departmental AIS Security Incident Reporting policy for VA.

(4) Providing assistance to Administration Heads, Assistant Secretaries, and other key officials in preparing their AIS Security Incident Reporting policy, procedures, and standards to comply with Departmental policy.

(5) Monitoring, reviewing, and evaluating compliance with AIS Security Incident Reporting procedures and tracking major AIS incidents annually.

(6) Reporting and advising the Deputy Assistant Secretary for Information Resources Management on major AIS security incidents.

(7) Establishing an Incident Reporting and Response Capability in the Department to assist VA Administrations and staff offices by:

(a) Identifying causes for AIS security violations/incidents.

(b) Recommending corrective measures and solutions to resolve incidents.

(c) Coordinating information exchange of VA AIS security violations and incidents with Computer Emergency Response Team (CERT) organizations.

e. The Inspector General is responsible for:

(1) Investigating and auditing major AIS security incidents when appropriate, and conducting criminal investigations, as warranted.

(2) Providing advice on coordinating an investigative process for AIS security incidents and reconciliation of those incidents.

f. The General Counsel is responsible for:

(1) Interpreting laws, regulations, and directives applicable to VA AIS security activities, and specific to AIS incident occurrences and reporting of those occurrences.

(2) Rendering legal advice and other legal services with respect to AIS security incidents upon request to Administration heads, Assistant Secretaries, and other key officials.

g. Administration Heads, Assistant Secretaries, and other key officials are responsible for:

(1) Ensuring their Administration or staff office comply with the requirements of the VA AIS Security Incident Reporting policy.

(2) Ensuring that policy, procedures, and standards which meet the requirements of the VA AIS Security Incident Reporting procedures are developed for their respective Administration or staff office.

(3) Ensuring that their Administration or staff office Information Security Officer (ISO) identifies and reports major AIS security violations of AIS security policies, procedures, and accepted practices to the VA IRSO.

(4) Creating an incident response capability within their automated information system security program.

h. Each Facility Director is responsible for:

(1) Implementing the AIS security requirements of their respective facility.

(2) Ensuring that the facility ISO investigates, reviews and records AIS security incidents at the facility and reports the incidents to the appropriate Administration or staff office ISO.

(3) Ensuring that the assigned Incident Response team is notified when a reportable incident occurs

ı The facility ISO is responsible for:

(1) Establishing the facility's AIS security incidents reporting system.

(2) Logging, investigating, and reviewing AIS security incidents at the facility and reporting the incidents to the appropriate Administration or staff office ISO.

(3) Establishing contact with the assigned Incident Response team when a reportable incident occurs.

j. Managers and Supervisors are responsible for:

(1) Implementing the requirements of their respective Administration or staff office Information Security Officer AIS Security Incident Reporting procedures within their assigned areas of management control.

(2) Ensuring that AIS security violations/incidents occurring within their assigned area of management control are reported to the appropriate facility ISO.

(3) Ensuring on a regular basis that all assigned employees, contractors and other individuals, who develop, operate, administer, maintain, or use VA AIS, understand they are responsible for reporting actual or suspected AIS security incidents to their immediate supervisor or facility ISO.

k. All VA employees, contractors, and other individuals with access to sensitive areas or automated information systems are responsible for

reporting AIS security violations or incidents to their supervisor or ISO.

3. PROCEDURES - AIS SECURITY INCIDENT REPORTING SYSTEM

a. **Security Incident Standards**

(1) Computer security incidents can range from a single virus occurrence to a hacker attacking many networked systems, or such things as unauthorized access to sensitive data and loss of mission-critical data. An incident refers to a computer security problem arising from a threat.

(2) AIS security incidents to be reported and tracked can be categorized as follows (these types of acts are not all-inclusive):

(a) Circumvention of AIS security controls, safeguards and/or procedures;

(b) Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of data and AIS;

(c) Theft, fraud, or other criminal activity committed with the aide of AIS resources;

(d) Theft, loss or vandalism of AIS hardware, software or firmware;

(e) Issues affecting confidentiality, integrity and availability of data and AIS; and

(f) Unauthorized downloading or copying of VA sensitive information.

(3) Examples of specific reportable incidents which can be reported under the six categories of incidents include (but are not limited to):

(a) Unauthorized access to or use of sensitive data for illegal purposes;

(b) Unauthorized altering of data, programs, and AIS hardware;

(c) Loss of mission-critical data, i.e. patient, financial, benefits, legal, etc.;

(d) Environmental damage/disaster (greater than $10,000) causing loss of AIS services or data, or which may be less than $10,000 in damage yet have affected the Administration's or staff office's capabilities to continue day-to-day functions and operations;

(e) Infection of sensitive systems or software by malicious code, i.e. virus, Trojan Horse, etc.;

(f) AIS perpetrated theft,fraud and other criminal computer activity;

(g) Telecommunications/network security violations, i.e., networks (including local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs)) which experience service interruptions that cause an impact to an indefinite number of end users;

(h) Theft or vandalism of AIS hardware, software or firmware whose loss did or may affect the organization's capabilities to continue day-to-day functions and operations;

(i) Unauthorized access to data when in transmission over communications media;

(j) Loss of system availability impacting the ability of users to perform the functions required to carry out day-to-day responsibilities; and

(k) Unauthorized access to and/or unauthorized use of the Internet.

(4) VA Administrations and staff offices shall require their subordinate offices and facilities to report AIS security incidents, which the organization interprets as damaging to the organization's mission, to VA Administration or staff office ISO.

(5) VA Administration's or the staff office's ISO shall report those incidents which the organization interprets as damaging to the organization's mission, to the VA's OIRM Information Resources Security Officer (VA IRSO).

b **Reporting Procedures**

(1) AIS security incidents as defined in paragraph 3.a.(2) will be reported by the person observing or discovering the occurrence to the facility ISO. The facility ISO is responsible for recording and reporting security incidents to the Administration or staff office ISO for tracking and reconciliation of the suspected incident. Suspected AIS security incidents will be reported to ISOs within 48 hours of the occurrence. Additionally, those incidents which are determined to affect an Administration or staff offices' capability to accomplish critical functions, restrict the availability of a system or communications medium, i.e. LAN, MAN, WAN, network, etc., or result in a monetary impact to the Administration or staff office, will be reported within 48 hours of the occurrence to the VA IRSO, located in the Office of Information Resources Management, by the Administration or staff office ISO.

(2) AIS security incidents shall be recorded on a security incident form or log as defined by the facility. Essential information about the security incident should be identified in as much detail as possible, at the time of occurrence. Some information may need to be added at a later time based on the investigation/closure of the incident. The following minimum information about a security violation or incident shall be entered on the AIS security violation/incident form:

(a) Location of incident and organization filing report;

(b) Reported by (Name, Title and Organization);

(c) Date and time of report filing;

(d) Date and time of incident;

(e) Details of incident (include names of personnel involved and description of the who, what, when, where, how, and why);

(f) The name and title of the person to whom the incident initially was reported to;

(g) Identification of whether the Inspector General or appropriate law enforcement organization has been notified;

(h) Incident impact on day-to-day operations;

(i) Action taken to contain the incident and resources required to correct the incident (in cases of system outage note what vendors have been contacted);

(j) Short-range corrective action, such as discontinuing the use of an infected computer diskette, immediately removing a terminated employee's access privileges;

(k) Long-range corrective actions, as necessary;

(l) Estimated monetary damage; and

(m) Additional information, as appropriate.

(3) The information collected on the AIS security incident form shall be reported to the Administration or staff office ISO in a confidential manner, which may include the following methods. Initial reports of serious incidents or violations may be reported by telephone. Reports may be sent by U.S. mail using the double-envelope method, couriers, or secure facsimile. Follow-up contact will be

established with the reporting facility or office by the Administration or staff office ISO , and tracking for each incident will be continued until final closure. Each facility, local or office level ISO, or manager/supervisor will be responsible for making the determination of whether the AIS security incident at their level is reportable based on the definitions provided in this procedure and ensuring that reports are filed with their respective Administration or staff office ISO.

(4) Significant AIS security incidents shall be reported first to assigned VA Incident Response and Security Team which will identify and assist in resolving reported incidents.

c. **Protection of Report Information**. AIS security incident report information will be treated as sensitive information and safeguarded as equivalent to Privacy Act information, at a minimum. Access to AIS

security incident information should be restricted and shall be stored in locked areas.

d. **Tracking of AIS Security Incidents**

(1) Each VA Administration or staff office ISO is responsible for tracking AIS security violations and incidents for their organization. Tracking will include monitoring each incident through final closure and maintaining a copy of the incident report for a period of three (3) years. Reports of security violations and incidents shall be prepared and maintained by the Administration or staff office ISO. Those security violations and incidents which threaten critical organization functions shall be reported within 48 hours to the office of the VA IRSO by the Administration or staff office ISO.

(2) The office of the VA IRSO shall advise the DAS/IRM of security violations and incidents reported from VA Administration or staff offices which threaten critical VA functions.

e. **IRSO Handling of Reported AIS Security Violations and Incidents**

(1) The VA IRSO shall establish a log of reported security incidents. Automated files of reported incidents shall be protected against unauthorized access and not accessible through a network.

(2) Major elements of security incident records created and maintained by the VA IRSO shall include: name of VA Administration or staff office making the report; number of violations and incidents by type or nature, total number of violations and incidents; number of unresolved violations and incidents; and the estimated monetary loss attributable to all reported incidents.

f. **Reporting of Security Incidents and Violations to the Media.** All VA components shall refer questions from the media (e.g., newspapers, television, and radio) concerning AIS security violations or incidents to VA's Office of Public Affairs in VACO. The Department will respond to media requests for records concerning security under the Freedom of Information Act (FOIA) in accordance with VA procedures for responding to FOIA requests rather than with the procedures specified here.

4. REFERENCES

a. Information Resources Security Handbook, Office of Information Resources Management, H-003-1, 1991.

b. National Institute of Standards and Technology (NIST), NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC), November 1991.

c. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, dated February 8, 1996.

CHAPTER 4. VIRUS CONTROL PROCEDURES

1. PURPOSE. The following components provide prevention, detection, identification and recovery from computer viruses. This handbook contains mandatory Department of Veterans Affairs (VA) procedures for:

a. Reducing VA vulnerability of VA personal computers, local/wide area networks (LAN/WAN) from the threat of computer viruses and other forms of malicious code.

b. Ensuring timely detection of computer virus infections.

c. Providing a reliable means for containing and eliminating infections when they do occur.

2. BACKGROUND. The following includes basic background information necessary for a basic understanding of the computer virus threat:

a. What is a computer virus? A computer virus is a malicious software program with the ability to replicate itself, thereby spreading from computer to computer. The result of this infestation may simply be annoying, such as a display of messages or minor degradation of system performance. Viruses can also have catastrophic consequences, such as the complete destruction of all programs and data stored on a system's hard disks. Damages may not be limited to individual computers as accessible network disk drives may be infected and become a standing source of infection for other connected computers. Viruses may modify or destroy data rendering systems and possibly entire networks unusable. For the sake of simplicity in this document, any type of malicious program code will be referred to as a virus.

b. There are four types of viruses: The boot sector infector, the file infector, the companion virus and the Macro virus. Some viruses fit into more than one category because they infect boot sectors and files and so are called multipartite viruses. Some of these viruses may try to hide themselves by taking control of the operating system; these viruses are called stealth viruses. Some viruses encrypt themselves so every infection appears to be different; these are called encrypted viruses.

(1) **The Boot Virus.** The boot sector virus writes itself into the DOS system area on the floppy disks and hard disks it infects. This type of virus accounts for over 70% of all reported virus infections. It can only be passed to your computer when you inadvertently attempt to boot from a floppy disk left in the disk drive (generally people boot their computers from the hard drive). Once the computer's hard disk has become infected, the computer becomes a source for spreading the virus. The virus becomes active each time the system boots up and writes itself out to every floppy that passes through your computer. The boot virus cannot infect a network and cannot be passed throughout the organization through the LAN.

(2) **The File Virus**. The file virus or program virus, as it is often called, infects program files by attaching themselves to them or overwriting a portion of the program with the virus code. These viruses are easily passed over LAN/WANs or any other network, including Internet. They can be sent as attachments to e-mail or placed on electronic bulletin boards for the unsuspecting to download. They become active when the program they are attached to is executed.

(3) **The Companion Virus**. The companion virus may exist as a duplicate file but have the COM extension instead of the EXE extension. The COM companion virus executes first and after becoming active, it passes control back to the EXE which executes normally. There is also a type of companion virus that modifies the pointers in the directory to point to a virus instead of the intended program.

When a user attempts to execute a program, the virus executes and after becoming active, it executes the program that the computer user actually was trying to execute.

(4) **The Macro Virus.** Many software products include macro programming languages or tools allowing users the ability to automate tasks that were once repetitive. Due to the continual enhancements developers have made to these macro languages many are now sophisticated enough to create malicious programs which technically are computer viruses. Macro viruses can replicate and spread from computer to computer so they technically fall into the realm of the computer virus.

c. There are three main components to the logic code of a virus: the replication logic, trigger logic, and the attack or bomb logic. The replication logic is the portion of code that allows the virus to replicate itself; the trigger logic decides whether to attack or go dormant (replicate but not attack); and the attack logic destroys data or could be a relatively benign taunting message.

d. Other Forms of Malicious Programs. Though not covered specifically, many of the procedures described within this Chapter are equally applicable to other forms of malicious program code.

3. RESPONSIBILITIES

a. **The Department IR Security Officer (IRSO) will:**

(1) Manage the VA Computer Virus Protection Program. Collect AIS security violation and incidents information consistent with VA AIS Security Incident Reporting policy (Chapter 3, VA Handbook 6210). Maintain reports of incidents and share information on detection and removal of acute infections.

(2) Establish and disseminate virus protection procedures and guidelines to VA organizations on the prevention, detection, and removal of computer viruses.

(3) Serve as the Department point-of-contact for virus-related issues, including information on reputable anti-virus software and the identity of local VA office AIS security representatives.

(4) Provide Department-wide technical assistance in response to virus incidents, by recommending anti-virus software or other methods of detection and removal.

(5) Consult with automation personnel and VA network administrators (those having the responsibility of managing or maintaining a PC-based network) regarding virus prevention, detection and identification, and recovery procedures.

(6) Conduct reviews as necessary to ensure compliance with the mandatory security program requirements.

b. **All VA offices shall:**

(1) Establish operational procedures for network system administrators to implement an effective virus protection program.

(2) Assist the Department IRSO in responding to virus incidents.

(3) Contribute to the free flow of information concerning viruses by reporting incidents to the Department IRSO.

(4) Assist the Department IRSO in compliance reviews of the virus program.

(5) Ensure that maintenance contracts with consultants, repair technicians and troubleshooters contain security requirements for non-VA employees to follow, and includes security measures, such as virus scanning and prevention techniques.

c. **VA Network System Administrators will:**

(1) Where a network utility, facility, or mechanism exists, restrict network users so they cannot write to program files on network drives. Installed programs are never written to and so should be set as "read only or execute only." When possible,access controls should be set to prevent even network administrators from being able to write to program files (though they should have "delete" privileges). Doing this will prevent computer viruses from attaching to program files that are shared by all.

(2) Follow virus protection, detection and identification, and recovery policies and procedures. Maintain a current copy of licensed virus protection software on bootable write-protected diskettes.

(3) Use system administrator privilege on a LAN or a WAN only when doing administration or maintenance of the network requiring such higher levels of privilege. When assisting customers, privileged users should not log onto the network as system administrator from any machine that has not first been determined to be virus-free. For routine work, such

as e-mail, word processing, etc., administrators shall use accounts with normal user privileges.

(4) Keep write-protected copies of original software loaded to network servers to perform a necessary restore to workstations and to do regular back-ups of critical server data.

(5) Comply with directives provided by the Department IRSO in response to specific virus incidents, where applicable.

(6) Prepare additional local direction, such as operating memoranda, policies and procedures, where applicable.

(7) Report all computer virus incidents to the facility Director or designee and the facility ISO, and notify all network users.

d. **VA computer users will:**

(1) Employ physical access protection for all Department microcomputers to restrict access by unauthorized persons. Unknown and potentially unauthorized persons will be challenged in regard to their authorization to use equipment.

(2) Ensure that software loaded or data disks used on their computer are first scanned for possible viruses.

(3) Perform regular back-ups of computer data files. The frequency of these back-ups should be commensurate with the nature and criticality of the data stored.

(4) Use current anti-virus software on a daily basis for any microcomputer used in processing sensitive or critical VA information, including:

(a) portable microcomputers;

(b) microcomputers used to process diskettes received from sources outside VA;

(c) microcomputers returned from outside repair facilities;

(d) microcomputers that have had diagnostic utilities or other software run on them by repair technicians;

(e) employee-owned microcomputers that are used to process VA information (whether at home or office); and

(f) sales demonstration disks and beta test versions of software.

(5) Use anti-virus software to scan the entire hard disk after files have been recovered from back-ups if the recovery was required due to a virus-related incident.

(6) Use only software proven to be virus free after scan testing. Refrain from using unsolicited software sent to you by mail or obtained from external sources until tested.

(7) Obtain "shareware" software directly from official sources such as the developers' electronic bulletin board systems (BBS).

(8) Use only one write-protected boot disk for each floppy-based microcomputer and control access to this disk. On systems with hard disks, ensure the system boots from the hard disk and no floppy has been inadvertently left in the floppy drive (the computer may attempt to boot from it). If possible, configure the computer to boot only from the hard disk.

(9) Ensure original manufacturer software is securely stored in the event that programs must be restored to disk. Data can be backed up and software retained on original diskettes as back-ups.

(10) Comply with additional direction by the Department IRSO and organization AIS security representatives in response to specific virus threats, where applicable.

(11) Report all computer virus incidents to the facility or organization ISO.

e. **Consultants, Repair Technicians and Troubleshooters will:**

(1) Employ a reputable and current anti-virus product and scan all operating PCs before beginning to work.

(2) Report all computer virus incidents to their organization ISO.

4. PROCEDURES. While current physical and logical access controls provide protection against unauthorized system access on many networked computers, an authorized user may unknowingly introduce virus-infected software locally through floppy drives or remotely via a modem. A single infected microcomputer on a network can rapidly infect every workstation and server on that network. Implementation of the measures prescribed in this chapter will provide reasonable protection of VA information resources against the threat of computer viruses.

a. **FIRMR** (Federal Information Resource Management Regulations). VA must continue to develop an environment that will minimize the risks and consequences of virus infection to computers and LAN/WANs and is bound by the FIRMR Bulletin C-28, "Computer Viruses."

b. **Physical Access Control**. Physical access control will be employed on all Department computers to restrict use to authorized persons. This means that computers should be physically secured to prevent access by an unauthorized person.

c. **Key Locked**. Every newer personal computer has a key lock though it should be noted that this may only give an extremely low level of security. If keys are used as a first line of defense, then the

supervisor or other individual should keep the backup key in the event that the organization needs access to that computer.

d. **CMOS Security**. Many PCs have a CMOS setup routine that can be accessed from DOS by hitting the correct key combination. On many PCs the key combination is Ctrl-Alt-Esc, but your PC may be different. Before you attempt to change your PC's CMOS setup, see your owners manual for the key combination for your PC. Once you bring up the CMOS setup routine you can password protect your CMOS so it cannot be changed without the password, and you can password protect your PC so that it will not boot without the password. This gives you a low level of access control to your PC and may help to keep unauthorized persons from using your PC. In the same CMOS routine you should also set your PC to force booting from only the C: drive (hard disk). This will eliminate the possibility of your ever getting a boot virus, as it makes it impossible for your PC to boot from an infected floppy.

e. **Backups**. If anti-virus software efforts fail you will always be able to resume business as usual if a reliable backup has been done. Regular and frequent back-ups of computer data files should be performed to aid in the recovery from a virus or any data loss situation. Of course, if the system has been unknowingly infected by a virus for sometime, backups may be infected. When backups are infected, generally only the program files will be infected - not the data. In order to restore the program files to their original state, the user should be able to fall back to the original manufacturer's software diskettes. These should have been write-protected prior to installation (when possible) and stored securely for use in restoring original program files. In some cases where a mirror image of a complete disk is taken as a backup, a boot virus can be transferred to the backup. Restoring from such an infected backup will certainly restore the virus. For this reason, it is important to do file-by-file type backups rather than the "mirror" image or complete back-up.

f. **Virus Scanning.**

(1) When personal computers are attached to a LAN, they should contact the LAN System Administrator about having anti-virus software installed to secure each workstation against computer viruses. The LAN Administrator will monitor the LAN servers for virus activity through the use of anti-virus software. Set up the anti-virus software so that it scans the PC automatically when it is booted. Anti-virus software will be used on all local area networks (LAN) and connected workstations. Workstations to be connected should be determined to be virus-free before connection. There are anti-virus products that will check the boot area of the disk on boot up and may even restore the correct boot area if a virus has infected it. There are resident monitors that run continuously in the background. These should be used whenever possible because they prevent the admittance of viruses during the workday (after the initial scan has been done). However, in some instances, shortages of system memory may preclude the use of a resident scanner.

(2) An office may be using a variety of anti-virus software, possibly different products from what are used on the LAN or elsewhere. There is strength in diversity. No single anti-virus product can detect every

virus, so the fact that you are using an additional product may help to identify a virus that may otherwise go undetected. Special consideration should be given to the purchase of products that do not rely strictly on signature scanning as the primary method of detecting viruses. Signature scanners must be continually updated with the signatures of new computer viruses and may not be able to detect many encrypted viruses. Many products now use signature scanning merely as a method of identifying a computer virus once detected. It is highly recommended that a product be chosen that uses one of the following methods of detection: Generic Differential Detection, Holistic scanning, Heuristics or another non-signature based method, as the primary detection method.

g. **Scan Incoming Software**. Software obtained from external sources should be used only after it has been "scanned" by a reputable and reasonably current anti-virus product. All PCs and servers should undergo regularly scheduled scanning. Public domain "shareware," as well as commercial software, will be "scanned" for viruses before use. Computers returned from outside repair facilities will be "scanned" for viruses before being attached to a network or put into operation. Software utilities used by repair technicians will also be "scanned" before use. Repair/troubleshooting technicians should scan their software before use and keep it write protected while in use.

h. **VA Developed Software**. Software produced within VA will be designed to prevent it from being an avenue for infection, where possible. Developers may choose to write program routines that incorporate integrity checking algorithms or encryption for the program itself. All program disks should be "scanned" using a reputable and reasonably current anti-virus product before distribution. Only write-protected diskettes should be distributed.

i. **Diskettes from Home**. Diskettes taken home and used on home computers or brought from any non-VA location should be "scanned" with a reputable and reasonably current anti-virus product before use on a VA computer. Many home PCs are infected due to downloading anonymous software from electronic bulletin boards, trading games, etc. It is easy for a PC to become infected with a virus under these circumstances. If diskettes are taken home to do work, then they should use the same good security practices at home as at work. However, scanning the disk for viruses after returning to work is a good preventive measure.

j. **Trophy Viruses**. Unless you are a member of an AIS Security staff and need to save computer viruses for study and distribution to anti-virus community, do not attempt to save them. However, an infected file or disk can be retained for the purpose of supplying the anti-virus software developer with the virus for analysis. This diskette should be clearly marked as infected and sealed in an envelope so that it is not inadvertently used. Other than these exceptions, when a virus is detected, it should be destroyed immediately.

5. REFERENCES

a. For Your Eyes Only, quarterly AIS security bulletin for the Department of Veterans Affairs, Library of Congress serial publication number ISSA 1071-4286.

b. National Institute of Standards and Technology (NIST) Special Publication 500-166 Computer Viruses and Related Threats: A Management Guide, by John P. Wack and Lisa J. Carnahan.

CHAPTER 5. COPYRIGHT SECURITY PROCEDURES

1. PURPOSE AND SCOPE

a. All VA employees are required to protect government and public interests as they perform their duties. This includes assuring that government-acquired software protected under the Copyright Act is used in accordance with the law and the software licensing agreement. It is the responsibility of all VA organizations and employees to ensure that copyrighted software is licensed properly before being installed on VA equipment. Title 17, United States Code, Section 106, gives copyright owners exclusive rights to reproduce and distribute their material; Section 504 states that copyright infringers can be held liable for damages to the copyright owner. Title 18, United States Code provides felony penalties for software copyright infringement. This policy does not apply to software developed by the Department or for use by the Department under a Departmentwide license.

b. Special purpose software shall be used to perform a software audit which will inventory and document software on each PC in the organization. Such software may be a commercial product or may be acquired free from the Software Publishers Association (SPA) through the organization's Information Security Officer (ISO).

c. Individual employees may not install privately-owned software on government equipment unless it is in the best interest of VA. Authorization and justification for the installation of privately-owned software must be approved, in writing, by the VA employee's facility or organization management. Prior to authorization, the employee's management should require the employee to provide the software license and give assurance that copyright infringement will not result from the installation, in addition to other local management requirements. Individuals not following these procedures may be held personally liable for any violations of the copyright law and subject to the penalties specified in Titles 17 and 18 of the United States Code.

d. The Computer Software Rental Amendments Act of 1990 (Title VIII Public Law 101-650) prohibits the rental, leasing, or lending of

original copies of any computer program for the purposes of direct or indirect commercial advantage without express permission of the copyright owner.

e. Old versions of software that have been upgraded shall be disposed of in accordance with the licensing agreement and may have to be returned to the manufacturer or destroyed, depending on the software licensing agreement terms. The new upgrade is usually intended to replace the old software, resulting in a single copy license. It may be a violation of copyright to continue to operate old versions after the upgrade has been installed. VA facility management shall ensure that software licensing agreements permit old versions of software that have been upgraded, to be loaned or taken home by VA employees. This practice will avoid violating the copyright law.

2. RESPONSIBILITIES

a. Each facility director is responsible for ensuring that software copyright procedures are included in the facility's AIS security program and are complied with.

b. Managers and immediate supervisors are responsible for ensuring that employees are trained in and follow the established procedures and acceptable practices allowed under software copyright laws and VA facility policy and procedures.

c. The facility ISO, for the Director, implements the facility's AIS security program and its components, and ensures the facility security program is in compliance with software copyright laws and VA facility and Central Office policies.

d. All VA employees, contractors, and other individuals using IRM technology resources, shall adhere to software copyright laws and VA facility security policy and procedures.

3. PROCEDURES. The following practices and procedures will be adhered to by all employees. VA managers and supervisors will be held accountable for conducting periodic audits to ensure compliance:

a. Install on VA systems only commercial software, including shareware, that has been purchased through the government procurement process. An exception to this rule is when privately-owned software is authorized to be installed on government equipment by VA facility or organization management.

b. Follow all provisions of the licensing agreements issued with the software and register organizational ownership.

c. Make only authorized copies of copyrighted software. Normally, the license will allow a single copy to be made for archival purposes. If the license is for multiple users, the authorized number of copies shall not be exceeded.

d. At least annually, inventory and maintain written records of all software on each individual PC. This inventory shall be compared with the organization's licensing agreement records to ensure licensing compliance.

e. Maintain written records of software installed on each machine and ensure that a license or other proof of ownership is on file for each piece of software.

f. Store licenses, software manuals and procurement documentation in a secure location (e.g., locked file cabinet, etc.).

g. When an upgrade to software is purchased, dispose of the old version in accordance with the licensing agreement. Upgraded software is considered a continuation of the original license, not an additional one. The continual use or redistribution of old versions (that have been upgraded) may be a violation of copyright law.

h. Some government-owned software licenses allow employees to take copies home for use on their privately-owned computers under specific circumstances (e.g., for government work, but not personal business). Unless the license allows this specifically, doing so is in violation of the copyright law, and the individual may be held liable.

i. All unauthorized copies of software, identified during audits or compliance reviews, shall be removed immediately.

4. REFERENCES

a. P.L. 102-561, Amendment to Title 18, Criminal Penalties for Copyright Infringement.

b. P.L. 101-650, The Computer Software Rental Amendments Act of 1990.

l. Title 17, U.S.C, Copyright Act.

CHAPTER 6. PROCEDURES FOR SAFEGUARDING SENSITIVE INFORMATION STORED ON AUTOMATIC DATA PROCESSING EQUIPMENT DURING DISPOSAL

1. PURPOSE AND SCOPE. This Chapter provides the authority, responsibilities, procedures and controls required for removing sensitive information that resides on automatic data processing equipment (ADPE) storage media prior to its disposal. The provisions of VA Directives 6300 and 6210 govern the protection and disclosure of sensitive information in VA. Sensitive information must always be protected from unauthorized access and disclosure. Inadvertent disclosure of sensitive information can occur when the storage media for this information is released for disposal without the permanent erasure of the sensitive information. The residual physical representation of data on storage media is known as data remanence. This Chapter provides

the appropriate procedures, safeguards, and actions to be taken to protect sensitive information before the storage media containing the sensitive information is released for disposal. The provisions of this Chapter and governing directive are applicable to all organizational elements within the VA and must be implemented at all VA offices and facilities within 180 days from the date of issuance.

2. RESPONSIBILITIES

a. The VA CIO is responsible for developing and recommending policies and controls for the selection and protection of sensitive information in the Department.

b. Administration heads, Assistant Secretaries, Deputy Assistant Secretaries and other key officials are responsible for ensuring that offices and facilities under their control include policy and procedures in their computer security programs for the protection of sensitive information during the disposal of ADPE storage media.

c. Each facility director, manager or other person accountable for the control of ADPE is responsible for the development and implementation of rules and procedures for safeguarding sensitive information contained on storage media before it is disposed of.

d. The VA Information Resources Security Officer (IRSO) is responsible for monitoring, reviewing and evaluating compliance with this automated information system (AIS) security program directive. The IRSO reports the results of reviews to the Deputy Assistant Secretary for IRM.

3. PROCEDURES

a. This Chapter provides the procedures and methods to apply when ADPE with permanent storage capabilities (retention of data occurs in storage, on either removable or "non removable" media), including magnetic, solid-state and optical storage media, is being released for disposal. This Chapter only applies to the removal of sensitive information from ADPE slated for disposal, not the disposal of the ADPE. The disposal of ADPE must comply with the FIRMR Part 201-23, Disposition, and the applicable VA policies. The term disposal, as used in this Chapter, applies to actions where equipment is excessed, transferred, discontinued from rental/lease, exchanged, or sold.

b. Mandatory Disposal Procedures. Procedures and standards governing the disposal of sensitive information must be developed and implemented by each facility director, manager or person accountable for the control of ADPE that processes or stores sensitive data in VA. Disposal procedures for storage media that meet these criteria are mandatory and shall include, as a minimum, the following methods, controls and practices:

(1) **Operating Procedures.** Written operating procedures which specify security requirements and standards for disposal of storage devices that contain sensitive information shall be used. Procedures for the removal or clearance of those media before release or reuse of the equipment is permitted shall also be included in the procedures. A quick reference

guide detailing procedures for disposing of a personal computer is contained in Appendix A.

(2) **Trained Staff Assigned**. Staff trained in data eradication methods and procedures shall be used to irrevocably clear and remove sensitive information from equipment and storage media scheduled for disposal or release.

(3) **Method for Cleaning Storage Media**. The method selected for clearing/purging storage media must fit your situation, storage device to be cleared, the sensitivity of the data, the acceptable level of data remanence (how much data remains on the storage media) and the possible or potential risk of data recovery after the equipment is released. The principal methods for safeguarding sensitive information during the disposal or repair of equipment include: overwriting; degaussing; destruction of the storage media; removal of the storage media; or declassification of the information.

(4) **Approved Software**. Only software adhering to the VA standard shall be used for overwriting and removing of sensitive information; overwrite software itself must be protected from unauthorized modification or use. The VA standard used for overwrite software is found in the National Computer Security Center's publication, A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025 Version-2.

(5) **Approved Demagnetizing Device or Demagnetizing Services**. Only manufacturer recommended degausser products that are listed for your hardware or storage media shall be used. Contracting with the appropriate vendor for this service may be an acceptable alternative to the purchase of equipment to demagnetize storage media. Where contracts with vendors already exist for services and maintenance of PCs, contact the VA project manager for that specific contract. An agreement for demagnetizing services may exist or could be centrally developed. When using contracted vendor services, specific measures, such as non-disclosure agreements with the vendor, must be devised and implemented to ensure that vendors or other personnel authorized to access sensitive data preserve the confidentiality of that data during the data clearance process.

(6) **Sensitive Data Protected during Maintenance and Repair**. Procedures shall be established by Department components to ensure that authorized personnel, including non-VA personnel, such as vendors and contractors, preserve the confidentiality of sensitive data and that unauthorized personnel do not access sensitive files during repair or maintenance. These procedures shall be consistent with statutes and existing policies which govern actions during maintenance and repair of ADPE.

(7) **Equipment and Storage Devices Certified**. An official at each station, facility and key VA Central Office organization shall be appointed to certify, in writing, that equipment with storage media has been properly cleared of all information before it is excessed, transferred, discontinued from rental/lease, exchanged, sold or otherwise released.

(8) **Information Removed from Storage Media Properly Retained or Disposed of.** Prior to disposal or release of the computer storage media, all records maintained on the storage media shall be retained or disposed of in accordance with the instructions in the approved records control schedule. The responsible records control office shall be contacted for guidance.

c. When maintenance or repair is required for ADP equipment with storage media or the storage media alone, sensitive data residing on that equipment must also be protected. Specification of procedures for the protection of sensitive information when maintenance or repair is planned is beyond the scope of this policy. Department components are expected to establish procedures to preserve the confidentiality of sensitive data under these circumstances consistent with any applicable statutes and existing directives.

d. When disposal of storage media involves transfer between or within VA facilities, these procedures are limited to instances where ADPE storage media containing sensitive information is sent to a VA facility or to a VA component within a VA facility where individuals with access do not have a need to know. "Need to know" is the principle that a Department official or employee may have access to sensitive information in VA computer systems and storage media only when the official or employee needs access to that information in order to perform an assigned task or duty within the official assigned responsibilities of the individual.

e. Security planning that includes mandatory disposal procedures will help prevent the compromise of sensitive information contained in a computer system or its parts after it is out of the control of the VA organization that had custody. Appendix A to this Handbook contains a list of steps for the removal of sensitive information from a personal computer before it is released.

f. Requirements established in this handbook for safeguarding sensitive information are in addition to requirements in other VA directives that govern the handling and disposition of FIP resources.

g. Sensitive information as used in this Chapter does not include computer software or computer programs that process sensitive information or other VA data.

4. REFERENCES

a. Computer Security Considerations in Federal Procurements, National Institute of Standards and Technology; Special Publication 800-4.

b. DOD Computer Security Center (NSA), A Guide To Understanding Data Remanence in Automated Information Systems, NCSC-TG-025 Version 2, September 1991.

c. DOD 5200.28 STD, "Trusted Computer System Evaluation Criteria," December 1985.

d. Privacy Act of 1974, 5 U.S.C. 552a.

Chapter 7. LOCAL AREA NETWORK SECURITY PROCEDURES

1. PURPOSE AND SCOPE. Local area networks (LANs) have become an important tool for organizations to meet their information processing, communications, and office automation needs. LANs provide the distribution of data, applications, and communications services to network members. By way of a common network operating system (NOS), LANs connect file servers, workstations, printers, and mass storage devices, and enable users to share resources and functionality. With the distribution of data over the LAN to the organization, security for the protection of data must also be distributed. It is important to understand the security needs before appropriate security procedures and measures can be devised and implemented.

2. RESPONSIBILITIES

a. Administration Heads, Assistant Secretaries, and other Key officials are responsible for ensuring development of LAN security policy and procedures in their organizations.

b. Each facility director is responsible for implementation of LAN policy and procedures.

c. Managers and immediate supervisors are responsible for informing staff about this policy, assuring that each affected person has access to a copy, and ensuring employees receive training on this aspect of AIS security.

d. LAN managers and administrators are responsible for implementing specific LAN security measures and techniques to protect PCs, network servers, and other network resources and comply with the facility's or organization's LAN security policy.

e. All VA employees, contractors, and other individuals using IRM resources are responsible for complying with security policy established by those primarily responsible for the security of the data, and for reporting to management any suspected breach of security.

3. PROCEDURES

a. **LAN Security Requirements**

Minimum essential security requirements for local area networks (LANs) in VA shall include:

(1) Define LAN configuration

(2) Determine the risks to the LAN: A risk assessment should be done to determine the criticality of the LAN based on the level of sensitivity of the information, the vulnerabilities and the safeguards to be taken to reduce those vulnerabilities.

(3) Select security measures: Determine security procedures and

devices needed to secure the LAN at an acceptable level of risk.

(4) LAN information security policy.

(5) Maintenance of confidentiality of sensitive data as it is stored, processed or transmitted on a LAN.

(6) Maintain the integrity of data as it is stored, processed or transmitted on a LAN.

(7) Maintain the availability of data stored on a LAN, as well as the ability to process the data in a timely fashion.

b. **Components of Network Security Design**

Mandatory elements of a network system design shall include:

(1) LAN Configuration description. LANs should be configured to limit each user's access to only the resources they need to accomplish their job.

(2) Develop LAN security requirements.

(3) Implement and test security measures. Unauthorized LAN Access:

(a) List possible vulnerabilities, such as lack of or insufficient identification and authorization process, improper password management, etc.

(b) Computer users shall be required to have a separate ID and passwords. Users shall be required to change their passwords at least once every six months, password length must be at least six characters in length, and are not an English word or name.

(c) The LAN must have an intruder lock out feature that would suspend an account after three invalid attempts to logon. This will help the systems administrator determine if efforts are being made to compromise LAN security. This limits the number of failed login attempts before suspending that account ID. When a lock out occurs, the systems administrator should investigate to determine whether the action was that of an authorized user or an attempt to intrude. Attempted

intrusions should be studied for ways to improve the security of the network.

(d) Require the use of encrypted passwords when available. This features should be implemented at the time the LAN is installed as it is most transparent to the users at that time.

(e) When employees are no longer part of the organization, or their duties change, their account access should be appropriately modified or terminated.

c. **Unauthorized Access to LAN Resources**

(1) List possible vulnerabilities, such as improper use of LAN manager, system operator (sysops) privileges, etc.

(2) Limit the number of individuals who have systems administrator privileges. The systems administrator should have a separate ID and password for exercising systems administrator privileges.

(3) Limit the number of individuals who have print queue management privileges. These personnel should have a separate ID and password for exercising queue management privileges. Ensure that personnel who possess this privilege are properly trained and monitored to ensure they do not use the print queue login only for its intended use.

d. **Disclosure of LAN Data**

(1) List possible vulnerabilities such as data stored in open area, data stored in unencrypted form, etc.

(2) Ensure that provisions for physical security of data in the work place are commensurate with the nature of the data to which users have access.

Physical controls used for an area should take into account those employees authorized to be in an area but who are not authorized access to sensitive information.

(3) Determine who has access to the work place during regular working hours to safeguard all information technology resources.

e. **Unauthorized Modification of Data and Software**

(1) List possible vulnerabilities, such as improper or unnecessary permissions granted to employees, viruses, etc.

(2) Restrict the access of users to the LAN by limiting their access to specific business hours only.

(3) Limit the number of active logins employees may use at any one time.

(4) Restrict employee access to the LAN by permitting them access from their workstation on his/her desk only.

(5) Employee workstation access to such network resources as the Internet needs to be addressed by use of firewalls or other such features. The Internet for all its usefulness is also an access point for virus infection.

f. **Backup of LAN Data**

(1) List critical data on the LAN and determine the frequency of backups, which should be performed at least weekly, or more often, depending on the nature of the data.

(2) Several generations of monthly backups should be retained and the restore process tested regularly to ensure that the LAN server disks can be restored to their original state.

g. **Disruption of LAN Functions**

(1) List possible vulnerabilities, such as inability to redirect LAN traffic, "single point of failure" LAN configuration, etc., to identify and prevent denial of service situations.

(2) During the design of the LAN architecture, plan system redundancy and system backup at critical junctures of the system. Good systems design improves continuity of operations prospects by not creating "a single point of failure" where the failure of one system component can bring down the entire LAN.

(3) List possible threats, vulnerabilities and resultant risks for assessment.

h. **Selection of Security Controls**. Security mechanisms, procedures, software, etc. should be installed on the LAN to control or reduce the risk resulting from threats posed by LAN weaknesses. These "Security Services" include the following:

(1) Identification and authentication. A mechanism that provides an assurance of the identity of an individual.

(2) Access Control. A mechanism to restrict use of system resources.

(3) Data Confidentiality. A process of keeping data secure.

(4) Data Integrity. A process to ensure that data is not destroyed or modified.

(5) LAN Message Confidentiality. A process of protecting the privacy of e-mail so that only the intended recipient(s) can read it.

(6) LAN Message Integrity. A process of protecting the contents of a message to ensure that it is not modified.

(7) Non-repudiation. A method which ensures senders and receivers of data cannot repudiate their processing of data.

(8) Logging and Monitoring. Audit trailing of specific system activities.

i. **Match Security Controls with Security Requirements**

(1) Determine the appropriate security services compared with risk of a threat and the cost for implementing a security mechanism that reduces a risk.

(2) Calculate costs for security mechanisms.

(3) Rank security measures.

j. **Implement and Test Security Mechanisms**

(1) Develop security controls implementation plan.

(2) Independently test mechanisms.

(3) System test the mechanisms/controls.

(4) LAN security requirements should be reviewed.

(5) Risk should be reduced to lowest acceptable level.

4. REFERENCES

a. FIPS Pub 191, "Guideline for Local Area Network Security."

b. "Glossary of Computer Security Terms," National Computer Security Center, NCSC-TG-004, version-1.

JANUARY 30, 1997

VA HANDBOOK 6210

APPENDIX A

REMOVAL OF SENSITIVE DATA-

QUICK REFERENCE GUIDE

Prior to the release of a PC with sensitive data (as distinguished from the software which processes the data) stored on the hard disk, one of the following methods for removing or destroying that data must be applied. Select from the following acceptable options the method your office will use to accomplish this requirement:

1. If possible and permissible, remove the PC's hard disk (removable drive).

2. If removal of the hard disk drive is not feasible, the following procedures and techniques are recommended to remove or destroy sensitive data on the PC's hard disk(s):

a. Overwrite software. Overwrite software, which employs a computer program to write a pattern of characters (usually 1's, 0's, or a combination of both) onto the location of the storage media (hard disk) where the sensitive data is located, may be used to obliterate data on the PC. Overwriting using 1's and 0's should be performed at least twice on hard disks used to store sensitive data. After using overwrite software on a disk, the overwrite should be verified. This may be done by attempting to recover the data on the overwritten disk by using any one of several commercially available "data recovery utilities." Overwrite software is commercially available in most local computer retail stores and also appears on approved VA and GSA product lists.

b. Degaussing. Degaussing is a method to magnetically erase data from magnetic storage media, such as hard disks. Degaussing involves using an alternating current (AC) to generate a magnetic field to demagnetize the hard disk. Two types of degaussers are used: strong magnets and electric degaussers. Degausser products and equipment are tested by the DOD, approved by NSA, and then placed on NSA's Degausser Products List (DPL). If this method of data destruction is selected, contact a security specialist in the IR Security Office, in the Office of the DAS for IRM, for specific information on degausser options.

c. Destruction. Destruction of the media (hard disk) containing sensitive information may involve incineration, application of an acid solution, or processing at an approved metal destruction facility. When possible, sensitive information should be removed from the disk before it is destroyed. Most destruction methods or procedures involve potentially hazardous conditions and should be done only by qualified and approved personnel. Refer to NSA's NCSC-TG-025 Guide for specifics on this method and its applicability.

3. Document that sensitive data has been cleared from the PC being released.

Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 5011/5
Transmittal Sheet
September 22, 2005

HOURS OF DUTY AND LEAVE

1. REASON FOR ISSUE: To revise Department of Veterans Affairs (VA) policies and procedures for the approval of alternative workplace arrangements (telework). "Telework" means to work from an alternative worksite other than the traditional office setting. Alternative worksite locations may include work-at-home, community-based telecenters and/or satellite centers, and virtual employment arrangements.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook revises the policies and procedures for home-based telework, community-based telework, mobile and virtual employment arrangements, and other appropriate telework arrangements. The pages in this issuance replace Part II, Chapter 4, and Appendix B of VA Handbook 5011. The revised policy:

a. amends participation to include title 38 employees on a case-by-case basis;

b. clarifies the responsibility of senior officials with respect to program implementation;

c. includes updated information on legislative initiatives on telework;

d. provides information on "how to participate;"

e. includes references to two new telework forms VA Form 0740a, Telework Proposal, and VA Form 0740b, Telework Self-Certification Safety Checklist Work-at-Home;

f. eliminates the Office of Personnel Management (OPM)-based annual or semi-annual review of pilot telework arrangements; and

g. provides for privacy data to be accessed remotely.

3. RESPONSIBLE OFFICE: Office of Human Resources Management and Labor Relations, Worklife and Benefits Service (058).

4. RESCISSION: VA Handbook 5011, Part II, Chapter 4, Alternative Workplace Arrangements (Flexiplace), and Appendix B, Sample Alternative Workplace Work Agreement, dated April 15, 2002.

CERTIFIED BY:

/s/
Robert N. McFarland
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
R. Allen Pittman
Assistant Secretary for
Human Resources and Administration

ELECTRONIC DISTRIBUTION ONLY

CONTENTS

PARAGRAPH PAGE

CHAPTER 4. ALTERNATIVE WORKPLACE ARRANG[E]MENTS (TELEWORK)

APPENDICES

[CHAPTER 4. ALTERNATIVE WORKPLACE ARRANGEMENTS (TELEWORK)

1. PURPOSE. This chapter sets forth Departmental policies and procedures on flexible work arrangements (telework). Telework provides employees with the opportunity to perform their work at locations other than the traditional office setting. It may include home-based telework, community-based telecenters, mobile and virtual offices, and U.S. General Stores. This chapter covers employees under the General Schedule, including those covered by the Performance Management and Recognition System Termination Act of 1993, members of the Senior Executive Service (SES), and employees compensated under the Federal Wage System (FWS). On a case-by-case basis, this chapter also covers Veterans Health Administration (VHA) employees appointed under 38 U.S.C., chapters 73 and 74.

2. POLICIES AND PROCEDURES

a. Telework may benefit the Department and employees by providing an alternative work situation, which may improve services to veterans, improve productivity, help recruit and retain personnel, and improve the quality of life of participants.

b. Employees who meet the criteria for telework may participate in telework arrangements in accordance with applicable laws, and collective bargaining agreements. Participation in a telework arrangement is subject to supervisory approval. Whenever appropriate, management may consider establishing telework arrangements to meet its needs as well as those of employees. Employee participation in a telework arrangement is voluntary. Telework provides managers, supervisors, and employees with alternatives to the traditional worksite in accomplishing work objectives. Telework may be used as a reasonable accommodation for employees with qualifying disabilities under the Americans with Disabilities Act, 42 U.S.C. § 12101 et seq. However, each telework arrangement must meet the minimum requirements as specified in paragraph 6.

c. The primary intent of the program is to support the mission of the office in an alternative work setting. Telework must not be used as an alternative to or in lieu of dependent care.

d. Telework arrangements may be established at community-based telecenters, the employee's residence, and mobile/virtual offices when determined by work unit supervisors to be consistent with the mission of VA.

e. Prior to initiating, modifying, or terminating a telework arrangement that affects employees in a collective bargaining unit, appropriate labor relations obligations must be fulfilled.

f. It is recommended that each supervisor conduct a periodic review of the telework arrangements to determine the impact on work operations.

g. If management determines that a telework arrangement is not meeting the operational needs of the organization, the arrangement will be modified no sooner than two weeks after the employee is notified, or in accordance with the required notice periods specified in applicable collective bargaining agreements. Supervisor modification or termination of the arrangement requires two weeks notice except where:

(1) otherwise specified in a collective bargaining agreement,

(2) work-related circumstances require otherwise, e.g., emergency situation,

(3) management determines that the teleworker is not meeting performance criteria,

(4) the employee breached information security protocol, or

(5) the employee works overtime without prior advanced approval.

h. Equal employment opportunity principles are fully applicable to the operation of this program.

3. RESPONSIBILITIES

a. Under Secretaries, Assistant Secretaries, Other Key Officials. These officials, or their designees, are responsible for implementation and administration of telework programs and this policy within their organizations; ensuring that managerial, logistical, organizational, or other barriers to implementation and successful functioning of the telework program are removed; and approving or discontinuing telework arrangements in VA Central Office. Each Administration will be required to provide timely employee participation data to meet the Departmental annual reporting requirement; specifically July 15 of each calendar year until otherwise notified. Reporting data will be submitted to the Office of Human Resources and Labor Relations, Worklife and Benefits Service.

b. Facility Directors. Facility Directors are responsible for implementing telework programs and approving or discontinuing telework arrangements for employees under their jurisdiction. The approval of telework arrangements should be coordinated with facility Human Resources Management Officers and Information Security Officers.

c. The Deputy Assistant Secretary for Human Resources Management and Labor Relations will advise management and operating officials on the policies and procedures in this chapter.

d. Supervisors are responsible for determining position and employee suitability for telework arrangement and coordinating the completion of the User's Remote Computing Security Agreement with the employee. The Agreement is available in the "VA Remote Access Guidelines" located at the VA intranet address http://vaww.admin./vpn.va.gov/one-va-vpn/home/VARemoteAccessGuidelines.doc. Supervisors must then ensure that the employee coordinates the request for remote access through the Information Security Officer. They must also ensure adequate coverage during public business hours, that operations continue to be carried out in an efficient and economical manner, and that participating and non-participating employees are treated equitably.

e. Employees are responsible for maintaining productivity and for fulfilling their obligation to account for a full day's work.

f. Employees are responsible for working with their supervisor in completing the User's Remote Computer Security Agreement and coordinating the request for remote access with the facility Information Security Officer.

4. REFERENCES

a. Office of Personnel Management Memorandum, "Alternative Workplace Arrangements (Flexiplace)," dated October 21, 1993.

b. OPM Guidance to Heads of Executive Department and Agencies (February 9, 2001).

c. President's Management Council National Telecommuting Initiative Action Plan.

d. Public Law 105-277, Omnibus Appropriations Act, Title IV, § 630.

e. Public Law 106-346 Sec. 359, Department of Transportation and Related Agencies Appropriations, 2001 (October 23, 2000).

f. Public Law 106-359, Joint Resolution making further continuing appropriations for the fiscal year 2001, and for other purposes (October 26, 2000).

g. 5 U.S.C. § 552a.

5. DEFINITIONS

a. Community-based Telecenter is an office typically in a space owned or leased through General Services Administration (GSA), and/or other Federal government facility, which may be shared by multiple agencies, or a satellite office of a single agency where an employee works one or more days in the workweek. For an update of the most recent telework centers, see GSA/OPM Web site *www.gsa.TeleWork.gov*.

b. Home-based/Work-at-Home Telework means allowing employees to use information technology and communication packages to work one or more days in the workweek at the employee's place of residence.

c. Mobile/virtual office means a location or environment, which may include customer sites, hotels, cars, or at home, where an employee performs work through the use of portable information technology and communication packages.

d. Official duty station means the official duty station for an employee's position of record as indicated on the most recent notification of personnel action.

e. Telework means working from an alternative worksite, rather than the traditional office. This may be an employee's home or a telework center. Flexiplace, telecommuting, work-at-home, and telework all refer to paid employment away from the traditional office. The terms Flexiplace, telecommuting, and telework are synonymous and may be used interchangeably.

6. TELEWORK CRITERIA

a. **Participation.** Participation in a telework arrangement is voluntary. Position suitability and availability of staff and resources are considerations for management when determining employee participation.

(1) Telework is a voluntary work arrangement that can be terminated by the employee or supervisor at any time with appropriate notice, at least two weeks. However, for employees covered by a collective bargaining agreement, the notice must be consistent with the agreement. In the event of a change in supervisor, the supervisor shall evaluate the need to continue the telework arrangement and inform the employee of their decision to continue or terminate the arrangement, consistent with applicable collective bargaining agreements.

(2) VA employees selected for telework arrangements must have a performance rating of successful or equivalent. They should have a history of being reliable, responsible, and able to work independently. Both full-time and part-time employees may participate in a telework arrangement. Telework is not recommended for trainee positions.

(3) The supervisor is responsible for determining how many days per week are appropriate for a telework arrangement. Each arrangement to telework is to be considered individually.

(4) The supervisor should discuss the requirements and expectations of the telework arrangement with the employee prior to recommending approval of a telework agreement.

(5) All teleworkers and their immediate supervisors should receive training designed to provide the employee and supervisor with a smooth transition to telework. Statistical studies show that participants who receive training have a much better chance at succeeding.

b. **Position Suitability**

(1) Management officials are responsible for determining which positions are appropriate for telework arrangements consistent with labor relations obligations.

(2) Position suitability should be reviewed by management officials based on the functions and duties of the position rather than the title. Tasks that can be performed away from the traditional office are generally more suited for a telework arrangement. In some instances, duties performed in the traditional office location could be separated from the employee's duties and performed at the alternate worksite. This approach to "job reengineering" can assist in providing appropriate avenues toward telework. Guidelines for position suitability include but are not limited to:

(a) Work activities must be portable and can be performed effectively outside the traditional office location;

(b) Job tasks are quantifiable or primarily project-oriented;

(c) Contact with other employees, the supervisor or manager, and serviced clientele is predictable and normally scheduled;

(d) The computer technology needed to perform work off-site is currently available;

(e) Employees may be linked electronically to the traditional office location by computer and modem or may simply take work to the alternative worksite, requiring no computer;

(f) No classified documents may be taken to, used, or stored at an employee's home office or telecenter. The employee must return to the traditional office to access and work on such documents or materials; and

(g) Privacy Act materials, evidence, or sensitive documents (hard copy or electronic) may be accessed remotely provided that the employee agrees to protect Government/VA records from unauthorized disclosure or damage and will comply with the requirements of the Privacy Act of 1974, 5 U.S.C. § 552a, and all applicable Federal law and regulations, VA Directive and Handbook 6210, and other applicable VA policies.

c. **Process for Establishing a Telework Arrangement**

(1) The employee completes VA Form 0740a (Appendix II-B of this handbook), Telework Proposal, which describes how the proposed arrangement would work and submits it to the immediate supervisor.

(2) The immediate supervisor makes a preliminary determination as to position and employee suitability for telework.

(3) The immediate supervisor agrees/disagrees to the employee's participation and approves/disapproves the Telework Proposal noting any modifications to the proposal.

(4) The immediate supervisor and employee develop a telework agreement which lists all terms and conditions for the telework arrangement (Appendix II-A of this handbook), and complete the User's Remote Computer Security Agreement. The Agreement is available in the "VA Remote Access Guidelines" located at the VA intranet address http://vaww.admin./vpn.va.gov/one-va-vpn/home/VARemoteAccessGuidelines.doc.

(5) The employee notifies the Information Security Officer (ISO) of the telework arrangement and obtains ISO certification approving that the appropriate security controls are in place.

(6) If this is a work-at-home Telework Proposal, the employee must complete a VA Form 0740b (Appendix II-C of this handbook), Telework Self-Certification Safety Checklist, and submit it to the immediate supervisor.

(7) VA Form 0740a, Telework Proposal, a telework agreement, approved ISO certification and VA Form 0740b, Telework Self-Certification Safety Checklist (if appropriate), are submitted to the designated management official or his/her designee within the chain of command for final approval by signing the Telework Proposal.

(8) Management must address all collective bargaining obligations if applicable.

(9) If a telework arrangement is denied, the Telework Proposal form must annotate the reason why the request was denied. The decision to deny the telework agreement is not subject to any formal appeal procedure; however, it may be grieved under applicable negotiated grievance procedures.

(10) If a telework arrangement is approved, the employee and immediate supervisor sign the telework agreement.

d. **Minimum Participation Criteria**

(1) The employee's position must be suitable to telework.

(2) All appropriate forms must be completed and contain approval signatures (VA Form 0740a, Telework Proposal, Telework Agreement, and if appropriate, VA Form 0740b, Self-Certification Safety Checklist).

(3) The telework arrangement must not adversely affect VA's mission and functions. If, at any time, it is determined that an arrangement is having an adverse impact on work operations or performance, the supervisor or the employee may terminate the arrangement with two weeks notice. Supervisor modification or termination of the arrangement requires two weeks notice except where:

(a) otherwise specified in a collective bargaining agreement,

(b) work-related circumstances require otherwise, e.g., emergency situation,

(c) management determines that the teleworker is not meeting performance criteria,

(d) the employee breached information security protocol, or

(e) the employee works overtime without prior advanced approval.

e. **Automated Information System Security**. Each Administration and Staff Office with a telework program will ensure that Departmental information security policies, established by the Office of Information and Technology, are strictly enforced and that telework employees are informed that periodic remote computer surveillance may be conducted to ensure information security policy compliance. Each telecommuter will be assigned a VA-owned computer or agree to have the One VA-VPN software installed on their personal computers. Technical requirements for computer connections to the VA network by telecommuters will be published and issued by the CIO. Offices sponsoring telework must also ensure that adequate technological security protections are in place on all electronic devices issued to telework participants. If Federal and VA information security policies, procedures and guidelines are not followed, telework must be terminated. Prior notice to the employee is not required for enforcement and reporting of security violations. Additional security policy information and clarification can be obtained from the VA Office of Information and Technology, Office of Cyber and Information Security (005S). (See VA Directive 6210, Automated Information Systems Security, and VA Directive 6000, VA Information Resources Management Framework.).

f. **Security and Privacy Considerations.**

(1) No classified documents (hard copy or electronic), may be taken to, used, or stored at an employee's home office or telecenter. The employee must return to the traditional office to access and work on such documents or materials. Privacy Act materials and VA data and systems may be accessed remotely provided that the employee agrees to protect Government/VA records from unauthorized disclosure or damage. The employee must also comply with all legal requirements (for example, Privacy Act of 1974, 5 U.S.C. § 552a), policies and procedures (for example, VA Directive and Handbook 6210) identified by the Administration or Staff Office as necessary to protect the VA data and systems to which the employee will have access under the telework arrangement. Prior notice to the employee is not required to terminate telework arrangements due to security violations.

(2) If any legal requirements (for example, Privacy Act of 1974, 5 U.S.C. § 552a), departmental and office policies and procedures change (for example, VA Directive and Handbook 6210), the employee, upon proper notice, agrees to comply with the changed requirements. Failure to so agree constitutes a basis for termination of the employee's participation in the program.

g. **Telework Agreement.**

(1) Each teleworker, whether in a telecenter or a home-based office, must sign a telework agreement. The agreement covers the terms and conditions of participation in the telework program. The agreement is not a contract, but rather serves as a document that defines all expectations and parameters of the arrangement (see Appendix II-B for a sample agreement). At a minimum, the agreement must include:

(a) a preamble statement of voluntary participation;

(b) the identity of the signatories, duty station and alternative worksite;

(c) a description of the work schedule and tour of duty;

(d) a description of required equipment/supplies an explanation of the responsible provider;

(e) provisions describing requirements for leave, overtime, liability, work area (for work at home only), worksite inspection, alternative worksite costs, injury compensation, cancellation, privacy obligations, standards of conduct, and paragraph on appropriate disciplinary or adverse action; and

(f) parameters of work assignments to be performed as well as performance criteria.

(2) The telework agreement must be approved by the employee's immediate supervisor and appropriate approving official. Before approving agreements, supervisors and approving officials must determine the impact the telework arrangement will have on work operations.

(3) The completed agreement should be forwarded to the servicing human resources office and is to be used for administrative reporting purposes only (see paragraph 3.a). If the completed agreement is retrieved by individual identifiers such as the individual's name or social security number, then the provisions of the Privacy Act (PA) 5 U.S.C. § 552a will apply. If use of a satellite telecenter is approved, the Departmental Telework Coordinator, or other designee, will contact General Services Administration (GSA) to procure available space and initiate a written Interagency Agreement for services.

h. **Performance Evaluation.** The performance of an employee on a telework arrangement should be evaluated based on the applicable performance standards for his or her position or for that portion of the overall performance plan which applies. Supervisors and employees should fully discuss performance expectations in the initial phase of the process of establishing a telework arrangement to assure expectations are fully understood. Performance should be measured on achieved results. Periodic reviews between the supervisor and the employee are encouraged.

i. **Time and Attendance Accounting.** The employee's time and attendance will be recorded as performing official duties at the official duty station or alternative worksite, as applicable. To verify attendance at the alternative worksite, supervisors may periodically contact the employee and/or permit employee self-certification. To help ensure that employees on telework arrangements work as scheduled, supervisors should focus on the completion of work products as applicable.

j. **Work Schedule.** Based on work requirements, supervisors may arrange telework schedules to allow employees to work on a telework arrangement one day per pay period, one day per week, or as often as five days per week. Normally, the supervisor may change telework schedules only with notice to the employee in advance of the applicable administrative workweek. Work unit supervisors may also approve alternative work schedules for employees on telework arrangements when doing so is consistent with work requirements. Supervisor modification or termination of the arrangement requires two weeks notice except where:

(1) otherwise specified in a collective bargaining agreement,

(2) work-related circumstances require otherwise, e.g., emergency situation,

(3) management determines that the teleworker is not meeting performance criteria,

(4) the employee breached information security protocol, or

(5) the employee works overtime without prior advanced approval.

k. **Leave.** Current absence and leave policies and regulations apply to employees on telework arrangements.

l. **Emergency Closing/Group Dismissal.** On a day when an employee is scheduled to work at the Alternative Worksite and their official duty station facility is closed for all or part of a day, the following rules apply:

(1) Full Day Closing. The employee is not *required* to perform work at the ADS. However, if the employee *voluntarily* chooses to perform any work at the ADS, the employee is not entitled to additional compensation such as overtime, compensatory time, or credit hours.

(2) Late Openings. On a day when an employee is scheduled to work at the ADS and the employee's official duty station facility opens late, the employee is entitled to the exact amount of excused absence the employee would have received if scheduled to work at the official duty station. In this situation, the voluntary work provisions in Paragraph 1 of this Section apply.

(3) Late Arrivals and Early Dismissals. On days when a late arrival or early dismissal occurs, the employee is required to perform their full ADS schedule if located at home.

(4) On a case-by-case basis, an agency may excuse a telework employee from duty during an emergency if the emergency adversely affects the telework site (e.g., disruption of electricity, loss of heat, etc.).

m. **Ad Hoc Arrangements.** When management determines exigent circumstances exist (for example, an employee's sudden illness precluding work at the official duty station), management may institute an ad hoc telework arrangement without completion of required documentation. Ad hoc arrangements should only be instituted to assist employees and management in unforeseeable and unavoidable emergency circumstances, and to ensure improvement of services to veterans, increase productivity, recruit and retain personnel, and improve the quality of life of participants. After effecting an ad hoc arrangement, a telework agreement should be completed at the earliest possible opportunity.

n. **Pay.** All entitlements for pay, including locality based comparability pay, special salary rates, and travel benefits will be based on the employee's official duty station. Premium pay entitlements are not affected by a telework arrangement, including coverage under the Fair Labor Standards Act (FLSA), if applicable. *(Note: Employees covered by FLSA should be given explicit written instructions not to exceed daily and weekly overtime pay limits).* The premium pay provisions in VA Handbook 5007, Pay Administration, Chapter 2, Section 2, shall apply to hybrid title 38 employees who are being paid premium pay on the same basis as nurses.

o. **The Alternative Worksite.**

(1) The alternative worksite must be suited to conducting business. Before a work-at-home Telework Proposal and Work Agreement are approved, the employee must complete a VA Form 0740b, Telework Self-Certification Safety Checklist, and submit it to the immediate supervisor.

(2) The supervisor and employee should identify resources needed to facilitate the work assignment, assuring all property and equipment needs are satisfied in accordance with the telework agreement.

NOTE: GSA has developed a number of telework centers, commonly called telecenters, across the country and in the Washington, DC area. Information about the interagency agreement for renting space and billing procedures for use of telecenters can be obtained at the following Web site: http://www.gsa.TeleWork.gov.

p. **Expenses and Equipment**

(1) The Department may issue and/or pay for equipment, software, equipment maintenance, and repair based on the availability of funds and equipment. Work-at-home arrangements may require minimal equipment such as pen and paper; or they may require considerable equipment such as computers, modems, additional telephone lines, fax and copying machine(s), as well as, telecommunications for connectivity including high speed data communications, such as, cable modems, DSL or ISDN lines. The decision to purchase or provide Government issued equipment is discretionary on the part of management.

(2) When needed, the Department may pay expenses associated with working- at-home such as: pens, paper, phone charges (long-distance and other); and the cost of computers, typewriters, fax machines, computer software, modems, and equipment maintenance and repair. Employees will incur the costs of additional electrical outlets and telephone lines.

(3) Employees will incur the cost of utilities associated with working-at-home. In some limited situations, VA may pay for telephone installation when the service is considered essential and the employee agrees that the installed telephone will only be used for work assignments and contact with the VA office.

q. **Liability and Worker's Compensation.** Employees on telework arrangements are covered under the Federal Tort Claims Act and the Federal Employees' Compensation Act. As with injuries which occur in the traditional office setting, for injuries that occur during telework arrangements, supervisors may only attest to what they reasonably know. In all situations, employees are responsible for informing their immediate supervisor of an injury at the earliest time possible.

r. **Telework Coordinators and Teams.** It is recommended that each operating Administration and Staff Office designate a Telework Coordinator to implement, monitor, and track administration of their respective telework program(s). Telework teams may be formed at all levels of the organization to include human resources, information technology, and security to respond to the personnel, equipment, security, and other issues associated with telework arrangements.

7. EVALUATION. It is recommended that telework arrangements be evaluated periodically to determine the impact on work.

8. TERMINATION. The telework arrangement must meet the operational needs of the Department and VA's ability to accomplish its mission and functions. If not, the supervisor may terminate the arrangement after meeting any applicable notice requirements. For bargaining unit employees, termination is subject to applicable provisions of their collective bargaining agreements.

Since telework is a voluntary work arrangement, the employee may terminate it at any time with appropriate notice, at least 2 weeks. For bargaining unit employees, termination is subject to applicable provisions of their collective bargaining agreements.

APPENDIX A.
SAMPLE ALTERNATIVE WORKPLACE TELEWORK AGREEMENT

The following constitutes an agreement between the employer (VA approving official and organization) and employee (name, title, grade, and organization) to the terms and conditions of this alternative workplace arrangement. This is neither a contract nor intended to create any contractual obligations between the parties.

1. Voluntary Participation. The employee voluntarily agrees to work at the agency-approved alternative workplace indicated below and to follow all applicable policies and procedures. The employee recognizes the telework arrangement is not an employee benefit but an additional method the agency may approve to accomplish work.

2. Trial Period. The employee and management agree to try out the arrangement for at least (specify number) months unless unforeseen difficulties require earlier termination.

3. Salary and Benefits. Management agrees that a telework arrangement is not a basis for changing the employee's salary and benefits.

4. Duty Station and Alternative Worksite. The employee and management agree that the employee's official duty station is (list duty station for regular office) and that the employee's approved alternative worksite is (specify location, street address, etc.). The employee understands that all pay, leave, and travel entitlements are based on the official duty station. With reasonable notice to the employee, management has the right to change the days spent at the official duty station or alternative worksite.

5. Official Duties. The employee agrees to only perform official duties when on duty at the regular office or alternative worksite. The employee agrees not to conduct personal business while in official duty status at the alternative worksite, for example, caring for dependents.

6. Work Schedule and Tour of Duty. Management and the employee agree that the employee's official tour of duty will be (specify days, hours, and location).

7. Time and Attendance. The employee's supervisor will ensure that the employee's timekeeper has a copy of the employee's telework work schedule. The employee's time and attendance will be recorded as performing official duties at the official duty station or alternative worksite, as applicable.

8. Leave. The employee agrees to follow established office procedures for requesting and obtaining approval of leave.

9. Overtime. The employee agrees to work overtime only when ordered and approved by the supervisor in advance and understands that working overtime without such approval may result in termination of the telework arrangement and/or other disciplinary action.

10. Equipment/Supplies. The employee agrees to protect any government-owned equipment and to use it only for official purposes. Management agrees to install, service, and maintain any government-owned equipment issued to the telework employee. The employee agrees to install, service, and maintain any personal equipment used. Management agrees to provide the employee with necessary office supplies and to reimburse the employee for business-related long distance telephone calls. Management has the option to provide the employee with a government-issued calling card for business-related long distance calls.

11. Liability. The employee understands that the government will not be liable for damages to an employee's personal or real property while the employee is working at the approved alternative worksite except to the extent the government is held liable by the Federal Tort Claims Act or the Military Personnel and Civilian Employees Claims Act.

12. Work Area (work-at-home only). The employee agrees to provide a distraction-free worksite adequate for the performance of official duties, and sign the Self-Certification Safety checklist.

13. Worksite Inspection. The employee agrees to permit the government to inspect the alternative worksite during the employee's normal working hours to ensure proper maintenance of government-owned property and conformance with safety standards. The employer will give the employee reasonable notice of a planned inspection.

14. Alternative Worksite Costs. The employee agrees that the government will not be responsible for any operating costs that are associated with the employee using his or her home as an alternative worksite, for example, home maintenance or utilities. The employee understands that he or she does not relinquish any entitlement to reimbursement for authorized expenses incurred while performing official duties, as provided for by statute or regulation.

15. Injury Compensation. The employee understands that he or she is covered by the Federal Employees' Compensation Act if injured while performing official duties at the alternative worksite. The employee agrees to notify the supervisor immediately of any accident or injury that occurs at the alternative worksite and to complete any required forms.

16. Work Assignments/Performance. The employee agrees to complete all assigned work according to procedures mutually agreed upon by the employee and the supervisor. The employee's performance will be evaluated against standards contained in the employee's performance plan.

17. Cancellation. The employee may cancel participation in the telework arrangement at any time with appropriate notice, at least 2 weeks. Supervisor modification or termination of the arrangement requires 2 weeks notice except where (1) otherwise specified in a collective bargaining agreement, (2) work-related circumstances require otherwise, e.g. emergency situation, (3) management determines that the teleworker is not meeting performance criteria, (4) the employee breached information security protocol, or (5) the employee works overtime without prior advanced approval. The decision to cancel the telework arrangement is not subject to any formal appeal procedure; however, it may be grieved under applicable negotiated grievance procedures. Management agrees to allow the employee to resume his or her regular work schedule at the official duty station if the telework arrangement is canceled. Management agrees to follow any applicable negotiated procedures in canceling the arrangement.

18. Disclosure. The employee agrees to protect government/VA records from unauthorized disclosure or damage and will comply with the requirements of the Privacy Act of 1974, (5 U.S.C. § 552a), Federal privacy laws and regulations, and VA policies and procedures.

19. Standards of Conduct. The employee agrees that he or she is bound by VA standards of conduct while working at the alternative worksite.

20. Agreement. Nothing in this agreement precludes management from taking any appropriate disciplinary or adverse action against an employee who fails to comply with the provisions of the agreement.

_____ _____

Employee Date

_____ _____

Employer (title of Approving Official) Date

Department of Veterans Affairs

TELEWORK PROPOSAL

1 DATE PREPARED: 01/10/2005

IMPORTANT: For additional information, see VA Directive 5011, Chapter 4.

2 NAME OF EMPLOYEE (Last, First, Middle initial)	3 POSITION TITLE, SERIES, AND GRADE	4 NAME OF YOUR TELEWORK COORDINATOR
Davis, Breanna L	Program Analyst GS-345-14	Maxcine Sterling

5 NAME AND ADDRESS OF DUTY STATION	6 ORGANIZATION AND LOCATION	7 OFFICE PHONE NUMBER (Include area code)
16999 Indian Head Highway Upper Marlboro, Maryland 20772	Organizational Effectiveness 810 Vermont Ave NW Washington, DC 20420	(202)273-0099

8 WHAT IS YOUR CURRENT WORK SCHEDULE

☒ ALTERNATE WORK SCHEDULE (Eight 9-hour days, one 8-hour day and one day off) ☐ COMPRESSED WORK SCHEDULE (Four 10-hour days and one day off) ☐ FLEXITIME WORK SCHEDULE (Setting core work hours) ☐ REGULAR WORK SCHEDULE (Five 8-hour work days that has a fixed start and end time)

☐ PART-TIME WORK SCHEDULE ☐ OTHER WORK SCHEDULE (Explain)

9A ALTERNATE WORK SCHEDULE REQUESTED	9B ALTERNATE WORKSITE ADDRESS	9C ALTERNATE WORKSITE PHONE NUMBER (Include area code)
☒ WORK AT HOME (If checked, please complete VA Form 0740b) ☐ VIRTUAL OFFICE (Mobile) ☐ TELECENTER	16999 Indian Head Highway Upper Marlboro, Maryland 20772	(301) 952-0099

9D. TYPE OF ARRANGEMENT

☐ AD HOC ☐ TEMPORARY SCHEDULE ☒ REGULAR SCHEDULE

9E. NUMBER OF DAYS

☒ 1 DAY PER PAY PERIOD ☐ 2 TO THREE DAYS PER PAY PERIOD ☐ 4 OR MORE DAYS PER PAY PERIOD ☐ 5 OR MORE DAYS PER CALENDAR YEAR

9F. LENGTH OF TIME

☒ SIX MONTHS OR LESS ☐ SIX TO TWELVE MONTHS ☐ TWELVE MONTHS OR MORE

10 ANTICIPATED EQUIPMENT TO WORK OFF-SITE

☒ COMPUTER ☒ SOFTWARE ☒ CELL PHONE ☐ SECOND HOME PHONE LINE ☐ FAX MACHINE ☐ PRINTER

☐ FILE CABINET ☐ DESK AND CHAIR ☒ CALLING CARD ☐ TYPEWRITER ☐ OTHER (Identify)

11 ESTIMATED COST FOR TELEWORK ARRANGEMENT: $

12. LIST PROPOSED WORK SCHEDULE

	WEEK 1					WEEK 2				
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
HOURS	7:00-4:30	7:00-4:30	7:00-4:30	7:00-4:30	Off	7:00-4:30	7:00-4:30	7:00-4:30	7:00-4:30	7:00-4:30
LOCATION	VA	VA	VA	VA	CWS	VA	VA	VA	VA	Off-Site

EXAMPLE	WEEK 1					WEEK 2				
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
HOURS	7:00-4:30	7:00-4:30	7:00-4:30	7:00-3:30	OFF	7:00-4:30	7:00-4:30	7:00-4:30	7:00-4:30	7:00-4:30
LOCATION	OFF-SITE	OFF-SITE	OFF-SITE	VA	HOME	OFF-SITE	OFF-SITE	OFF-SITE	VA	VA

13 EXPLAIN HOW YOUR PROPOSED TELEWORK ARRANGEMENT WILL HELP YOU AND THE ORGANIZATION GET YOUR JOB DONE

Working from home will allow me to review regulations, legal precedents and decisions without interruptions. I will be able to concentrate on developing a sound basis for the Department's position. Requests for extensions should be significantly reduced.

14 WHAT POTENTIAL CHALLENGES WILL YOUR PROPOSED TELEWORK ARRANGEMENT POSSIBLY CREATE FOR YOUR CUSTOMERS (Internal/external to VA), CO WORKERS, SUPERVISOR, AND HOW DO YOU PLAN TO RESOLVE THEM?

None. e-mail capability from my home will allow me to respond to special requests, or emergency requests on an as needed basis. There will be no adverse impact to fellow co-workers and/or management, as I expect to be in the office 8 days out of 10 (with 1 off-site day at home and 1 CWS day). I have been assigned a cell phone which will allow for emergency calls.

VA FORM JUN 2003 (RS) **0740a**

AdobeFormsDesigner

15. DOES YOUR JOB INVOLVE CONFIDENTIAL OR SECURE FILES OR INFORMATION?

☐ YES (If "YES," see Supervisor for additional guidance.) ☒ NO

16. WHAT SPECIFIC PROJECTS AND/OR ASSIGNMENTS DO YOU PROPOSE TO ACCOMPLISH WHILE WORKING OFF-SITE, AND HOW WOULD YOU AND YOUR SUPERVISOR ASSESS ACCOMPLISHMENT OF IDENTIFIED ASSIGNMENTS/PROJECTS? *(Be specific and provide periods.)*

1. Review of the E-gov and impact to VA. This assignment is expected to take six to eight weeks for completion. Weekly progress reports will be provided.

2. Review of the new government-wide contracting regulations. This assignment will involve collaboration with outside agencies and will require approximately three months to complete. Start date is May 30.

3. Development of a departmental position paper on realignment and restructuring of SBA. Expected start date is 02/05; weekly updates will be provided.

COMPLETED BY SUPERVISOR

17A. ACTION OF SUPERVISOR

☒ APPROVED

☐ DISAPPROVED (Explain why)

☐ APPROVED WITH MODIFICATION

17B. COMMENTS OF SUPERVISOR

18. APPROVED EQUIPMENT TO TELEWORK

☒ COMPUTER ☒ SOFTWARE ☒ CELL PHONE ☐ SECOND HOME PHONE LINE ☐ FAX MACHINE ☐ PRINTER ☐ FILE CABINET

☐ DESK AND CHAIR ☒ CALLING CARD ☐ TYPEWRITER ☐ OTHER (Identify)

19. APPROVED DATES TO TELEWORK

BEGIN 03/10/05 END 09/15/05

NOTE: If employee work involves confidential or secured information, please check with security for more specific guidance/direction

20A. SIGNATURE OF SUPERVISOR	20B. DATE	21A. SIGNATURE OF EMPLOYEE	21B. DATE
John Stetlar	01/12/2005	Breanna K. Davis	01/10/2005
22A. SIGNATURE OF APPROVING OFFICIAL		22B. DATE	
J. A. Cooper		01/12/2005	

BACK OF VA FORM 0740e JUN 2003 (RS) AdobeFormsDesigner

Department of Veterans Affairs

TELEWORK SELF-CERTIFICATION SAFETY CHECKLIST
WORK-AT-HOME

1. NAME OF EMPLOYEE (Last, First, Middle Initial)	2. NAME OF YOUR TELEWORK COORDINATOR	
Davis, Breanna L.	Maxcine Sterling	
3. HOME ADDRESS (Street, city, state, and ZIP Code)	**4. OFFICIAL DUTY STATION ADDRESS (Street, city, state, and ZIP Code)**	**5. HOME OFFICE PHONE NUMBER**
16999 Indian Head Highway Upper Marlboro, Maryland 20772	810 Vermont Avenue NW Washington, DC 20420	(301) 932-0099 **6. OFFICE PHONE NUMBER** (202) 273-0010

The following checklist is designed to assess the overall safety of your home office. Please answer each question, sign and date. You should also have your supervisor sign and date after you have completed this form.

7A. OFFICE ENVIRONMENT	
1. Are temperature, noise, ventilation and lighting levels adequate for maintaining your normal level of job performance?	☒ YES ☐ NO
2. Are all stairs with four or more steps equipped with handrails?	☒ YES ☐ NO
3. Are all circuit breakers and/or fuses in the electrical panel labeled as to intended service?	☒ YES ☐ NO
4. Do circuit breakers clearly indicate if they are in the open or closed position?	☒ YES ☐ NO
5. Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires to the ceiling)?	☒ YES ☐ NO
6. Will the building's electrical system permit the grounding of electrical equipment?	☒ YES ☐ NO
7. Are aisles, doorways, and corners free of obstructions to permit visibility and movement?	☒ YES ☐ NO
8. Are file cabinets and storage closets arranged so drawers and doors do not open into walkways?	☒ YES ☐ NO
9. Do chairs have any loose casters (wheels) and are the rungs and legs of the chairs sturdy?	☒ YES ☐ NO
10. Are the phone lines, electrical cords, and extension wires secured under a desk or alongside a baseboard?	☒ YES ☐ NO
11. Is the office space neat, clean, and free of excessive amounts of combustibles?	☒ YES ☐ NO
12. Are floors surfaces clean, dry, level and free of warn or fray seams?	☒ YES ☐ NO
13. Are carpets well secured to the floor and free of frayed or warn seams?	☒ YES ☐ NO
14. Is there enough light for reading?	☒ YES ☐ NO
7B. COMPUTER WORKSTATION	
1. Is your chair adjustable?	☒ YES ☐ NO
2. Do you know how to adjust your chair?	☒ YES ☐ NO
3. Is your back adequately supported by a backrest?	☒ YES ☐ NO
4. Are your feet on the floor or fully supported by a footrest?	☒ YES ☐ NO
5. Are you satisfied with the placement of your VDT and keyboard?	☒ YES ☐ NO
6. Is it easy to read the text on your screen?	☒ YES ☐ NO
7. Do you need a document holder?	☒ YES ☐ NO
8. Do you have enough leg room at your desk?	☒ YES ☐ NO
9. Is the VDT screen free from noticeable glare?	☒ YES ☐ NO
10. Is the top of the VDT screen eye level?	☒ YES ☐ NO
11. Is there space to rest the arms while not keying?	☒ YES ☐ NO
12. When keying, are your forearms close to parallel with the floor?	☒ YES ☐ NO
13. Are your wrists fairly straight when keying?	☒ YES ☐ NO

8A. SIGNATURE OF EMPLOYEE	8B. DATE	9A. SIGNATURE OF IMMEDIATE SUPERVISOR	9B. DATE
Breanna L. Davis	01/10/2005	John Stettler	01/12/2005

VA FORM JAN 2003 **0740b**

AdobeFormsDesigner

Questions for the Record
The Honorable Lane Evans
Ranking Democratic Member
House Committee on Veterans' Affairs

May 25, 2006

"Oversight hearing on the recent theft of sensitive information belonging to as many as *26.5* million veterans and spouses from a VA employee's home"

Question 1: The VA memo dated May *5,* 2006, detailing the data potentially stored on the stolen personal equipment referred to a VHA data base that was involved. Describe the contents of that VHA database.

Response: The Department of Veterans Affairs (VA) Office of Inspector General issued a report on July 11, 2006, entitled, "Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans." In regard to the referenced Veterans Health Administration (VHA) database that was involved, the report states on page 8 that one of the six files on the stolen external drive included, "A file extracted from both the VHA national enrollment data file and the compensation and pension file. The file represented the population from which some veterans were sampled during the [National Survey of Veterans] (other veterans were selected based on random telephone dialing.) According to the employee, the file contained over 5.5 million records, containing the veteran's address, date of birth, claim number, combined degree of disability, enrollment priority, social security number, and telephone number."

The VHA national enrollment database is used to manage VHA's national health care enrollment system as well as for reporting of enrollment related data for a variety of internal and external reporting purposes. The database includes demographic and eligibility related data required for the administration of the enrollment system.

Question 2: VA records are accorded a sensitivity level from 0 to 9 relative to each individual record maintained in VA databases. It is our understanding that sensitive records must be manually screened during batch downloads. Did this screening occur during the batch download of any segment of the potentially compromised files? If so, what sensitivity level was that threshold set? Who performed the manual screening and how was this action verified? How many sensitivity level "9" records were potentially part of the compromised data?

Response: The Veterans Benefit Administration (VBA) has a formal process for individuals to request data extracts from VBA information systems. The data extract must be authorized by the appropriate individual from the VBA business unit, who is designated as the system of record owner under the Privacy Act. There is no requirement to execute a screening of sensitive records as part of the extract request. There were 159 sensitive level "9" records on the file of compromised data.

Question 3: Provide a copy of all proposals to modify what is now referred to as VA Directive 6500 since 1996. Provide coordination documentation and the rationale for each proposed modification's acceptance or refusal.

Response:

- Directive 6210, "Automated Information Systems Security," was the official Cyber Security policy document in 1997.

- Directive 6500, "Information Security Program," was to replace Directive 6210. Directive 6500 was approved by all necessary officials within VA and submitted for printing and distribution in June 2002. However, the Associate Deputy Assistant Secretary for Cyber and Information Security at the time elected to revise the document before it was printed and distributed.

- A revised version of Directive 6500 was sent out for comments and concurrence in December 2003. Comments and requested changes were received up until July 2005. These changes were made and in April 2006 a revised version of Directive 6500 was dispatched for internal review and comment within the Office of Information and Technology. Internal concurrence was received, and the revised version of Directive 6500 was published August 4, 2006.

Attached are copies of all proposed revisions of VA Directive 6500, along with documentation from offices that disagreed with the modifications.

The Honorable Luis V. Gutierrez

Question 1: Secretary Nicholson, it has been reported that the VA informed the Inspector General of the robbery shortly after it occurred, but many news outlets stated both the VA and the IG withheld this information from the FBI until late last week. Who's idea was *it* to keep this out of hands of the Department of Justice? Could have the IG notified the FBI themselves? If so, why did the IG wait so long to get law enforcement involved?

Response: The theft occurred on May 3rd and local law enforcement was notified immediately. On May 10th while attending a VA Information Security Officer's meeting, an information security officer of the Office of Inspector General (OIG) learned that an employee's home had been burglarized and that VA electronic records may have been stolen. On May 11th that information security officer submitted a written report to alert the Office of Investigations within the OIG. On May 12th OIG opened a criminal investigation; the OIG was unable to interview the employee until May 15th. It was during this interview that the OIG became more fully aware of the extendt of the situation. On May 16th the OIG meet with local law enforcement, and informed them of the suspected loss of veteran's personal information. On May 17th OIG advised the Federal Bureau of Investigation (FBI) and a full-scale investigation into this matter was launched. Law enforcement agencies reported on June 29th that the lap top and hard drive had been recovered.

Question 2: In some states, consumers can freeze access to their credit reports for a fee. If veterans choose to have a freeze on their reports, is the VA willing to reimburse veterans for the costs of doing so? Will Congress seek a supplemental appropriation request from the Administration to cover these costs?

Response: As the stolen equipment has been recovered and the FBI is highly confident the data were not accessed or otherwise compromised, the Administration has withdrawn its request for supplemental appropriation to cover the cost of credit-protection services for the identified individuals.

To date, and with the help of Congress, VA has reprogrammed up to $25 million to establish and operate a call center for veterans. In addition, VA has conducted a mass mailing to notify as many veterans as possible of the potential compromise of their personal data. A total of $7 million to cover the cost of this mailing was funded within existing resources by adjusting our priorities in our General Operating Expenses account.

Question 3: Mr. Secretary, the Inspector General has stated in his testimony that the data analyst has been taking home veterans' personal information on a routine basis since 2003. How many other VA employees are taking home the personal information of veterans on a routine basis? This analyst is said to have just had the names, social security numbers and dates of birth of veterans with him, but are employees taking home the medical and financial records of veterans? If so, how often is this happening and what do you intend to do to stop the open door policy on our nation's veterans' personal information.

Response: VA is working diligently to ensure that veteran's personal information is secure 24 hours a day, 7 days a week. VA has worked just as hard to balance the security of this information and to enable VA's workload to progress smoothly, uninterrupted and remain veteran focused. In order to strengthen security policy and procedures, on June 2006, the Secretary of Veterans Affairs issued Directive 6504 "Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities." The Directive establishes policy and responsibilities for VA employees' and applies to all VA organizational elements. It describes required security measures for mobile or fixed computers, other electronic and storage media used to transmit, transport, process, store, or access information or connect to VA information technology systems from home, on travel, or at alternative work locations. It also restricts the use of VA data stored in non-electronic from outside the regular work site.

VA employees are permitted to transport, transmit, access and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor and where appropriate security measures are taken to ensure that VA information and services are not compromised. The privilege to use or access VA data outside VA facilities may be revoked or limited at any time by appropriate VA officials.

Only VA-owned government furnished equipment, including laptops and handheld computers, may be used when accessing the VA intranet remotely. VA employees may not use non-VA owned equipment to access the VA intranet remotely or to process VA Protected Information (VAPI) except as specifically provided in the Directive. VAPI is sensitive information as defined in paragraph 5 titled "Definitions." Access to the VA intranet using non-VA owned equipment will be provided via approved VA Virtual Private Network (VPN) access protocols which will offer access to a limited set of VA applications and services. Only remote access users with VAGFE will be permitted to connect to the VPN in such a way that grants full VA access provided all required security software is installed and updated.

Employees must request and obtain supervisory approval for remote access to the VA intranet. The employee or supervisor may apply for a remote access account through the Information Security Officer (ISO).

On May 26, 2006, the Secretary of Veterans Affairs issued a memorandum directing all employees to sign a "Statement of Commitment and Understanding" confirming their understanding of the training, the consequences for non-compliance, and their commitment to protecting sensitive and confidential information in the Department. The statement committed to safeguarding the personal information that veterans and their families have entrusted to the Department.

Employees were instructed to contact their local Privacy Officer, Freedom of Information Act Officer, Information Security Officer, or Regional or General Counsel representative when unsure whether or how they may gather or create, maintain, use, disclose or dispose of information about veterans and their families, and VA employees and applicants.

Failure to comply with applicable confidentiality statutes and regulations subjects employees to civil and criminal penalties, including fines and imprisonment. VA may also impose administrative sanctions, up to and including removal, for violation of applicable confidentiality and security statutes, regulations and policies.

Question 4: Mr. Secretary, we have yet to see any evidence that this information has led to identity theft, and I hope that we never do. But what steps are being taken at the VA to assist veterans who may become victims of identity theft due to this breach of information?

Response: The FBI has completed its forensic test on the recovered equipment. FBI has concluded with a "high degree of confidence" that the VA information had not been accessed or copied between the dates of the theft of the equipment and the date of its recovery. VA has worked with Congress, the news media, veterans' service organizations, and other government agencies to help ensure that veterans and their families were aware of the situation and of the steps they may take to protect themselves from the unauthorized use of their personal information. VA sent out individual notification letters to veterans. VA briefed the Attorney General and the

Chairman of the Federal Trade Commission, co-chairs of the President's Identity Theft Task Force. Task Force members took actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans received the free credit report they are entitled to under the law.