

# HEARING III ON INFORMATION TECHNOLOGY

---

---

**HEARING**  
BEFORE THE  
SUBCOMMITTEE OVERSIGHT AND INVESTIGATIONS  
OF THE  
COMMITTEE ON VETERANS' AFFAIRS  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED SEVENTH CONGRESS  
FIRST SESSION

APRIL 4, 2001

Printed for the use of the Committee on Veterans' Affairs

**Serial No. 107-5**



U.S. GOVERNMENT PRINTING OFFICE  
WASHINGTON : 2001

## COMMITTEE ON VETERANS' AFFAIRS

CHRISTOPHER H. SMITH, *New Jersey, Chairman*

BOB STUMP, Arizona	LANE EVANS, Illinois
MICHAEL BILIRAKIS, Florida	BOB FILNER, California
FLOYD SPENCE, South Carolina	LUIS V. GUTIERREZ, Illinois
TERRY EVERETT, Alabama	CORRINE BROWN, Florida
STEPHEN E. BUYER, Indiana	COLLIN C. PETERSON, Minnesota
JACK QUINN, New York	JULIA CARSON, Indiana
CLIFF STEARNS, Florida	SILVESTRE REYES, Texas
JERRY MORAN, Kansas	VIC SNYDER, Arkansas
J.D. HAYWORTH, Arizona	CIRO D. RODRIGUEZ, Texas
HOWARD P. (BUCK) MCKEON, California	RONNIE SHOWS, Mississippi
JIM GIBBONS, Nevada	SHELLEY BERKLEY, Nevada
MICHAEL K. SIMPSON, Idaho	BARON P. HILL, Indiana
RICHARD H. BAKER, Louisiana	TOM UDALL, New Mexico
ROB SIMMONS, Connecticut	
ANDER CRENSHAW, Florida	
HENRY E. BROWN, Jr., South Carolina	

PATRICK E. RYAN, *Chief Counsel and Staff Director*

---

## SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

STEPHEN E. BUYER, *Indiana, Chairman*

BOB STUMP, Arizona	VIC SNYDER, Arkansas
MICHAEL BILIRAKIS, Florida	BARON P. HILL, Indiana
TERRY EVERETT, Alabama	TOM UDALL, New Mexico

# CONTENTS

## OPENING STATEMENTS

	Page
Chairman Buyer .....	1
Hon. Vic Snyder .....	2
Hon. Terry Everett .....	3
Prepared statement of Congressman Everett .....	31
Hon. Tom Udall .....	11
Prepared statement of Congressman Udall .....	32

## WITNESSES

Brandt, Ken, Managing Director, Tiger Testing .....	15
Prepared statement of Mr. Brandt .....	79
Griffin, Richard J., Inspector General, Department of Veterans Affairs; accompanied by Michael Slachta, Jr., Assistant Inspector General for Auditing, Office of the Inspector General, Department of Veterans Affairs .....	3
Prepared statement of Mr. Griffin .....	35
McClure, David L., Director, Information Technology Management Issues, U.S. General Accounting Office; accompanied by Valerie C. Melvin, Assistant Director, Information Technology Management Issues, U.S. General Accounting Office .....	5
Prepared statement of Dr. McClure .....	40
Principi, Hon. Anthony J., Secretary, Department of Veterans Affairs; accompanied by Guy McMichael, Acting Assistant Secretary for Information Technology, Department of Veterans Affairs; Thomas L. Garthwaite, Under Secretary, Veterans Health Administration, Department of Veterans Affairs; Joseph Thompson, Under Secretary, Veterans Benefits Administration, Department of Veterans Affairs; and Roger R. Rapp, Acting Under Secretary, National Cemetery Administration, Department of Veterans Affairs .....	22
Prepared statement of Secretary Principi .....	89
Sherman, Scott C., Director, Advanced Technology Architectures, EMC <sup>2</sup> Corporation .....	16
Prepared statement of Mr. Sherman .....	85
Ware, Karl, Executive Vice President of Operations, Bionetrix Systems Corporation .....	13
Prepared statement of Mr. Ware .....	69

## MATERIAL SUBMITTED FOR THE RECORD

Cover page of GAO documents, entire report retained in committee files:	
“Maximizing the Success of Chief Information Officers” .....	66
“Information Security Management” .....	67
“Information Security Risk Assessment” .....	68
Statement of Majority Leader Richard Arney .....	33
Written committee questions and their responses:	
Chairman Buyer to Department of Veterans Affairs .....	93
Congressman Snyder to Department of Veterans Affairs .....	100
Chairman Buyer to Richard Griffin, Inspector General, Department of Veterans Affairs .....	106
Chairman Buyer to General Accounting Office .....	109



# HEARING III ON INFORMATION TECHNOLOGY

WEDNESDAY, APRIL 4, 2001

U.S. HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,  
COMMITTEE ON VETERANS' AFFAIRS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10 a.m. in room 334, Cannon House Office Building, Hon. Steve Buyer (chairman of the subcommittee) presiding.

Present: Representatives Buyer, Everett, Snyder, and Udall.

## OPENING STATEMENT OF CHAIRMAN BUYER

Mr. BUYER. This hearing of the Subcommittee on Oversight and Investigations of the U.S. House of Representatives Committee on Veterans' Affairs will come to order.

This subcommittee will conduct a third hearing to follow up on the Department of Veterans Affairs' information technology programs. The VA's IT budget is \$1.4 billion this year and has been close to a billion dollars per year for the last 10 years. Our hearing will focus on the VA's progress in addressing computer security, VA's efforts to develop a department-wide data architecture, and the VA's computer systems, known as VHA's decision support system, DSS, and VBA's VETSNET compensation and payment system.

We will hear testimony from representatives of the General Accounting Office, the VA Inspector General's Office, the private sector and the Secretary of the VA. We also had solicited a statement from the House Majority Leader, Mr. Armey. He could not be here to provide testimony today, he has a conflict, and his statement will be submitted for the record.

[The statement of Hon. Richard Armey appears on p. 33.]

Mr. BUYER. I believe the subcommittee is again taking on an issue that is extremely serious. The current department-wide information security weaknesses were revealed in previous and updated GAO and VA IG reviews. Last September, this subcommittee, then chaired by Terry Everett, took these issues, and the subcommittee quotes from that hearing. The GAO report stated, "these weaknesses place critical VA operations, such as financial management, health care delivery, benefits payments, life insurance services, and home mortgage loan guaranties, and the assets associated with these operations, at risk of misuse and disruption. In addition, the sensitive information contained in the VA's systems, including financial transaction data and personal information on veterans' medical records and benefit payments, is vulnerable to inadvertent

or deliberate misuse, fraudulent use, improper disclosure or destruction, possibly occurring without any detection.”

Unfortunately, I think the IG’s testimony then, and again today—I read your testimony last night—shows how prophetic these words were in 1998 and again today. The Department’s past history in selecting and managing department-wide IT projects has been extremely poor and provided little to show in terms of improved delivery of more timely and quality service to veterans—and, I believe, has been a poor return on investment for the U.S. taxpayer.

This subcommittee would like to know why the VA continues to see itself as three separate administrations when it re-engineers its business processes as a department. Today’s testimony will show that the VA has still not defined its integrated IT systems architecture, even after the subcommittee requested the VA provide an integrated plan last May that includes actual milestone dates for completion of the most essential foundation for the department. That request is now almost one year old.

We will also hear what progress the Veterans’ Health Administration has made in utilization of its \$261 million decision support system. Last September, the GAO testified that 59 out of 140 medical centers had not or could not provide information on their utilization of DSS. Perhaps today we will also find out how much longer VBA’s decade-old modernization project, VETSNET, is going to take, and what it is finally going to do to improve services to veterans.

We have a pretty full agenda today, and hopefully we are not going to be interrupted by votes. But let’s not count on that. And so we will try to proceed as quickly as we possibly can.

I am pleased that Dr. Snyder is the ranking member of the O&I subcommittee. Both of us have worked very well over the years, not only here on the Veterans’ Affairs Committee, but on our service together on the Armed Services Committee, and his insights, his medical knowledge, especially in the arenas of medical privacy, are welcome on this subcommittee. And I yield to the gentleman for any opening comments he may have.

#### **OPENING STATEMENT OF HON. VIC SNYDER**

Dr. SNYDER. Thank you, Mr. Chairman. I appreciate your kind words and look forward to working with you on this committee, also.

I also read through your statement, Mr. Griffin. I read it through this morning—I couldn’t stay up late last night—and it is concerning. I think it is the kind of information that doesn’t mean much, and shouldn’t mean much, to most veterans. And yet I had the experience the other day, and I am sure everybody on this committee has had at some point, of sending out a copy of medical records to one of our veterans from the St. Louis fire. And you know, we had xerox copies, and you could still see the burn marks, half-pages, missing pages.

Well, I am sure there wasn’t a whole lot of focus on fire prevention at records centers in the past. And hopefully we are getting ahead of this by having this kind of hearing today that will per-

haps tell us where we are at on these very important issues of safeguarding records and information in the system.

Thank you for being here.

Mr. BUYER. Mr. Everett.

Mr. EVERETT. Thank you, Mr. Chairman. I don't have a statement prepared; I will submit one for the record. I just want to congratulate you on taking over this subcommittee. You are known for your mild but probing insights and questions. And Dr. Snyder, both of you are veterans of this committee, and I look forward to working with you. Thank you.

Mr. BUYER. Thank you. I will now recognize our first panel. Mr. Griffin, from the IG, will you please introduce who is accompanying you here today before you begin?

Mr. GRIFFIN. With me today is Assistant Inspector General Michael Slachta, who is in charge of our audit group, which does our IT oversight work.

Mr. BUYER. And you have two other witnesses with you?

Mr. GRIFFIN. Dr. McClure from GAO will be testifying from GAO's perspective.

Mr. BUYER. Ah, I am sorry. I didn't squint ahead. Go ahead, Mr. Griffin.

**STATEMENTS OF RICHARD J. GRIFFIN, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MICHAEL SLACHTA, JR., ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS; AND DAVID L. MCCLURE, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY VALERIE C. MELVIN, ASSISTANT DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE**

**STATEMENT OF RICHARD J. GRIFFIN**

Mr. GRIFFIN. Mr. Chairman and members of the subcommittee, I am here today to report on our current assessment of the Department of Veterans Affairs Automated Information System security program. Our evaluation is based on the following initiatives: a national audit of the information security in VA; the annual audit of VA's consolidated financial statements; and our Combined Assessment Program reviews of VA facilities.

Since our September 21, 2000, testimony to this subcommittee, we continue to identify significant information security vulnerabilities that place the Department's data systems at risk of unauthorized access and disclosure.

During the course of our national information security audit, we notified the Department of our review results so that prompt corrective actions could be taken to address the vulnerabilities identified. Unfortunately, a number of the identified vulnerability areas had been previously reported to the VA and continue to exist in violation of VA policy.

Audit results indicate that the Department has prepared a comprehensive plan for department-wide improvement of information security, but much work remains to be done to implement nec-

essary security enhancements. The Department's information security plan included unacceptably long timelines for addressing the following key security vulnerabilities: first, staffing qualified Information Security Officers; second, implementing department-wide intrusion detection; third, deploying a department-wide antivirus program; and finally, upgrading to VA-standard external electronic connections. At our request, the Acting Assistant Secretary agreed to amend the plan with accelerated implementation actions in these areas.

Vulnerabilities to unauthorized access and misuse of sensitive automated information and data need to be addressed. We found that many of these vulnerabilities exist in violation of VA policy. Examples of serious vulnerabilities identified included inadequate user identifications and passwords; program patches not installed; workstation access not restricted; use of active modems that can circumvent network security; and use of remote access software.

Other vulnerabilities identified include lack of centralized information security oversight and control over VACO Network operations. Desktop computers used in VA's automated systems should meet minimum acceptable security standards. Physical security weaknesses continue to place the Department's data center operations at VACO and the Austin Automation Center at risk.

VA facility responses to our information security survey identified significant weakness in the following areas: inadequate password management and controls; information security officer positions not fully staffed; IT contingency planning not completed; security risk assessments not completed; security incidents not reported to the Critical Information Response Capability Team; and finally, the operating of uncertified, independent Internet gateways.

Computer security implications from the fiscal year 2000 Consolidated Financial Statements Audit included weaknesses in application program change controls and operating system change controls at certain data centers and at selected medical centers. Weaknesses included inappropriate access capabilities by application programmers and system support staff to production data, lack of application change procedures, inadequate procedures for testing, approving and migrating system software changes, and inadequate application program change tracking procedures.

Since our September 21, 2000, testimony before the subcommittee, our Combined Assessment Program reviews completed at facilities this year have again identified the following key security control weaknesses: full-time security officer positions had not been established; strong password controls had not been implemented; user access levels needed to reflect current access requirements; physical security of computer room and equipment needed to be strengthened; annual security awareness training had not been provided; and facility information system risk assessment and contingency plans needed to be developed.

Given the serious nature of VA's information security weaknesses, computer security should continue to be identified as a departmental material weakness under the FMFIA. However, we believe that with more effective security management, oversight, and control over its systems and data, the Department would have the opportunity to enhance its security posture and move toward cor-

rection of this material weakness. A key step in this process would be the expeditious appointment of a Department-level Chief Information Officer to provide necessary leadership and direction over VA's information security program.

This concludes my testimony. Mr. Slachta and I will be pleased to answer any questions that you and the members of the subcommittee may have.

[The prepared statement of Mr. Griffin appears on p. 35.]

Mr. BUYER. Thank you very much. Dr. McClure.

#### **STATEMENT OF DAVID L. MCCLURE**

Dr. MCCLURE. Thank you, Mr. Chairman. It is a pleasure to be here. With me this morning is my Assistant Director for VA Audits, Valerie Melvin. We are pleased to be here to testify in front of you today on the work that we have been doing lately for the committee.

We have five areas that we want to cover, and I thought I would briefly go over them. First, as you know, the appointment of a Chief Information Officer at VA is long overdue. Secretary Principi has clearly indicated that filling the Assistant Secretary for Information and Technology is one of his top priorities. We welcome that, and we know that he has an executive team of advisors doing a thorough candidate search as we speak.

A recently issued report on factors that influence the success of chief information officers is a telling document on the characteristics of CIOs in organizations both public and private that are successful. It points out many characteristics that are associated with successful outcomes in both public and private organizations. We examined Fortune 500 firms, as well as several leading state organizations.

Three compelling factors are associated with the selection of a good chief information officer. First, executive-level support and commitment; knowing what you want the chief information officer to do, and having the role's responsibilities and authorities clearly defined and established. Secondly, positioning that person for success is also critically important, so that the individual occupying that position has other executive-level support throughout the organization that he or she is serving. And lastly, good chief information officers structure their organizations to meet business needs and staff it with appropriate talent. There are many examples in the product that we issued in February.

Even with these fundamental kinds of characteristics in place, the placement of a CIO at VA will be a challenge for anyone, because of the highly decentralized environment in which IT is administered. As you mentioned, the VA IT budget is \$1.4 billion, and most of that is in the component organizations.

Let me turn to information security. As VA continues to expand its services to veterans over the Internet, it will be faced with ensuring the privacy of sensitive records containing personal information. We again have issued a couple of reports that are very important and accepted government-wide on risk assessment approaches to security, and are embodied in a lot of the approaches that the federal CIO council has endorsed. And VA, again, is following many of these practices.

We found since September that VA has taken some constructive steps in the area of computer security. They have established a department-level information security plan. They have hired an executive-level person for a position to head the security office. And they have finalized several actions in their framework, both short-term and long-term in nature, that are focused on some of the vulnerabilities that the Inspector General has pointed out.

Despite those positive steps, there are many other actions that the department has not taken to ensure that it has a comprehensive, integrated computer security framework in place. For example, VA has not adequately defined steps for ensuring risk identification and categorization. VA has not performed risk assessments on a continuing basis, or when significant changes occur in its environment. And they are not routinely analyzing or taking action on security incidents. Even though an incident response system is in place, we are not confident that the information from that system is being thoroughly used.

Also, the VA has a central security management group that is not performing functions that it should be, including performing adequate monitoring and oversight of the computer security testing in the component organizations.

As part of our security update, we also looked at VA's compliance with privacy policies. And I have good news to report, in that visiting a handful of VA websites we saw strong compliance with OMB's Internet privacy policies—being posted, clear guidance, clear instructions on how information on the site was being used, and if information was being collected how it was being used.

The one thing we did discover in the case of two website visits were the collection of cookies, Internet cookies, which are small strings of text which simply identify a user once they return to the website, for navigation purposes, customization, and to track where you are going. We have notified VA of that. They have said they have taken action to remove those cookies.

Let me turn to the investment management process at VA. This is the cornerstone, really, of the decision making process for their investments. Again, there are many positive things to report in VA's CIB process, their investment and capital planning process. They have strengthened it with better guidance. They have put in place many of the guidelines that we and OMB have established.

But unfortunately, we found that some of the most principal components of the investment process were not being followed: in-process reviews, quarterly execution reviews, and post-implementation reviews—none of which have been conducted since September, our last testimony. Several are planned, but none conducted. In an organization that is spending at the rate of \$1.4 billion on IT annually, we would expect to see in-process reviews and post-implementation reviews being conducted for great lessons learned on how to repeat success and how to avoid failure.

We have also looked at a couple of systems that you have expressed interest in, the decision support system (DSS) and VBA's compensation and pension replacement. As you know, the DSS system has been used with mixed reaction in both the centers and in the VISNs. What we ended up doing was actually going back and following up on some of our prior work. And we see progress in the

acceptance of DSS. Twenty-one of the 22 VISNs now report using it. Three of the four VISNs that we had previously visited that were not using it provided us with examples of reports and data they were collecting that supported their use of it. So it is, again, better than the last time we were here.

Last September we also reported that 59 out of the 140 medical centers had not provided examples of DSS use. We did not specifically follow up on the medical centers, but we went to both Long Beach and Portland, who are heavy users of DSS, and again, were provided compelling examples of how data out of DSS were being used for resource allocation and other clinical decision making.

In the case of the compensation and pension replacement system, we have again some good news and some bad news. There are some really strong steps that have been taken for the overall program management of the C&P replacement system. But it is plagued with some of the same problems that we have seen in the past. There is not an integrated project plan with schedules and milestones for specific deliveries. And we are somewhat troubled by the limited nature of the pilot test that was conducted; only ten claims being processed. With a system that is expected to be processing 3.2 million claims a month, that is probably not an adequate pilot to justify full-scale operational roll-out.

So in short, Mr. Chairman, the VA is making progress on several fronts. We are glad to report that. But again, there are still some fundamental weaknesses across these areas that deserve the attention of the Secretary, and certainly the attention of the new CIO.

Thanks. I will be glad to answer any of your questions.

[The prepared statement of Dr. McClure appears on p. 40.]

Mr. BUYER. Mr. Griffin and Dr. McClure, your written testimony will be submitted into the record. And Dr. McClure, you made reference to three different documents. I would like for you to give me the title of both of them, along with the month and date, and submit all three of these for the record.

Dr. MCCLURE. I would be happy to do that, Mr. Chairman.

Mr. BUYER. Would you please state it right now?

Dr. MCCLURE. The first one is on "Maximizing the Success of Chief Information Officers," published in February 2001.

Mr. BUYER. It will be entered in the record.

Dr. MCCLURE. The second is "Executive Guide on Information Security Management," issued in May 1998.

Mr. BUYER. It will be entered in the record.

Dr. MCCLURE. And the last is "Information Security Risk Assessment: Practices of Leading Organizations," issued in November 1999.

Mr. BUYER. And it will be entered into the record.

[The material is retained in committee files.]

Mr. BUYER. The subcommittee will take a short recess for a vote and return.

[Recess.]

Mr. BUYER. The subcommittee will come back to order.

Mr. Griffin and Dr. McClure, I would like to personally thank you and your staff for the hard work that you have done in this area. Dr. Snyder and I have chosen to continue to work from former Chairman Terry Everett because of a great concern we

have. And we, as a Congress, are taking on these privacy issues. As you know, the Clinton administration issued a lot of medical privacy issues. And those of us on the Energy and Commerce Committee, in particular the Health Subcommittee and the Trade Subcommittee, are taking a re-look, as well as the Secretary of Health and Human Services. So the issues of medical privacy are at the forefront. And so I want to thank you for your hard work. We are going to continue our oversight on the issue.

Mr. Griffin, I understand you recently briefed Mr. Young, the Chairman of the House Appropriations Committee, on your work with the \$1.2 million fraud case in St. Petersburg, FL, and in Manhattan, NY. Would you please refresh the subcommittee, were there vulnerable computer security issues that allowed this fraud to be perpetrated?

Mr. GRIFFIN. In the instance of the case in New York, which involved about \$600,000 worth of fraud, the employee at that time created a fictitious veteran and caused electronic funds transfers to be made to a bank account which he had established. These payments went on for a number of years, accumulating the \$600,000 value.

In St. Petersburg, again, an employee sent benefit payments to her fiancé, in the amount of \$620,000. There were some IT issues identified, including people walking away from their terminals without disabling them, potentially allowing someone else to come in and take action on claims without the proper authority.

Mr. BUYER. How about the recent indictment of a VBA employee at the Houston regional office? Were these same computer vulnerability issues identified there as they were in St. Petersburg?

Mr. GRIFFIN. That case was identified through the work of a unit that the Department has, which is assigned in Austin, TX, at the Automation Center. It is the Financial Systems and Quality Assurance Service, which was doing some computer matching after we had established some of these Areas of vulnerability.

The circumstances did involve another fictitious veteran. The employee and her co-conspirator, who was her ex-common-law husband, were both indicted and were charged with 26 counts of mail fraud, wire fraud, conspiracy and theft. It is a pending prosecution, so there is not a lot of specific information to be discussed at this point concerning the investigation. However, the issues from the St. Petersburg audit concerning multiple authorities existing in individual employees allowed the employee in Houston to perpetrate this crime.

Mr. BUYER. Both of you have provided, not only in your oral but your written testimony, about the vulnerability and the weaknesses of the security systems within the VA. I am asking for your professional opinions: in your advice to a new Secretary, what would be the priorities that he should take on, here, within the first 6 months? How do we correct this and make it right?

Mr. GRIFFIN. I know that the Secretary is well aware of the problem at this point. There is obviously a need to get the Chief Information Officer in place, as we indicated in our testimony. Then it is a matter of giving that person the authority and the accountability to make this program work. I think that when you have the type of decentralization and the stove-piping that exists in the de-

partment—if there isn't one person who has ultimate authority over the entire operation, you will continue to have an accountability problem. So I think you need a strong leader who has authority across all administrations for this particular area.

Dr. MCCLURE. Mr. Chairman, there are several priorities that I would suggest. Number one, I would make sure that I would revisit the risk assessments that have been done, be very comfortable with those, that they were done with adequate guidance and understanding as to the true vulnerabilities that the business lines of VA are threatened by.

Two, I would really focus on testing, and testing of controls. This is a recurring weakness at VA. It needs constant attention, so that we can understand better what the real vulnerabilities are and risks are as they are happening. VA has put in an incident tracking system, but as I mentioned in my statement, we are not convinced that anything is truly being done with the information coming from that. And in this environment that we are in today, you have to monitor your systems real-time, and be able to take corrective action quickly. And I believe that the incident response system deserves a great deal of attention in this environment.

And lastly, I think I would probably focus on the central information security management group, and looking at what role and value that group is bringing, add to that function if necessary to ensure there is monitoring and validation of these very issues that we have brought up with you today occurring at the component level in VA. Security has to be administered at the business level, but someone certainly should be ensuring that it is being done, and that the results are validated so that we can have confidence that the systems are secure.

Mr. BUYER. Thank you. I yield to Dr. Snyder.

Dr. SNYDER. Thank you, Mr. Chairman. Mr. Griffin, in your written statement you have a comment here where you say, "not all the department's operating elements have responded to our review findings," but those that did were positive about what you had to say. What does that mean, they haven't responded? I mean, are there people out there that you sent a copy of the report to and said, please respond to this, and they just flat-out didn't send you anything back?

Mr. GRIFFIN. That is right.

Dr. SNYDER. Well, that seems like a poor thing. I see Mr. Secretary is—

Mr. GRIFFIN. I think that, as we indicated in our testimony, there is a good plan. The implementation has not happened, and some of the implementation planning, in our estimation, was not timely enough.

Dr. SNYDER. But this specific situation, where you are sending something from the Inspector General that says, these are our findings; please comment on them. They can flat-out say they don't agree with them, but you are saying you don't even get the courtesy of a reply, as they say.

But I wanted to ask a specific question about the external electronic connections. Now, that seems like something that is fairly straightforward. Am I wrong on that? I mean, you are talking about something concrete that somebody needs to go in with a new

component and take out the old component, and put it in. What do you think the delay is there, on having that work done?

Mr. GRIFFIN. I am going to have my technical expert speak to that. We are mainly talking about Internet connectivity in that area.

Dr. SNYDER. Yes.

Mr. GRIFFIN. Mr. Slachta will respond to that.

Mr. SLACHTA. Mr. Snyder, first of all, it is not a new issue. We reported this several times, 7, 8 years ago. The Department has strong policy and procedures on what is supposed to be done. It is a matter of implementation and monitoring.

The situation that we currently have arose as a result of a scan that we were doing jointly with the Department. VHA has helped us considerably in doing these scans. But we found some sites that were not in compliance with departmental policy, which created the vulnerability, or the potential vulnerability, of open access to the system.

Dr. SNYDER. But this is an example where this is fairly straightforward. Is that an accurate thing to say? I mean, you are talking about replacing—

Mr. SLACHTA. It is not—I am sorry, it is not really just putting one piece of equipment in over another piece of equipment.

Dr. SNYDER. All right.

Mr. SLACHTA. It is making sure you have adequate firewalls, making sure you have adequate policies and procedures for access to the sites, making sure that it is into the network properly.

Dr. SNYDER. All right. Mr. Griffin, you made comments in there about the facility management, I agree with a lot of what you have to say, et cetera. How do you follow up? I am new to this committee. What is your role, say, over the next year, or this next 2 years, or this Congress?

Mr. GRIFFIN. In all of our audit work, our administrative and investigative work, and our health care inspections, we issue draft reports to the administration, giving them the opportunity to respond to our findings or to add any additional information. We then evaluate those replies and incorporate them where appropriate into our final report.

Our final report gets issued with recommendations as to specific areas that need to be addressed. We have a follow-up system within our organization, and quarterly we will send an inquiry as to the status of our recommendations to determine whether or not the appropriate actions have been taken. We will continue to follow up on a quarterly basis until all of the recommendations have been addressed.

Dr. SNYDER. And you share those findings with this committee?

Mr. GRIFFIN. In some instances, we will check back after the first 90 days and we will find that all of the recommendations have been addressed. If all of our recommendations haven't been completely addressed, we will continue to track them on a quarterly basis to make sure that they are accomplished.

Dr. SNYDER. Dr. McClure, would you give me a brief summary of how you think VETSNET is doing?

Dr. MCCLURE. I think VETSNET, from our look at it, particularly at the C&P component at this time, indicates there is atten-

tion to some of the problems that we have seen in the past to project management, certainly attention to putting together better plans and using those plans to manage. There are still too many issues associated with sequencing, with actual milestone dates being met and set out in time, and certainly we are very concerned about adequate testing of it, to determine if all pieces of it are deployable.

And as I mentioned in my statement, C&P has had ten test claims cases run through it. And it is questionable whether, if you are going to have 3.2 million cases running through a system a month, that that is an adequate field testing of it. Not to say that VA does not intend to do more, we would encourage them to do more. But it certainly puts you at risk to be able to justify a large-scale deployment of a system with that limited amount of testing.

So those are the issues that continue to, I think, plague some of the systems like VETSNET.

Mr. BUYER. Mr. Udall.

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

Mr. Griffin, you mentioned in your written testimony that the VA's program and financial data continue to be at risk due to serious problems related to the Department's control and oversight of access to its information systems. You go on to say that sensitive veteran medical and benefit information is at risk. And I note that you, in your testimony, talk about some specific weaknesses. But I am wondering about what specific steps that ought to be taken to remedy this situation. I think that medical information, and benefit information is something that is very sensitive, and should be secure.

Mr. GRIFFIN. Go ahead, Mike.

Mr. SLACHTA. In our prior testimony before the committee in September, and in some of our reports, we have outlined some of the most basic security measures that needed to be addressed—something as simple as strong password control, and not leaving the computer on when you walk away from it; turning it off. It is implementation of security at the operation level. That is where your security begins.

It is training people to be aware of security. The security awareness briefings that need to be made. If you can get that across to all levels of the organization, it goes a long way. People have to understand that the greatest vulnerability is from the inside. The vulnerability is the people who have access to the system. So you need to make sure that people have the right access, that the right people are identified to the system, and their levels of access are identified. I would start there.

Mr. UDALL. And how much progress has been made on those items you just mentioned?

Mr. SLACHTA. The Department has issued the policy. VBA, when we brought these initiatives to them originally, back in July of 1999 and September of 1999, sent out letters to the stations, do these things. The former Secretary issued a stand-down for the Department to say, hey, we have to be aware of what's going on in security.

The problem is continuous monitoring and accountability.

Mr. UDALL. Were training sessions implemented and put in place?

Mr. SLACHTA. I don't know that training sessions were implemented and put in place everywhere. I do know it was in some places.

In our program of CAPS, we do security briefings, fraud and integrity briefings. They are pretty well-attended by the stations that we go to. Not as well as we would like, but they are attended. I can't speak to the Department as a whole at this point.

Mr. UDALL. However your recommendation would be for agency-wide training for issues like passwords and turning off computers and things like that, that subject the security system to a threat?

Mr. SLACHTA. Yes, sir, it would be. And the Department has stated that they will have information security officers at each facility, and these people should be monitoring security and monitoring to make sure the training is actually taking place, and looking at the security vulnerabilities and making risk assessments at their facilities to address these issues.

Mr. UDALL. Now, when you talk about ensuring that the right individuals have access, does that imply that there were individuals that had access that should not have had access to secure kinds of information like medical data and sensitive benefit information of veterans?

Mr. SLACHTA. Yes, sir, it does. We have examples of people who have improper access. Generally it is the result of not monitoring what is going on in the system.

Mr. UDALL. And to remedy that, on the right people having access, I assume you have to do a thorough review of who has access and who should have access, and then cut the people off that shouldn't have access. Has that been done?

Mr. SLACHTA. That has not been done across the board, no. That is something that needs to be done, and it needs to be done on an ongoing basis. It is not a one-time thing, you do it every 90 days, every quarter, something of that nature.

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

Mr. BUYER. Thank you, gentlemen. I have some questions that I am going to submit to all of you for the record. What I would like to do next—Mr. Secretary, I am aware of the meeting you have down at the White House. But what I would like to do is I am not going to advance you forward, because I would like you to listen attentively to the next panel.

We, the taxpayers, have invested a lot in security assurances, and you have inherited a mess. So we are going to hear from really some very sharp corporations out there in the arena of quality assurance. And I think it would be a very valuable 15 minutes, and then we will immediately take your testimony. Would that be agreeable, Mr. Secretary?

All right, thank you. This panel is dismissed. The next panel we will hear from is Mr. Karl Ware, Executive Vice President of Operations, BioNetrix Systems Corporation; also testifying is Mr. Ken Brandt, Managing Director of Tiger Testing; also testifying is Mr. Scott C. Sherman, Director of Advanced Technology Architectures of EMC<sup>2</sup> Corporation.

Mr. Sherman, you may begin.

Dr. SNYDER. I thought Mr. Ware was going to go first.

Mr. BUYER. Is there an order here of preference? You have a tech program here to show? All right, Mr. Ware, we will let you go first.

**STATEMENTS OF KARL WARE, EXECUTIVE VICE PRESIDENT OF OPERATIONS, BIONETRIX SYSTEMS CORPORATION; KEN BRANDT, MANAGING DIRECTOR, TIGER TESTING; AND SCOTT C. SHERMAN, DIRECTOR, ADVANCED TECHNOLOGY ARCHITECTURES, EMC<sup>2</sup> CORPORATION**

**STATEMENT OF KARL WARE**

Mr. WARE. Thank you, Mr. Chairman and members of the Committee. I am here to talk about how strong authentication is being utilized in the commercial environment for reducing fraud and for facilitating access to systems.

One of the things that you already know, as has been pointed out this morning, there are many violations that occur due to compromised passwords. Well, these are just some of the, what I have here on the screen are some violations that have occurred in the commercial market with regards to authentication violations. But these are just very common occurrences. Every day, passwords are compromised and people gain access to systems illegitimately.

What I want to do, just to show people and the people who are here witnessing the testimony today, is kind of give you a quick view as to how weak passwords are. If you think of all the passwords that you have, whether they are PIN numbers for your ATM card, access to your home Internet, email access, any of those things, if you look at this list of things that I am putting up here on the screen—whether it is your name, your Social Security number or some permutation, your phone number—you will find that a lot of people create passwords that are based on any of these.

Just to give you a feel—

Mr. BUYER. Will the gentleman suspend for a moment? Mr. Secretary, there is a really nice seat here. Mr. Secretary, come on over. Mr. Secretary? Please, come on over. It is really a great seat. You won't have to squint, you won't have to lean, you won't have to—  
(Laughter.)

Secretary PRINCIPI. Thank you, sir. I appreciate that.

Mr. BUYER. Thank you.

Mr. WARE. If you take a look at this list—and I use this list in seminars, in speeches that I have given—it has actually better than a 92 percent hit rate. I can guess 92 percent of the passwords of people there. Usually I will ask for a show of hands of whose passwords did I not guess? And usually four or five people out of 100 will raise their hand, which meant, at that point, that their system has been hacked.

The next thing is just a quick scenario of what the environment looks like that we are trying to protect. At the bottom, you have the destinations—the systems of the VA, the systems of a hospital, the systems of a bank. Above that you have intricate systems that provide permission or authorization. And then you have the different methodologies. We talked about remote access or dial-in access to the different environments, and we typically will put encryption and integrity technologies in front of that.

But the weak link is still at the front end, passwords. What my company does, BioNetrix, is we provide strong authentication, the ability to manage personal authentication for access to any environment. At a very basic level, this is what we do.

On the right-hand side are applications. Those are the systems that the VA has, or that any hospital would have, or commercial environment would have. On the left are strong authentication methodologies—fingerprint, face, token, smart card. And including passwords; some people will continue to use passwords for different systems. Many of the banks and hospitals that we are using who had implemented strong password technology methodologies are now decommissioning the password methodologies and replacing them with other stronger authentication methodologies.

Authentication is something you know, which are passwords or PINs; something you have—a token, a smart card; something you do, so I can use your voice or your signature for authentication; or something you are, the strongest forms of authentication. All of these have come down in price, come up in performance, come down in price, so that these are now all available at a desktop level.

The other thing that our system does is enables you to deploy policies that can now be enforced. Before, you used to say that for something to happen, this plus this must happen. Well, with strong authentication in place, you must have, for example, a token for remote access. For desktop access, your fingerprint must be there, or to perform a particular transaction at your desk you must be there to do it. Nobody else can do it.

And let's say for a high-value transaction, I force two forms of authentication, fingerprint plus facial recognition. Or if it is truly a high-value methodology, what we could do is actually force two people, missile-key authentication, so that you have two people who have to be there to perform an authentication to effect the wire transfer.

In the past, it was true that as you increased security, convenience went away. Well, what we have done is turned that over. Your fingerprint should be with you all the time. If you leave your face at home, there is a bigger issue.

So what we do is we increase convenience, but we also increase security at the same time. And we do that cost-effectively.

We have a list of benefits that we tout with regards to our product. But I think that with regard to what we are discussing here today, we are able to reduce fraud through the use of strong authentication, we are able to augment the use of passwords if they are going to continue to exist. And oh, by the way, I don't care where you are sitting, standing, or coming into a system. We are able to utilize our infrastructure at all of those points from a single management point. So for all of the systems, I can now manage authentication from one platform.

And that concludes my presentation. I would address any questions that the Chairman has, if you have any.

[The prepared statement of Mr. Ware appears on p. 69.]

Mr. BUYER. Mr. Brandt.

**STATEMENT OF KEN BRANDT**

Mr. BRANDT. Thank you very much for inviting myself and Tiger Testing to speak. I have given many speeches and been on panels, but I have never testified before Congress, and I very much appreciate the opportunity, and am honored.

We were asked to speak about what is ethical hacking, what are the benefits, and how is it done? Ethical hacking is testing the security of the Internet sites, of access points to a given organization, the VA or any other place. Is the website secure? Are the underlying systems vulnerable, can they be reached? Can somebody from the outside get in? Can somebody take advantage of the email or the file transfer protocol systems? Can somebody get to the underlying system? Is the privacy of the individual records, the individual veterans or whatever the organization is, is that protected? Ethical hacking answers that question. Are systems safe from the outside? It is a test of the system.

It has many different names. It is also called network security assessment, vulnerability assessment, et cetera. There is not a good single standard name, but ethical hacking is one of them.

The government, Congress, has mandated security policies and procedures for all kinds of different government agencies, financial firms, health care firms, in order to protect this. Part of that process is testing whether these procedures are being followed. That is where ethical hacking comes in.

The "ethical" in ethical hacking has three meanings. One relates to integrity. The people doing the ethical hacking should be able to pass any type of background check whatsoever. They should not be criminals, ex-criminals, people who have a history of defacing, destroying or disrupting systems. Integrity is critical.

Second, the testing itself should be transparent. There should not be any destructive elements to the actual testing. You do not have to cause any system problems in order to identify security problems.

And third, it should be independent. There should not be a conflict of interest. The same people who provide consulting on protecting privacy and security should not be the same ones testing at their own suggestions, their own solutions, their own hardware.

What are the benefits of this approach? The benefits of ethical hacking are involved in sort of a virtuous cycle. You test; the firm being tested, or the agency, corrects the problems that are being identified; you test again; you repeat that cycle. You get safer and safer and safer. The information is more secure, the privacy is more protected.

You must stick with this on a continuous basis. It is not something you can do once every quarter, once every year, once every once in a while. Hackers do not just attack once in a while. Many systems on the Internet are under constant scan by unethical hackers. You want to keep your guard up.

There are two reasons why a system at any given moment could have a security problem. One is, changes have been made. New security holes have been opened up as a result of the system being changed, the Internet being changed, underlying systems, anything. Second, even if, miraculously, you are standing still in terms of technology, unfortunately the outside world, the hacker world, is

advancing in technology. So you need to test the same systems continuously to make sure that new gaps have not opened up.

The next part of the testimony relates to a more detailed explanation of the approach, some of the high-level how-tos of ethical hacking. They have been the basis of books that are coming out, actually one this week and one in a couple of weeks, for the legal basis of how it should be approached, and another for the system basis. There are industry standards. I won't go through them, but I would be happy to answer any questions about them, anything that just came up, or Tiger Testing. We are a firm that performs ethical hacking. This is 100 percent of what we do.

And again, thanks very much. I am really excited about being here. I don't know if you are supposed to say that, but—

(Laughter.)

[The prepared statement of Mr. Brandt appears on p. 79.]

Mr. BUYER. Thank you, Mr. Brandt. And I know the Secretary is just as excited to be here. (Laughter.)

Mr. Sherman.

#### STATEMENT OF SCOTT C. SHERMAN

Mr. SHERMAN. Chairman Buyer, Dr. Snyder, distinguished members of the subcommittee, my name is Scott Sherman, and I am the Director of the Advanced Technology Architectures with EMC.

It is an honor and a distinct pleasure to be here this morning, and I have submitted some written testimony. And I am just here to quickly summarize and hopefully allow time for some questions and answers. If you might know, EMC<sup>2</sup> is the world's leading provider of information storage infrastructure for both software, networks and services, as well as a leading provider of secure information storage infrastructure in the world. EMC stores approximately two-thirds of the world's mission-critical data, with revenues of approximately \$9 billion in 2000. We are based in Hopkinton, Massachusetts, founded in 1979 with approximately 16,000 employees in the U.S. and 23,000 internationally, with offices in approximately 43 States.

EMC customers have developed enterprise storage infrastructure solutions within very high-performance organizations. Well-represented are the world's leading banks, financial institutions, airlines, telecommunications, transportation companies, Internet service providers, educational institutions, as well as regional and national government agencies. One of the driving forces behind enterprise infrastructure is the recognition by the world's global 2000 companies that to stay competitive, they must ensure that the corporate activities are focused ultimately on providing high customer satisfaction. This is very similar to the mission of ONE VA, of caring for the veteran.

This customer-centric business architecture must be matched by an IT architecture that puts information of the customer and the business at its center. The information-centric approach makes possible the efficient information sharing and data management, and high-speed communications, among diverse business systems, regional locations and other entities.

The promise of IT to deliver massive operational efficiencies is finally being realized in high-performance organizations through an

enterprise information-centric approach that enables a single unified view of the customer and the business issue.

EMC develops robust enterprise-wide information infrastructure. It is a new paradigm necessitated from an explosive growth in information and its use. If you are familiar with some of the statistics that have come out, within the next 2 years we will see as much information created as was since the beginning of mankind, approximately what is known as 12 exobytes. If this is represented by a single sheet of paper, it is basically three thousand trillion sheets of paper. If you stack that paper up, it is about 500 million miles high. That is the information that will be created in the next 2 years.

That is enabling an enormous power that we can exploit inside our information infrastructure. Apply it within the health care community, the ability to store and retrieve and share medical imageries, do trend analysis, do image recognition of various health care initiatives, is a very powerful statement, but the infrastructure must be capable of supporting those types of initiatives.

Other things that are happening that are also represented inside the mobility inside the VA includes things like the aging and the mobility of the veterans themselves, necessitating the information be shared across the country and across the various regions.

In the commercial sector, these high-performance organizations have shifted their IT architectures in response to those trends, and employed a standardized enterprise-wide IT infrastructure. These organizations have created consolidated corporate information databases, which dramatically ease the sharing of data between different business functions, standardized and simplified data management processes, and guaranteed protection against loss or corruption and improved management decision making. These commercial organizations have demonstrated this challenge is best met by implementing an enterprise architecture that integrates all of an organization's systems and places information at the center.

EMC has revolutionized enterprise information technology strategies, and developed unprecedented interoperability with all information systems, sub-systems and emerging technologies to deliver a complete enterprise information framework that dynamically adapts to multiple mission-critical requirements.

This architecture eases information sharing across the different business functions and fast communication across all enterprise systems. It provides better information protection by isolating the complexities of data management, and it provides high availability as a result of online backup and disaster recovery. It provides cost-effective data management from centralized cross-platform management tools, and finally provides a much more flexible business environment that helps provide better customer service.

These are powerful examples where we can drive functionality from the information infrastructure itself, and provide cohesive information that can be leveraged across the various entities inside the VA. As an example, you can have critical infrastructure protection functionality implemented within the infrastructure itself, whereby you might have one entity located in Kokomo, Indiana, mirroring data to Little Rock, Arkansas, and have information immediately be up and running inside 15 minutes if one site might

happen to go down, guaranteeing availability to mission-critical information. And nothing is obviously more mission-critical than the health and care of the veterans themselves.

This example has been replicated across, through the Red Cross, Transamerica, various health care organizations, as well as major IT technology providers such as Oracle, Cisco, and even inside ourselves.

And with that, I will conclude my testimony.

[The prepared statement of Mr. Sherman appears on p. 85.]

Mr. BUYER. I just have one question for all of you. First of all, let me thank you for coming and preparing your testimonies. This is a valuable assistance. My sense, after the first panel, with regard to priorities and recommendations to a new Secretary is, it is about management. Okay?

Well, maybe perhaps true, but it is also about more than that, in my sense. So I want to turn to you as the experts on what here perhaps is critical. My sense is that the integrated architecture is critical, but I may be wrong. So let me turn for your advice. If the VA turned to you for assistance, what would you say?

Mr. WARE. Well, initially I would look at the consolidation of users of a system into a single authentication infrastructure. That is what we do for a living. This is not the first time that people have looked at consolidating different systems, but the ability to manage different environments but have one authentication methodology or set of methodologies that can be used across all the systems, across all the platforms, no matter where a person is standing, is what we see as very important. Protecting the front door of a system. We would rather deter fraud, rather than detect it.

So let's look at how do we keep the right guy honest by making sure that he is who he says he is, and he gets to where he is supposed to, versus worry about, gee, there are 500 bad guys out there. If they don't have a fingerprint, if they don't have an identity in the system, I have a way of instantly locking them out. So now I have this methodology for assuring that the front door of an environment is protected.

Now, if they have been given permission to go somewhere that they shouldn't be, they are only doing what they were told to do or what they have been permitted to do. But for me, looking at the first line of security, it is protect the front gate, whether it is over the web, dial-in, or sitting at a desk. Before you let somebody into the system, make sure that they are who they say they are. It is not a shared password, it is not my assistant saying, gee, I will finish that email for you and give everybody a vacation. It has got to be the person that they say they are.

Mr. BRANDT. Not knowing anything specific about the VA, other than what I heard this morning and read in prior testimony, it sounds like they have a lot of good plans, but they just need to get moving.

Our experience in the Internet world, and I am sure my colleagues would agree, the speed in which you need to move is very important. It is the management and the technology, but you have got to move, because the outside world that you need to defend against, the people going against the web sites and systems that you are worried about, the potential adversaries who are going

after the Veterans' Administration's records, they are not sitting still. They are moving. You need to test, find out what is going on, and remediate. You need to move fast.

Mr. SHERMAN. And then from an information infrastructure standpoint, you know, you brought up the issue of management. A lot of these organizations, both in the private and public sector, are turning to the industry leaders, like EMC, Oracle, Cisco, and defining what the best business practices are that can be immediately applied to their own requirements. We have our own incubation process within our organization that provides these commercial best practices. Inside the Federal Government, we have consulted with multiple agencies on this.

And more and more we are finding that all the organizations out there are continually pressing the IT suppliers to develop more and more integrated solutions. And we have actually done that with an initiative between, again, Oracle and Cisco and ourselves, called ecostructure, which is specifically geared towards building high-availability, high-secure web infrastructures as a general policy. They are IT blueprints, which are scalable and deployable immediately, today.

Mr. BUYER. Thank you. Dr. Snyder.

Dr. SNYDER. Just one quick question—and I appreciate all three of you being here today, it was very interesting. Mr. Brandt, your comment about moving fast, I want to be sure I understand. It is not moving fast to a fixed point. I mean, this committee needs to look on somehow. There is not some magical point in time at which we will say, we have arrived, the IG gives everybody an A-plus. Because 6 months down the line beyond that point, the potential adversaries out there are going to be moving faster, trying to break through. Is that a fair statement? It is going to be an ongoing process for all time to stay ahead of potential security lapses. Is that a fair statement?

Mr. BRANDT. Much more than fair. I am in 100 percent enthusiastic agreement. The problem is not reaching a fixed point at all, because outside technology continues to advance. You need to protect veterans and every other type of organization from, unfortunately, advanced technologies and potential intrusions. The only way to do that is to stay on top of these things.

We see, over and over and over again, firms—and we don't do any government work right now, but we see it in the private sector—where a firm will be very secure for a while, then they make a whole bunch of system improvements, and their security falls through the floor. So we identify all these gaps, and then they fix it, and it happens again. That pattern recurs to some degree over and over and over with many firms. You can't sit still. You have got to check constantly; when something happens, you have got to jump on it.

Dr. SNYDER. Thank you, gentlemen, for being here.

Mr. BUYER. If I could just make this statement, I thought it was very good. Mr. Sherman, in your written testimony, you noted that commercially—I guess this is with the comment from the first panel about the management and of whom the Secretary selects for that job, and what his role ought to be as you seek to then integrate, as Mr. Ware has articulated so well.

Quoted, "Commercially, it is EMC's experience that few, if any, high-performance organizations achieve an enterprise approach without a dictator-like commitment which departmental leaders must accept, regardless of organizational or cultural changes that result." Well, you must have seen a lot of things clear out there across the business sector to write a statement like that.

So if you want to talk about a culture, there is definitely one in the VA. And so whomever that individual is, is going to have to be a pretty strong-willed individual, and make some pretty strong demands. But will you give me a quick example out there of, why do you write such a strong statement like that?

Mr. SHERMAN. It must be accomplished, because there are certain problems. And it does exist inside the federal sector, too. With the diversity of the organizations that are out there, unless somebody takes command of establishing an enterprise-wide standardization of how these systems will come together, to build something like that, that is pictured there, with one infrastructure that can actually start driving all of these other various initiatives. But it has to come together to even begin to get to that stage.

I can pick out a couple of examples. One would be the Red Cross district locally. You know, they had a very diversified infrastructure. They were trying to consolidate down to nine regional processing sites. Until they had one person, a guy by the name of Doug Levy, take over and really drive the standardization and how the organizations were going to interoperate together, was the first time that the organization was actually able to jump up in scale and just actually truly manage the blood supply like it is supposed to be managed.

Mr. BUYER. So this sounds like your recommendation is the VA needs a security czar?

Mr. SHERMAN. I think that would drive and solve a lot of the problems that are occurring.

Mr. BUYER. Mr. Udall, do you have any questions?

Mr. UDALL. A brief one, Mr. Chairman. And it is along the same line, I think, that you were asking.

Mr. Brandt, you talked about doing upgrades, and then having security problems. And really the issue is how you specifically monitor those kinds of situations. I mean, do you assign a person, a security czar? I mean, what are the specific actions that need to be taken—and this is addressed to all three of you—in order to analyze and find and constantly be on top of weaknesses that might occur as you move along?

Mr. BRANDT. Well, the first step—and this will sound ridiculously untechnical and stupid—but the first step is actually having people that are paying attention all the time.

We see over and over, firms will install firewalls, they will install IDSes, which are intrusion detection system devices. They will install all kinds of stuff, and then no one reads the logs, and they are not paying attention. And when they expand their system around it, they don't realize what is going on.

Somebody in the organization has got to set up the basic blocking and tackling. Who is going to be paying attention to security? Do they have the clout? Are they going to be able to actually address security issues? The technology will absolutely change over time,

and it is going to change fast. Do you have the resources and the people in place who are paying attention to all of that as it moves forward?

Mr. WARE. One of the things that we have found, we work with a lot of financial institutions and hospitals. The security czar in those organizations works very closely with a person who is identified as the risk czar. And they move down the hallways in tandem constantly.

I guess the key thing is that an organization must have a strategic plan, but there are some tactical things that they have to do to get to the ultimate goal. There is no end game. I mean, at the end of the day, as was pointed out by Mr. Brandt, soon as you plug up all the holes, somebody has come up with a hole-maker for your security environment.

So what we find in all of the institutions that we are working with, the security czar plus the risk czar are the guys that are in there saying, let's protect the front door, let's figure out what applications need to be protected.

And one last thing that I might point out is the old school of security said, let's put a really big wall around the whole fort. That doesn't work, because you can't protect that entire perimeter. Let's identify what is really high-risk information and sensitive information; protect that. I don't care what is on the company bulletin board about next week's picnic.

And so a very strategic and tactical view has to be taken. But I think the statement made by my colleague here about a dictatorship approach to security, that is absolutely needed.

Mr. SHERMAN. And just to add to that comment, I think, you know, we are talking a lot about technology here. But in the end, when we get to that dictator-like initiative, you are making a cultural change. It is not the technology that ultimately is going to drive the change in behavior and the change in the organizational vulnerabilities. It is the culture that has got to change. And that is where it is important to be driven down from the top.

Mr. BUYER. Thank you, all three of you, for coming.

Mr. SHERMAN. Thank you, Mr. Chairman.

Mr. BRANDT. Thank you.

Mr. WARE. Thank you.

Mr. BUYER. The next panel we will have is the Honorable Anthony J. Principi, Secretary of the Department of Veterans Affairs. Mr. Secretary, welcome to the subcommittee. Your appearance and testimony here today, I believe, highlights the priority which you place upon this issue. You have not sent an underling, you have come here yourself. You have inherited something for which you have decided to take the reins and take on.

Let me publicly congratulate you on taking on the responsibility as the Secretary of the VA.

Secretary PRINCIPI. Thank you, sir.

Mr. BUYER. It is a difficult task. At times, it can be a thankless job, because your service, a lot of people are coming to you. A lot of people have a lot of demands on you, and you make a lot of judgments. And it is difficult to find and achieve satisfaction. That is why I said it almost can be thankless.

But obviously, for you to take on this particular job says a lot about your heart and says a lot about your principles, and a lot about your dedication. So I welcome your appearance, and please identify the individuals whom you have brought with you by their name and their title, and then you may proceed with your testimony, Mr. Secretary.

Secretary PRINCIPI. Yes, sir, I would be happy to. Sir, to my immediate right is Guy McMichael, who is the Acting Assistant Secretary for Information Technology, my acting CIO. To my far left is Dr. Tom Garthwaite, our Under Secretary of Health. To my immediate left is Joe Thompson, Under Secretary of Benefits, and to my far right is Roger Rapp, the Acting Under Secretary for Memorial Affairs.

**STATEMENT OF HON. ANTHONY J. PRINCIPI, SECRETARY, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY GUY MCMICHAEL, ACTING ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS; THOMAS L. GARTHWAITE, UNDER SECRETARY, VETERANS HEALTH ADMINISTRATION, DEPARTMENT OF VETERANS AFFAIRS; JOSEPH THOMPSON, UNDER SECRETARY, VETERANS BENEFITS ADMINISTRATION, DEPARTMENT OF VETERANS AFFAIRS; AND ROGER R. RAPP, ACTING UNDER SECRETARY, NATIONAL CEMETERY ADMINISTRATION, DEPARTMENT OF VETERANS AFFAIRS**

Mr. PRINCIPI. Thank you, Mr. Chairman. Thank you for those very kind words. I am indeed honored to be Secretary of the VA, and I know it is a major challenge. I applaud you, Dr. Snyder, you, Mr. Udall, and members of this committee for holding this hearing. This is a very, very important issue. It is clearly one of my priorities, as I stated in my confirmation testimony. And so I am pleased to be here to tell you how I plan to proceed and to be held accountable for success or failure of our efforts to improve the deficiencies in our information technology program.

In particular today, I will discuss our department's integrated systems architecture; VETSNET; our information security posture; and the Veterans' Health Administration decision support system.

Let me begin by giving you my personal commitment that I intend to reform the way VA uses information technology. First and foremost, I intend to ensure that all department policies, procedures and practices are in complete compliance with the mandates of the Clinger-Cohen act. Specifically, I will define roles, reporting relationships, and boundaries of authority among all CIOs within the department in ways that enhance the effective implementation of that act. I will provide appropriate authority to the CIO to ensure control over the IT capital planning and investment processes. We will increase quality control over our capital planning, and provide clear procedures on how CIOs and program managers communicate to senior management the status and progress of major IT projects.

Every effort is being made by me to attract and appoint a CIO with the background commensurate with the enormous responsibilities of overseeing a \$1.4 billion IT budget, as you have indicated. I need not tell you that trying to bring someone from corporate

America, from the private sector, to take on this enormous challenge for \$130,000 a year is a tough feat. But we are working towards that end, to bring someone with the leadership, the IT background, the discipline, the focus and the respect to get the job done.

You know, Monday afternoon I talked to the President about a range of issues. At one point, I talked to him about the fact that we have a \$1.4 billion IT budget and historical problems with information technology in the VA. I think I can say that he almost fell off his chair in the Oval Office. He looked at me and said, Tony, I expect you to fix it. I expect you to bring the team on board that is going to get this job done. And it was very direct, very to the point.

I have already pledged that I will not spend any new funds on information technology until an enterprise architecture has been defined that ends stovepipe systems design, incompatible systems development, and data collection that does not yield useful information—not one new penny. I will convene a panel of world-renowned experts almost immediately in systems architecture, to team with our key business unit decision makers in each of the VA's administrations and staff offices to develop a comprehensive, integrated enterprise architecture plan. And they will devote certain days of the week, Fridays and Saturdays, part of their weekend, until this architecture is completed and submitted to you. It is my highest priority, and I expect to deliver it to you in a matter of months.

Another issue that is one of my highest priorities is our IT security posture. I take the privacy and security of the information VA collects and uses very seriously. Our veterans entrust us with the most private and sensitive information imaginable. They must be sure that we will honor their trust by ensuring that no unauthorized person ever has access to this information. We must also ensure that our financial transactions are scrupulously protected, and that the networks and systems we depend on are secure and available.

We have made significant strides recently in improving our overall security posture, but as recent reports from the GAO and the Inspector General demonstrate, we still have much to do. I will hold all VA senior managers accountable for ensuring strict compliance with our security directives. I have created a senior executive service-level cyber-security director position. That director position has been recently filled by a highly qualified candidate, Bruce Brody. He comes to us from the Defense Department, and will be an important member of our IT management team.

I believe it is impossible to build a perfect security system. That is not an excuse for our failings. That is not an excuse for our inability to build a reasonable and cost-effective system. But you can never build a perfect system, and I think we have to recognize that.

I don't think a month goes by in this country that we don't learn about another unauthorized access into some of this nation's most sensitive information databases. I don't think a month goes by that we don't learn about another hacker breaking into some of the software systems of our nation's most noted information technology corporations. I think we need to understand that in this high technology world, there are dishonest people.

The IG responded to your question, Mr. Chairman, about some fraud cases. Regrettable incidents, but I don't think they are IT problems. I think those are internal control problems, internal control failings, where a dishonest employee—I should say, maybe, an alleged dishonest supervisor—betrays their trust and uses the system, the access they have, and gets other employees who have access to the system to fraudulently take money away for their own purposes. To the degree that they had access, I see this as an internal control weakness and problem that we need to fix.

With regard to the two specific programs you have asked about, VETSNET and VHA decision support system, I am sure you are aware that each of these programs has had a very troubled history. VETSNET has been under development for far too long. Its development was delayed as new technologies have come and gone. It has suffered from a lack of focus, the absence of clear goals and inadequate management. I believe, however, that these problems are now beginning to get solved. The current VETSNET management plan addresses these problems. But I am still concerned about critical performance, scalability, and systems integration issues. I have therefore directed that we will conduct an independent audit of the overall system before VETSNET becomes fully operational. This audit will provide me with the assurance that this system will meet all of the security, functional and performance tests we have set for it.

But let me be clear, Mr. Chairman and Dr. Snyder, I will not throw good money after bad. If the independent audit shows that this system will not work, we will stop. We will not implement it. We will continue with existing programs, and we will look for a new solution. But we will not throw good money after bad.

As to the VHA decision support system, or DSS, our department has made a significant investment, as you have pointed out, in both time and resources in the implementation of this system. Since its implementation in 1998, we have made strides to improve its data quality and access to that data. Clearly, as you have pointed out again, many of our medical centers and VISNs, or a number of them, are not using DSS the way I believe they should, but we are making progress.

Data from the system is now being used in the development of VERA allocations for fiscal year 2002. Our Practice Management Advisory Board is using DSS data in their work in practice profiling. There are now a total of 14 DSS-based performance measures, applicable either to VISN or facility directors to ensure that they move towards data-based decision-making. And to further integrate DSS use in financial management and day-to-day operations, responsibility for this program has been transferred to the Office of Finance in VHA as of March 11.

I am aware that significant efforts are still needed to ensure that we receive an appropriate return on our investment in DSS, which is in the hundreds of millions of dollars. And I am committed to making that effort.

Mr. Chairman, that concludes my brief review of these very serious information technology issues, and we would be pleased to answer any questions you might have, sir.

[The prepared statement of Secretary Principi appears on p. 89.]

Mr. BUYER. Mr. Secretary, your comments are stern, and welcome.

The point you made about some of the problems with the fraud cases you saw as really more internal security, internal control issues and access, when you use the word "access," I guess I look at it and I say it is all sort of the same. I mean, you have got people coming from the outside, and you have got those who are on the inside.

The reason we had the second panel testify is that Mr. Ware, who was very articulate, you know, was able to show that—I suppose whether it is key control, or in this particular case, access to a particular computer system—you have to change those passwords every so often. You know, it is a fingerprint, it is an iris. You know? And if that person doesn't have that job, or if they moved on, boom. I mean, you don't have a problem.

Secretary PRINCIPI. No.

Mr. BUYER. And a lot of that technology is out there.

We took on some of these issues, and President Clinton had to take on a lot of these security issues with the embarrassment of what occurred with a lot of the country's most secretive information ending up in wrong hands. And so he brought in, just as you suggested, some of the world's experts on security assurances. And you know what we discovered? There aren't as many of them out there.

And when I began to look at this one from the Armed Services Committee, I walked away sort of weak-kneed. We have some of these beliefs that we rest easy at night, that the best minds in the world are out there, because they are operating to ensure that the systems that are being built are so secure. And we think that they are only hacked by these extraordinary geniuses. And then in reality we are finding out that it is not necessarily so.

So my sense here, Mr. Secretary, it is sort of both. Would you concur?

Secretary PRINCIPI. Oh, absolutely, Mr. Chairman. Absolutely, sir. And I certainly didn't mean to imply that that was not a problem. It is a problem, from both the outside and the inside.

In this case, I just wanted to point out that, you know, you have some bad people. And I happen to think they are very few; I think the overwhelming majority of our people are honest. But in this case you have a supervisor who was rating cases, and you know, you have the ability, you have the access to this data, and you are using it for wrongful purposes.

That is an internal control weakness. We have to have mechanisms in place to identify that kind of situation and take appropriate steps. Just like you mentioned; an employee leaves the VA, he should be logged off, he should be locked out of that computer system. You know, your transfer data—again, every 90 days a password should change. You know, you try to get access to the system, if you have used the wrong password three times you should be locked out, and you have to get back on by a network administrator.

Mr. BUYER. Most of the security companies tell us that most of the hacking is from the inside, not the outside.

Secretary PRINCIPI. Some great advances in authentication have been made, as we heard in that testimony. I was a short time in

the wireless industry—great deal of cloning fraud and subscription fraud. In the wireless industry, for them that is hundreds of millions, if not billions, of dollars in lost revenue. So they take very careful steps to ensure that they have software built to identify that kind of fraud. And I think we need to do the same thing, again in a way that is reasonable, addresses our concerns, allows our doctors to get access into our system from the medical schools, different kinds of issues. But I think we can address those in a way that meets your requirements for security and privacy of this important data.

Mr. BUYER. Tell me about the selection of this department chief information officer. Who are they directly going to report to? Is that going to require a Senate confirmation? Tell me a little bit about that position. You heard the input from industry on what that person needs to be like. Tell us about that position.

Secretary PRINCIPI. Well, certainly that is an Assistant Secretary reporting directly to me. The question of whether an Under Secretary position is needed, and Under Secretary for Management, is something that I am grappling with, that I would like to talk to the Congress about. I think that position is so important that we might want to look at an Under Secretary, but that is something I need to discuss with the Congress.

I have been trying to find someone from industry who has an extraordinary background in engineering, computer science, that can bring the skills of industry to bear to help us accomplish our purposes. I see IT as an enabler to help Dr. Garthwaite and Mr. Joe Thompson and Roger Rapp get the job done, not a program unto itself. It enables our administration to succeed.

That individual has to bring, I think, great leadership. I would like to see someone who may have the respect of the Department of Defense, because I think we need to start tearing down those barriers that impede the transfer of data from DOD to VA. Focus and discipline and respect. The respect of the people in the administration. I intend to look—the CIO will be a very, very important position. Whether it will be a dictator or czar, I am not sure you need a dictator, but you sure need somebody who is strong and can work closely with the respective administration CIOs to make sure the job gets done.

But clearly this individual is going to have a very prominent role in our administration.

Mr. BUYER. Thank you. Dr. Snyder.

Dr. SNYDER. Thank you, Mr. Chairman. Kind of picking up there on this discussion of dictatorial qualities. I think it was the Inspector General's comments, in his written statement he talks about that there are current vulnerabilities, and I think the line is "in violation of existing policy." I mean, you are talking about coming up with a plan over the next few months, but we have already got policy. Part of the problem is that current plans are not being followed.

Also, it concerns me—I would like your comment on that specifically, but then on this general issue—the Inspector General also made a comment that, I think he used the phrase "all of the Department's operating elements have not responded to this report" that he just came out with. That seems to be of concern.

So in your written statement, when you are talking about strict compliance, apparently that word has not gotten down today to the operating elements out there. Would you discuss that issue?

Secretary PRINCIPI. Yes, sir.

Dr. SNYDER. I guess generally, how have you communicated throughout the VA system that you expect strict compliance with these issues, and how are you going to bring that about in the future?

Secretary PRINCIPI. Well, certainly strict compliance is just that, Dr. Snyder. I expect everyone to adhere to the policies, procedures, and priorities that I lay out. And of course, I consult with my under secretaries in formulating those plans and policies, but once they are established there is no deviation without good reason. There is always, perhaps, an exception.

But no, I grew up that way. I grew up with strict accountability. I mean, I was a naval officer a good part of my life, and you are held strictly accountable for your actions. And I intend to hold my people accountable, just as I expect you to hold me accountable. I don't want to be back here 6 months or a year. I don't want to go through this again. I want to show demonstrable improvement in our IT program. I am not a glutton for punishment.

And plus, I feel we have an enormous responsibility to our stakeholders to do the job and do the job well. And when we are spending money and we are not achieving our purposes, then something needs to be fixed.

So I will convey that message, and the CIO will be there to ensure that we are responsive, and that I know what is going on, so that if the IG submits a report—and I am not sure, I try to read every IG report. And I have read every IG report since I have been there. And I always look for the comments and the recommendations from either Dr. Garthwaite or Mr. Thompson. And we have discussed it on several points. I am not sure it was on IT. So I have not seen anywhere we have not responded to the IG. That would be wrong, and I will look into that.

Dr. SNYDER. Yes, I will just read. I mean, again, “while not”—this is from the IG's statement today—“while not all of the Department's operating elements have responded to our review findings”—it seems like someone is not responding, which is in contrast with your comment that you want strict compliance. And also, apparently, now coming from the President that he expects this to get fixed. I appreciate your comments today.

Secretary PRINCIPI. I assure you that was the case, sir. You know, I think a problem, I think we oftentimes, if not all times, we respond to the findings of the IG. But sometimes we don't follow through on the recommendations. We may say, we concur with recommendation one through four, and then 6 months later we haven't followed through. And it may be that case. But either way, we need to do better.

Dr. SNYDER. Thank you, sir.

Secretary PRINCIPI. Thank you, sir.

Mr. BUYER. Mr. Udall.

Mr. UDALL. Thank you very much, Mr. Chairman. I would first like to just ask the committee unanimous consent to put my statement into the record.

Mr. BUYER. No objection.

[The prepared statement of Congressman Udall appears on p. 32.]

Mr. UDALL. Thank you. And Secretary Principi, thank you very much for your very forceful statement and your desire, I think, to get this situation under control.

You note in your testimony that you have created a Senior Executive Service level cyber-security director position. And I may have missed this; is one of these gentlemen that individual that is with you here?

Secretary PRINCIPI. Oh, sure. Mr. Brody, please stand.

Mr. UDALL. Okay.

Secretary PRINCIPI. Mr. Brody is the new—if not the first in government, certainly one of the first cyber-security czar positions that we have established. And he will be overseeing this entire security program for the VA.

Mr. UDALL. Okay, great. Now we know what one looks like. (Laughter.)

Secretary PRINCIPI. I know, I gave it away.

Mr. UDALL. Could you tell us what direction you have given him, and based on today's testimony or what you may have seen from the earlier panels, what you would tell him based on today's testimony?

Secretary PRINCIPI. Certainly, sir. I see it in the short-term, the mid-term and the long-term.

In the short-term, I expect him to perform an independent technical assessment of the security programs throughout the VA, and to develop a strategic road map with milestones. In the medium-term, I expect to have all of the IG recommendations implemented, and GAO recommendations implemented as well. Recommendations that need to be addressed include: inadequate password management and controls; information security office positions not fully staffed; information technology contingency planning not complete; and security risk assessment not completed; security incidents not reported to the VA CIO.

Over the long-term, I expect the security czar to establish active testing and monitoring to support oversight responsibilities and integrate security requirements into VA's enterprise security management.

Mr. UDALL. Thank you.

Secretary PRINCIPI. So that is where I want him to start over the next 30, 60, 90 days. And then we will modify that in accordance to what the committee believes we should be doing. But that is, I think, the beginning point over the next 90 to 120 days, sir.

Mr. UDALL. Thank you, Mr. Secretary. Now, I would like to change direction a little bit and focus on some of the IT successes. The VA has had some IT successes, and I want to commend Benefits Under Secretary Joe Thompson, for instance, for implementing a phone system that is a genuine IT improvement, and has cut away and cut down on blocked calls. Mr. Secretary, would you or Mr. Thompson elaborate on how the VBA's PIES system has improved records retrieval?

Mr. THOMPSON. The Personnel Information Exchange System (PIES) is a way of securing personnel records from the center in

St. Louis. Traditionally you would fill out a piece of paper in a regional office and it would go into the mail. They would receive it in St. Louis and then, somewhere along the line, send the records back to you. PIES has, in effect, put that process on-line, so if you are sitting in a regional office and need a veteran's record, you can request it directly on-line. The request goes directly to the National Personnel Records Center in St. Louis, and then the records are sent back to you. So it obviously allows us to do it much faster and much cheaper, and pay claims more quickly for veterans.

Mr. UDALL. Thank you very much. And thank you, Mr. Chairman.

Mr. BUYER. Mr. Secretary, I want to compliment you and your staff for coming here today.

Secretary PRINCIPI. Thank you, sir.

Mr. BUYER. I wasn't prepared for such a stern statement. But I am pleased. It is not something I am used to. Usually, you get sort of a statement, and you have to work hard to figure out how to get the right answer. You have come in here, I believe with a swift hand, and said, I am going to take control of something that doesn't look right, smell right or feel right.

So with that, I am going to pause and permit you to act as a leader. And so we are going to watch and observe and conduct our oversight. The GAO has done enough, they have laid out the record. The IG has laid out the record. This subcommittee has been on this issue for the last 3 years. And so we are going to watch. We are going to observe. And we are going to give you that opportunity to exercise your leadership.

I think you have sent the right signal out there, that not a dime is going to be spent. You will have the attentive ear of a lot of different companies out there in the private sector who are eager to assist you in your endeavor. Congress is eager to also assist you. If monies are needed, we will be there to step in and do that, because I think the American people are pretty concerned on the privacy issue.

Now we, in our accountability function of how we spend the taxpayer dollar, sure, we don't want fraud, we are embarrassed by those types of things. But this privacy issue is not going to go away.

In 1964, right across the street, a Supreme Court Justice, on the issue of obscenity, said—Justice Stewart said, "I know it when I see it." On the issue of privacy, I believe it is you know it when you feel it. That is Steve Buyer's quote. Why? Because it is also subjective. Everybody has their own sense of privacy. What may concern me may not concern someone else.

But there needs to be a strong standard, because if in fact you are going to be the world-class organization, and look out for the care and concerns of the veterans, we have to take very seriously that private information that is out there, and how we secure it from the outside and from the inside.

So Mr. Secretary, I will have some other follow-up questions for the record we will submit to you. And I want to thank you for your appearance before this subcommittee, and of your staff.

Secretary PRINCIPI. Great pleasure. Thank you, sir.

Mr. BUYER. Thank you.

Secretary PRINCIPI. Pleased to be here.

Mr. BUYER. This hearing is concluded.

[Whereupon, at 11:58 a.m., the subcommittee was adjourned.]

# APPENDIX

---

## PREPARED STATEMENT OF CHAIRMAN EVERETT

I am pleased that Chairman Buyer is continuing vigorous oversight in regard to the Veterans Affairs Information Technology Program.

During my tenure as chairman of this subcommittee, I was determined to find out why the VA, despite both congressional encouragement and generous funding for modernization efforts, had not been successful in developing and implementing its new computer system. Billion of dollars, a large portion of which the agency still can't account for, had been spent. But, poor management and years of poorly focused and coordinated information technology had stood in the way of bringing the VA's databases together to provide seamless service to veterans as "One VA". As our investigation continued, I was also appalled to find out that not only were the weakness in the IT program standing in the way of veterans getting the service they deserved, serious VA-wide information security vulnerabilities had left the system susceptible to unauthorized penetration. This not only left room for compromising the system by corrupting data and defrauding the government, it meant veterans' personal information was not getting the protection it deserves and requires.

I believe our earlier hearings were a wake up call for this agency. In response, I know that the VA has been working to meet the expectation of veterans and the Congress. But, there is still a long way to go. I look forward to hearing all of the testimony today and hope we will see that the VA is continuing to move in the right direction. I will not be satisfied until there is a quality system up and running so that veterans can experience the positive results and we can restore accountability to the taxpayers funding this program.

**Statement of Congressman Tom Udall—3<sup>rd</sup> Congressional District of New Mexico**  
**House Committee on Veteran's Affairs**  
**Subcommittee on Oversight and investigations**  
**Hearing on Informational Technology**  
**April 4, 2001**

---

Thank you Mr. Chairman:

I want to make a brief comment concerning the subject of today's hearing, that being the VA's Information Technology and automated Information System (AIS) programs.

First, let me commend the VA, particularly Secretary Principi for making the reform of the IT program, and VETSNET, a priority. The reform of the way that the VA uses information technology, is of paramount importance if we are to properly ensure that no unauthorized person can access a veterans most private and personal information. I agree with the Secretary that good medicine is dependent on good communication; because if the VA is to improve the way it provides its services, they must first earn and maintain the trust of our Veterans. Whether that trust comes in the examining room, or in a Veteran being confident that their records are secure, the quality of service must center on an understanding that the VA is doing the best they can to protect the personal interests of the person. Thus, I believe that the focus on reforming the IT program and security posture of the VA is extremely important to improving the overall structure and mission of the Veterans Administration.

I look forward to hearing the testimony before the committee, and I am hopeful that the development of a comprehensive integrated enterprise architecture plan, as well as the necessary audits of the overall system, will be done promptly, professionally, and with very strict accountability.

Thank you Mr. Chairman.

**Majority Leader Dick Armev**  
**Testimony before the Veterans Affairs Committee,**  
**Subcommittee on Oversight and Investigations**  
**April 4, 2001**

Chairman Buyer:

Thank you for conducting this important oversight hearing and for providing me the opportunity to present this testimony.

Last fall, Veterans' Affairs Oversight Subcommittee Chairman Terry Everett held a hearing which revealed that the Department of Veterans' Affairs Inspector General was easily able to penetrate the Veterans Benefits Administration's computer security systems and freely access its computer networks. The personal records of individual veterans applying for benefits were potentially exposed – records that indicate disabilities, mental testing, and financial data. The VA was unaware their systems had been penetrated and thus was unable to assure veterans that their privacy had not been compromised. This despite the fact that the VA had spent well over \$5 billion upgrading its computer systems in the last 5 years.

Unfortunately, the Department of Veterans' Affairs is not the only agency with such a poor track record. Government Oversight Subcommittee Chairman Steve Horn last year conducted a comprehensive review of the Clinton Administration's computer security, which resulted in an overall score of D-. Numerous departments and agencies, which collect volumes of personal information about each of us, received failing grades.

Similarly, a study released last year by the General Accounting Office (GAO), requested by Representative Tauzin and me, revealed that 97% of federal agency web sites failed to meet the privacy standards that the Federal Trade Commission had recommended that Congress impose on the private sector.

The Clinton Administration seemed to have a double standard when it came to protecting personal information. While seeking to impose complicated and cumbersome rules on the private sector, the prior Administration ignored catastrophic problems in its own backyard.

A perfect example of this is the Clinton Administration's eleventh hour imposition of new regulations addressing medical privacy issued under the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA regulations were drafted to address a concern that many Americans have about the privacy of their personal medical records. The lengthy document outlines complicated new requirements for patients to sign authorizations for the release of personal information under specific circumstances.

It is not entirely clear to me how the new rules will actually address real medical privacy harms currently suffered by patients not already covered by tort law or other

remedies. What is clear, however, is that these regulations may have entirely the opposite effect by putting even more private, personally identifiable medical information in the hands of health care bureaucrats.

What has not been widely reported are the rule's new mandates requiring doctors, hospitals, and other health care providers to share patients' personal medical records with the federal government, sometimes without notice or advance warning. (See, for example, Federal Register, Vol. 65, No. 250, December 28, 2000, p. 82802, Sec. 160.310.)

The federal government is probably the single largest collector and compiler of personally identifiable medical information in America. Federal computer databanks are filled with intimate details about the medical histories of millions of Americans—and often the poor, who are least able to monitor and safeguard their own rights. The Medicare and Medicaid systems, the Veterans Health Administration, and other government-run health care programs all collect the kinds of medical information the proposed privacy regulation is supposed to protect. Far from protecting privacy, the proposed regulation actually provides the federal government with more access to personal medical records.

This "Trust me, I'm from the government" approach just won't wash. People who are concerned about having their medical histories wind up in the wrong hands don't care whether it is their doctor or their government that threatens their privacy. They want their privacy protected. In short, this proposed regulation puts the medical privacy of millions of Americans at risk.

Handing sensitive medical records to federal departments and agencies which are ill-equipped to protect that information is not a solution; it is inviting abuse, errors, scandal, and tragedy.

Fortunately, the Bush Administration seems to be more willing to lead by example when it comes to protecting personal information. I appreciate the fact that the problems with the VA computer system have reached the personal attention of Secretary Principi. I am confident that he is committed to taking the steps necessary to correct the problems he inherited. Likewise, Secretary Thompson has recently expressed his willingness to review and reconsider the Clinton Administration's HIPAA regulations.

Thank you again, Chairman Buyer for your leadership on this important issue. Figuring out how to protect sensitive personal information in today's high-tech world is no easy task. But one thing is certain, the federal government needs to improve its ability to protect the privacy of the American people.

I look forward to working with you, Mr. Chairman, and Secretary Principi to ensure that America's veterans can feel confident that their personal medical records are safe and secure.

**VA'S INFORMATION SECURITY PROGRAM****TESTIMONY OF  
RICHARD J. GRIFFIN  
INSPECTOR GENERAL  
OFFICE OF INSPECTOR GENERAL  
DEPARTMENT OF VETERANS AFFAIRS****HOUSE COMMITTEE ON VETERANS' AFFAIRS  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

(April 4, 2001)

Mr. Chairman and Members of the Subcommittee, I am here today to report on our ongoing work concerning the Department of Veterans Affairs (VA) Automated Information System (AIS) security program. During the past several years, the Office of Inspector General (OIG) has reviewed selected VA computer security issues and has identified Department-wide weaknesses in AIS security that continue to make VA's programs and financial data vulnerable to destruction, manipulation, and inappropriate disclosure. As a result of these information security weaknesses, since Fiscal Year (FY) 1998 the Department has designated information security as a material weakness under the Federal Manager's Financial Integrity Act (FMFIA).

Given the significant information security weaknesses that exist in VA, the OIG continues to focus audit coverage in the AIS program area. This effort includes an evaluation of the Department's implementation of the computer security requirements of the *Government Information Security Reform Act*. Our audit work is directed toward identifying areas where the Department's effort needs to be enhanced to help assure that a comprehensive Department-wide information security program is put in place.

Our current assessment of VA's AIS program is being accomplished as part of the following initiatives:

- National audit of information security in VA.
- Annual audit of VA's Consolidated Financial Statements (CFS).
- Combined Assessment Program (CAP) reviews of VA facilities

Our review results indicate that, since our September 21, 2000 testimony to this Subcommittee on VA's information security program, the Department has taken a number of planning initiatives to enhance its AIS security posture and comply with the *Government Information Security Reform Act*. While implementation of these initiatives is in process, our review effort continues to identify significant information security vulnerabilities that place the Department at risk of unauthorized access and sensitive data at risk of unauthorized disclosure.

These vulnerabilities exist throughout the Department's operating elements involving health care and benefits, and reflect a continuing number of security control weaknesses that must be corrected before VA can achieve an effective AIS posture. During the course of our national information security audit, we advised the Department of our review results so that prompt corrective actions could be taken to address the vulnerabilities identified. Unfortunately, a number of the identified vulnerability areas were previously reported to VA and exist in violation of VA policy guidance. While not all of the Department's operating elements have responded to our review findings, those that did respond, replied positively and have indicated that actions are being taken to address the vulnerabilities identified.

Given the serious nature of VA's information security weaknesses, computer security should continue to be identified as a Departmental material weakness area under the FMFIA. However, we believe that with more effective security management, oversight, and control over its systems and data, the Department can enhance its AIS security posture and move toward correction of this material weakness. A key step in this process

would be the expeditious appointment of a Department level Chief Information Officer (CIO) to provide necessary leadership and direction over VA's information security program.

Maintaining effective information security is a must for the Department if it is to adequately assure effective control over sensitive information, ensure continuity of operations, and support the Department's missions of providing patient care and the delivery of benefits to our nation's veterans.

A summary of our current information security review effort follows.

#### **National Audit of Information Security in VA**

Audit results indicate that the Department has prepared a comprehensive plan for a department-wide improvement of information security, but much work remains to be done to implement necessary security enhancements.

Key finding areas include:

##### **Timelines for addressing some security vulnerabilities need to be shorter**

Our review of VA's draft Information Security Management Plan found that it included key actions needed to help enhance department-wide information security. The plan also establishes responsibilities of key officials and committees for management, oversight, and implementation of security action areas. However, we found that the plan included unacceptably long timelines (completion in FY 2002-2003) for addressing the following key security vulnerabilities:

- Staffing effective Information Security Officer (ISO) positions to provide adequate oversight and implementation of necessary security control measures at the local facility level.
- Implementing department-wide intrusion detection to reduce VA's vulnerability to inappropriate and undetected access to its systems and data.
- Deploying department-wide antivirus regime to better prevent/contain virus outbreaks that continue to occur in VA and cause disruption of services, adversely affect staff productivity, and divert technical staff efforts.
- Upgrading to VA-standard external electronic connections to reduce the vulnerability of VA's systems to penetration because of weaknesses in its external connections.

During the review we advised the Department's Acting Assistant Secretary for Information and Technology that VA needed to expedite its implementation of these action items in order to provide the security protection that is needed now, and in the future. The Acting Assistant Secretary agreed to amend the plan with accelerated implementation actions in these areas.

##### **Vulnerabilities to unauthorized access and misuse of sensitive automated information and data need to be addressed**

From December 2000 through March 2001, we completed a series of electronic probes of VA systems in VA Central Office (VACO), at two data centers, and at selected medical centers and benefits offices that identified potential vulnerabilities and risks to unauthorized access and misuse of sensitive VA information and data. Based on the results of our vulnerability assessments at key VA facilities and operations, we believe that these system vulnerabilities and risks are widespread throughout the Department's operating elements and reflect a continuing unacceptable level of security and control weaknesses that must be addressed before VA can achieve an effective information security posture. We found that many of these vulnerabilities exist in violation of existing VA policy. Examples of serious vulnerabilities included:

- Inadequate user identifications and passwords that can provide opportunity for unauthorized access to sensitive information and data on individual computers and network resources.
- Program patches not installed that result in use of outdated system software and security vulnerabilities.
- Workstation access not restricted.
- Use of active modems that can allow attackers to circumvent network security.
- Use of remote access software that can provide inappropriate access to individual computers.
- Use of enumerator techniques that allow a user to connect to a network anonymously, providing no ability to identify and track a user's activity.

Given the significance of the security vulnerabilities identified, we provided the Department with information identifying the vulnerabilities and the suggested corrective actions to either eliminate or reduce the vulnerabilities. The Department responses we have received indicate that actions are being initiated to address the vulnerabilities identified.

*More centralized information security oversight and control is needed over VACO Network operations*

We found that the Department could enhance the overall security posture of VACO network activities by implementing a centralized organization structure for security oversight and management. Currently, the Office of the Acting Assistant Secretary for Information and Technology does not have security management control over significant parts of the VACO network, which was referred to by a senior VA official as more of a "confederation" and not a network. Authority over operation of parts of the VACO network is decentralized to 10 system administrators, providing the opportunity for varying levels of security controls and the existence of the security vulnerabilities that we identified during our vulnerability assessment. Centralized management over network operations would provide the opportunity to assure more consistent security control measures are in place and reduce the system vulnerabilities that exist.

*Desktop computers used in VA's automated systems should meet minimum acceptable security standards*

Our security vulnerability assessment of VACO and field facilities found that one cause for the significant number of system security vulnerabilities identified was that minimum acceptable security standards were not followed concerning desktop computers used in VA's automated systems. For example, our review of security vulnerabilities in the VACO network found that 461 desktop computers connected to the network were using operating systems that do not meet minimum security configuration standards recommended by VA's Information Technology Support Service. The security vulnerability associated with using these operating systems is that they can provide an unauthorized user with access to any data stored on the computer. A skilled user could add unauthorized applications that could be used to find passwords, access codes, or other sensitive information. These types of desktop computers are also being used throughout the Department at medical center and regional office facilities.

*Physical security weaknesses continue to place the Department's data center operations at VACO and the Austin Automation Center (AAC) at risk*

Our physical security assessment of the VACO and AAC data centers found that physical security weaknesses place the continuity of operations of the centers at risk.

- VACO—The data center at the 810 Vermont Avenue building is located below ground level despite federal standards describing this as the least desirable location due to potential flooding from water mains and surface water runoff. In addition to these risks, the data center is located below and next to toilets, and below a cafeteria from which water, in 1998, had gotten into the data center room. A sewer backup in 1996, had also flooded the data center. While these events have not resulted in any damage to equipment or disrupted data center operations,

the risk of damage to equipment and continuity of operations could be reduced by moving the center to a more appropriate location. A 1995 OIG audit recommended such a move, but no action was taken to relocate the data center.

- AAC—Parking is allowed too close to the AAC building. This situation increases the risk of potential damage to center equipment and operations and injury to employees who provide critical automation support to the Department. A 1996 OIG audit recommended that parking areas next to the building be eliminated, but vehicle parking next to the building continues.

*VA facility responses to our information security survey identified significant security weakness areas*

We have recently surveyed VA field facilities nationally to determine the implementation status of information security policy, procedures, and controls that are necessary to establish an effective security posture and adequately protect the sensitive information and data maintained. The survey responses identified a number of areas where local facilities had not implemented existing security policy, procedures, and controls, allowing the opportunity for increased risk for inappropriate access and disclosure of sensitive information. Key weakness areas included:

- Inadequate password management and controls.
- Information security officer positions not fully staffed.
- Information technology contingency planning not completed.
- Security risk assessments not completed.
- Security incidents not reported to the VA Critical Information Response Capability.
- Operating uncertified Independent Internet Gateways. (Issue was previously reported in OIG audits completed in 1993 and 1998.)

We advised the Chief Information Officers (CIO) in the Veterans Benefits Administration, Veterans Health Administration (VHA), and National Cemetery Administration requesting that they review the survey results and take appropriate actions to address the security issues identified. The VHA CIO has been very responsive in addressing the vulnerabilities identified, and has provided us with detailed corrective actions taken to address the identified vulnerability areas.

**Computer Security Implications from the 2000 Consolidated Financial Statements Audit**

VA's program and financial data continue to be at risk due to serious problems related to the Department's control and oversight of access to its information systems. These weaknesses placed sensitive information, including financial data and sensitive veteran medical and benefit information, at increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. The OIG has reported this condition in its FY 1997, 1998, and 1999 audit reports on the Department's Consolidated Financial Statements.

Our review noted weaknesses in the application program change controls and operating system change controls at certain data centers and selected medical centers. Weaknesses included:

- Inappropriate access capabilities by application programmers and system support staff to production data.
- Lack of application change procedures.
- Inadequate procedures for testing, approving, and migrating system software changes.
- Inadequate application program change tracking procedures.

We recommended that improved controls over program and operating system changes be instituted, communicated, and enforced throughout the data and medical center network.

The weaknesses found in the effectiveness of the information technology security controls contributed to our conclusion that VA is not in full compliance with the information security control requirements of Office of Management and Budget Circular A-130.

**Combined Assessment Program (CAP) Reviews of Facility Information Security**

Our CAP reviews provide an independent and objective assessment of key operations and programs at VA Medical Centers (VAMC) and Regional Offices (RO) on a cyclical basis. These reviews, which identify operational problems on an ongoing basis, continue to identify security weaknesses that need to be addressed. Since our September 21, 2000 testimony before this Subcommittee, CAP reviews completed at facilities this year have identified the following key security control weaknesses:

- A full-time ISO position had not been established.
- Strong password controls had not been implemented to reduce the risk of unauthorized access to VA systems.
- User access levels needed to be promptly updated to reflect current access requirements.
- Physical security of computer room and equipment needed to be strengthened.
- Annual AIS security awareness training had not been provided.
- Facility information system risk assessment and contingency plans needed to be developed to help ensure continuity of operations.

In response to each of the information security weaknesses identified, facility management agreed to take the necessary corrective actions that we had recommended. Additionally, VHA has issued national guidance to the Veterans Integrated Service Networks to implement security enhancements that should also help address the weaknesses identified.

This concludes my testimony. I would be pleased to answer any questions that you and the members of the subcommittee may have.

---

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations,  
Committee on Veterans' Affairs, House of Representatives

---

For Release on Delivery  
Expected at  
10 a.m. EDT  
Wednesday,  
April 4, 2001

# VA INFORMATION TECHNOLOGY

## Important Initiatives Begun, Yet Serious Vulnerabilities Persist

Statement of David L. McClure  
Director, Information Technology Management Issues



---

GAO-01-550T

Mr. Chairman and Members of the Subcommittee:

We appreciate the opportunity to join in today's hearing and share updated information on the Department of Veterans Affairs' (VA) information technology (IT) program. As you know, IT is essential to VA's ability to effectively serve the veteran population and is the cornerstone of the department's "One VA" vision of providing seamless services to veterans and their families.

Over the past 5 years, VA has spent about \$1 billion each year in support of its IT program, and it expects its IT expenditures to continue increasing over the next 5 years—from about \$1.4 billion in fiscal year 2001 to more than \$2.1 billion by fiscal year 2005. Yet, as we have testified and reported in the past,<sup>1</sup> the department has encountered numerous and consistent challenges associated with managing IT, including weaknesses in its processes for selecting, controlling, and evaluating investments; the absence of a departmentwide enterprise architecture; and ineffective computer security management.

At your request, we have conducted work to review the status of VA's efforts to continue to improve its overall IT management in response to concerns raised by our past reviews. In my remarks today, I will discuss VA's actions to

- fill its chief information officer (CIO) position;
- improve computer security, including securing its on-line compensation and pension applications;
- improve its processes for selecting, controlling, and evaluating IT investments;
- complete an enterprise architecture; and
- utilize the Veterans Health Administration's (VHA) Decision Support System and implement the Veterans Benefits Administration's (VBA) compensation and pension replacement project.

---

<sup>1</sup>VA *Information Technology: Progress Continues Although Vulnerabilities Remain* (GAO/T-AIMD-00-321, September 21, 2000); *Information Technology: VA Actions Needed to Implement Critical Reforms* (GAO/AIMD-00-226, August 16, 2000); *Information Technology: Update on VA Actions to Implement Critical Reforms* (GAO/T-AIMD-00-74, May 11, 2000); *VA Information Technology: Improvements Needed to Implement Legislative Reforms* (GAO/AIMD-98-154, July 7, 1998).

Collectively, these areas represent critically important challenges that VA needs to fully address if it is to successfully fulfill its goal of improving service delivery to veterans through the use of information technology.

#### RESULTS IN BRIEF

VA is continuing to make progress in improving its overall IT management; however, important actions in several areas remain incomplete and require continued attention and decisions from the department's executive management. To begin with, the department has yet to fill the position of assistant secretary for information and technology, created in June 1998 and intended to serve as VA's chief information officer (CIO). It is critical that the department fill this leadership position to help the Secretary's executive management team fully address VA's critical IT challenges and achieve improvements in investment results that support the department's programs and operations.

In the area of computer security, VA has established a department-level information security management program and developed an information security management plan that addresses many of the security concerns that we and VA's Inspector General have identified. In addition, the department has recently hired a senior executive for computer security to demonstrate its commitment to this crucial area. The department has also done a good job in developing and posting privacy and security statements for its primary and secondary Web sites that are consistent with OMB requirements.

However, we remain concerned about the lack of adequate department policy and guidance for security, vulnerability and risk assessments, assessments or reports of threats and incidents, and comprehensive coordinating and monitoring responsibilities for its central security management group. For example, while VBA's Veterans On-Line Application demonstrates attention to short-term security problems we have identified in the past—such as stronger application access and personnel controls—it remains vulnerable to continuing weaknesses in VBA's networks and general support systems. Further, despite strong privacy policy statement postings on its Web sites, we discovered two Web pages that were using persistent "cookies"—a short string of text

sent from a Web server to a Web browser that is often used to recognize returning users and track Web browsing behavior—despite OMB policies limiting their use.

Moreover, VA continues to show progress in improving its guidance used to manage its investments in information technology. However, more concerted actions and discipline are needed to enforce this decisionmaking process, particularly in regard to consistent and complete tracking of IT cost data and critical in-process and post-implementation reviews of projects funded with its existing \$1.4-billion annual IT budget. In addition, the department has not yet developed the integrated, departmentwide enterprise architecture needed to acquire and utilize information systems across VA in a cost-effective and efficient manner.

Lastly, two highly visible projects in the department's IT investment portfolio—VHA's Decision Support System (DSS) and VBA's compensation and pension (C&P) replacement project show progress. However, this latter project has not been fully implemented and both projects face managerial challenges related to their full and successful utilization. Some VHA medical centers and Veterans Integrated Service Networks (VISN) report greater use and specific clinical decisionmaking and resource allocation benefits from DSS usage. Clear top management expectations for its use in the centers and the assignment of staff knowledgeable in the use of the application are cited as important factors for higher use levels. Similarly, VBA's C&P replacement project is benefiting from greater project management attention; a limited pilot test was conducted in February 2001, with no reported problems. However, VBA will continue to face challenges as it attempts to move forward from its pilot to full-scale operational implementation.

**APPOINTMENT OF A CHIEF INFORMATION OFFICER  
IS CRITICAL TO THE SUCCESS OF VA'S IT PROGRAM**

Successful implementation of VA's IT program requires strong leadership and management to help define and guide the department's plans and actions. The Clinger-Cohen Act, passed in 1996,<sup>2</sup> directs the heads of major federal agencies to appoint CIOs to promote improvements in

---

<sup>2</sup>P. L. 104-106, Division E

their agencies' work processes; implement integrated agencywide architectures; and help establish sound investment review processes to select, control, and evaluate IT spending.

In September 2000,<sup>3</sup> we testified about actions VA has taken over the last 3 years toward establishing the CIO position, including separating the CIO function from that of the chief financial officer, and establishing the position of assistant secretary for information and technology to serve as the department-level CIO. To his credit, the newly appointed Secretary of Veterans Affairs has identified filling the department's CIO position as one of his top priorities, and is currently conducting an extensive search to identify suitable candidates for the position, which requires Senate confirmation.

Our recently issued research report on the effective use of CIOs in several leading private and public organizations<sup>4</sup> provides insight into factors contributing to CIO successes. Three key principles stood out:

- First, senior executives must embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making. Specifically, the type of CIO chosen is matched to the organizations' needs. Most important, the top executives of these organizations determined how a CIO would best fit within existing or new management tiers to guide technology solutions.
- Second, effective CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. While placement of the CIO position at an executive management level in the organization is important, effective CIOs earned credibility and produced results by establishing effective working relationships with business unit heads.
- Third, CIOs must structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy

---

<sup>3</sup> GAO/T-AIMD-00-321, September 21, 2000.

<sup>4</sup> *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations* GAO-01-376G, February 2001).

- structures, and available IT skills, this understanding is necessary to ensure that the CIO's office is aligned to best serve the needs of the enterprise.

Despite its creation in 1998 and the current recruitment effort by the Secretary, VA still does not have a person appointed as the departmentwide CIO. Instead, various VA officials have served as acting CIOs for the department during this time. The department's eventual CIO appointee faces challenges that will be difficult to resolve without constant support and involvement of VA's top executives. Under current arrangements, IT systems and services are highly decentralized among VA's administrations and staff offices. Out of VA's approximately \$1.4 billion fiscal year 2001 IT budget, VHA oversees approximately \$762.7 million, VBA approximately \$79.5 million, and the National Cemetery Administration (NCA) approximately \$0.4 million.<sup>5</sup> With such a large annual funding base and a decentralized IT management structure, it is crucial that the CIO ensure that well-established and integrated processes for leading, managing, and controlling IT investments are commonplace and followed throughout the department.

#### INFORMATION SECURITY AND PRIVACY CHALLENGES REMAIN

As you know, 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. If effective computer security practices are not in place, financial and sensitive information contained in VA's systems are at risk of inadvertent or deliberate misuse, fraud, improper disclosure, or destruction—possibly occurring without detection. Likewise, as VA continues to expand its use of Web-based electronic services for interacting with and providing services to veterans, ensuring privacy of sensitive records containing personal information becomes essential.

---

<sup>5</sup> The remaining \$589 million is for VA-wide initiatives in the financial management, human resources, infrastructure, security, architecture, and planning areas.

Steps Taken to Continue to Address  
Recognized Security Weaknesses

Over the past several years, we have issued numerous reports and testimonies on VA's computer security weaknesses. Most recently, in September 2000, we reported<sup>6</sup> and testified<sup>7</sup> that serious computer security problems persisted throughout VHA and the department because VA had not fully implemented an integrated security management program and VHA had not effectively managed computer security at its medical facilities. Consequently, financial transaction data and personal information on veterans' medical records continued to face increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. We recommended that the department develop computer security guidance and oversight processes, and monitor and resolve coordination issues that could affect the success of the departmentwide computer security program.

VA concurred with our recommendations and continues to take constructive steps to address them. Specifically, it has now established a department-level information security management program and hired an executive-level official to head it. In addition, in November 2000, it finalized an information security management plan that provides a framework for addressing departmentwide information security on a near- and long-term basis. The plan addresses some of the longstanding departmentwide security problems that we, VA's Office of Inspector General, and the department's own internal reviews have identified. The plan also responds to risks documented in a departmentwide risk assessment that VA completed in June 2000, by recommending specific controls to reduce several vulnerabilities.

Additionally, VA's information security management plan emphasizes an accelerated (near-term), enterprisewide improvement of information security that is directed primarily at improving access and personnel controls. The plan identifies eight near-term actions that are to be completed between December 1, 2000 and May 1, 2001, including (1) implementing stronger

---

<sup>6</sup>VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration (GAO/AIMD-00-232, September 8, 2000).

<sup>7</sup>GAO/T-AIMD-00-321, September 21, 2000.

passwords on computer workstations, (2) removing unsecured dial-in connections, and (3) conducting focused reviews of access and personnel controls.

VA's plan also identified a number of long-term actions emphasizing broader assessments and proposed measures to improve information security on a more comprehensive basis. These actions, which are to be implemented between July 1, 2001 and January 1, 2003, include proposals for establishing a regular cycle to test the department's compliance with established security requirements, and provisions for certifying and accrediting general support systems and major applications, as required by OMB Circular A-130.

A Stronger Management Focus Is Needed to  
Resolve Lingerin Departmentwide Security Problems

The success of VA's computer security management program is largely contingent upon how effectively the department manages risks to business operations that rely on its automated and highly interconnected systems. In our 1998 report on effective security practices used by several leading public and private organizations<sup>8</sup> and a companion report on risk-based security approaches in November 1999,<sup>9</sup> we identified key principles that can be used to establish a management framework for more effective information security programs. In our study, we found that the leading organizations we examined applied these principles to ensure that information security addressed risks on an ongoing basis. These have been cited as useful guidance for agencies by the federal CIO Council and incorporated into the Council's recently issued Information Security Assessment Framework, intended for agency self-assessments.<sup>10</sup>

A contributing factor to VA's continuing information security problems is that the department has not yet implemented key components of a comprehensive, integrated security management program. We brought many of these components to the department's attention last September.<sup>11</sup> Establishing its central security group, hiring a new information security executive who will

---

<sup>8</sup>Information Security Management: Learning from Leading Organizations (GAO/AIMD-98-68, May 1998).

<sup>9</sup>Information Security Risk Assessment: Practices of Leading Organizations (GAO/AIMD-00-33, November 1999).

<sup>10</sup>Federal Information Technology Security Assessment Framework, November 28, 2000.

<sup>11</sup>GAO/AIMD-00-232, September 8, 2000.

report to the CIO, and partially implementing its security program plan are positive steps forward, but several critical actions related to our past recommendations and leading security management principles mentioned above require additional work and senior management attention. Let me briefly discuss four specific areas:

- *Security Policy, Procedures, and Guidance.* Up-to-date, comprehensive, and well-communicated information security policies and implementation guidance serve as the foundation for effective information security programs and form the basis for adopting specific procedures and technical controls.<sup>12</sup> However, VA's information security management plan does not include steps for ensuring that policies and procedural guidelines adequately address the security of the department's interconnected computer environment, or that they cover other key security management areas, such as risk identification and categorization. Further, the plan does not include any provisions for developing technical security standards for system and security software. By setting technical security standards for system and security software and routinely evaluating the technical implementation of these standards, VA could eliminate or mitigate security exposure that we previously reported in these areas.
- *Development of Risk-Based Security Assessments.* Our study of computer security best practices found that procedures for conducting risk assessments generally specified (1) how risk assessments should be initiated and conducted, (2) who should participate in the risk assessment, (3) how disagreements should be resolved, (4) what approvals were needed, and (5) how assessments should be documented and maintained. However, VA's information security management plan does not include a requirement for developing policy and guidance related to performing risk assessments on a continuing basis or when significant changes occur.

---

<sup>12</sup> *Federal Information Systems Controls Audit Manual* (GAO/AIMD-12-19-6, January 1999); *Federal Information Technology Security Assessment Framework*, November 28, 2000; GAO/AIMD-00-33, November 1999; and GAO/AIMD-98-68, May 1998.

It also does not require establishing procedures for conducting risk assessments that include the best practices outlined above. Specifically, VA's security policy requires risk to be assessed when significant changes are made to a facility or its computer systems, or at least every 3 years; however, the policy does not provide additional guidance for determining when an event is a significant change, or explaining the level of risk assessment required for system changes. In addition, VA does not have guidance on how the risk assessments should actually be conducted.

- *Monitoring, Testing, and Evaluation.* Over time, policies and procedures run the risk of becoming inadequate by themselves because of changes in threats, changes in operations, or a general deterioration in the degree of agency compliance.<sup>13</sup> Periodic assessments or reports on threat activities can be invaluable for ensuring that adequate protections are in place and identifying needed security program improvements. Keeping summary records of actual security incidents is one way that an organization can measure the frequency of various types of violations as well as the damage suffered from these incidents. In response to our past recommendations, VA now maintains a computer security incident reporting and response process and a related information system. However, its information security management plan does not establish a mechanism for routinely analyzing security incident records. Such a practice could provide VA with an additional process for proactively identifying and responding to other system security vulnerabilities.
- *Central Management Focal Point.* Our leading practices guidance also notes that managing the increased risk associated with a highly interconnected computing environment requires increased central coordination to ensure that weaknesses in one organizational unit's systems do not place the entire organization's information assets at undue risk. A central management group generally coordinates activities associated with all the elements of a comprehensive security program. This includes keeping policies and controls up to date, devising common risk assessment processes, promoting general security awareness, and monitoring an organization's security-related activities by testing controls for general support systems, accounting for the number and types of security incidents, and evaluating

---

<sup>13</sup>GAO/AJMD-00-33, November 1999.

compliance with policies. However, VA's security plan does not require independent monitoring of the near-term actions taken by facilities or responsible units to improve their security. Instead, VA relies on its administrations and staff offices to certify completion of the specific actions. Independent monitoring, however, can provide the CIO and his chief security deputy and the Secretary with assurances that actions were taken as prescribed to remedy the vulnerabilities or that the actions were consistently applied throughout the department.

VBA's On-line Application (VONAPP) Illustrates Strengths and Weaknesses of the Department's Security Program

The inherent risks involved in VA's effort to serve veterans and their families via its on-line application for compensation and pension benefits require the department to have comprehensive and rigorous security measures that protect the integrity, confidentiality, and availability of individuals' data. VBA began making this application available to veterans via the Internet in July 2000, as part of its electronic government initiative.<sup>14</sup> By providing this on-line capability, VA sought to offer veterans an around-the-clock alternative to submitting claims through the mail or in person. Veterans can access the application at VA's Veterans ON-line APPlication (VONAPP) Web site.

This application incorporates several security features for safeguarding the applicant's data and demonstrate implementation of VA's short-term security corrective actions aimed at improving application level access and personnel controls. These features include (1) 128-bit encryption technology to protect the data during transmission, (2) user identification and passwords to control user access to the specific application forms, (3) firewall protection to ensure that the Web and database servers that accept VONAPP applications can only be accessed by other known servers, and (4) access authorizations that are granted on a limited, need-to-know basis.

Nonetheless, this on-line VBA service continues to face potential security vulnerabilities associated with weaknesses with general support systems and operating systems access controls.

---

<sup>14</sup>Application for Compensation and Pension (VA Form 21-1900).

VA has again reported information system security general controls<sup>15</sup> as a material weakness in its February 2001 FMFIA report. VA needs to resolve these weaknesses affecting the overall effectiveness and security of its computer operations. Because VONAPP resides in this computer environment, it is vulnerable to inappropriate access and other security breaches affecting the department's overall computer operations. In addition, independent network assessments performed for VA by contractors last summer identified and made suggestions for correcting various vulnerabilities affecting VONAPP. However, while the contractors' work included reviews of the VONAPP Web and data base servers, it did not address vulnerabilities that have been identified in VA's wide area network, which is used to access VONAPP. Until VA addresses all of the vulnerabilities in its wide area network, it cannot ensure that applicants' data are being adequately safeguarded.

VA Web Sites Provide Privacy Notices, But Internet  
Cookie Compliance Could Be Strengthened

As VA expands its offering of electronic services via the Internet and its various Web sites<sup>16</sup>, protecting electronic records containing personal information becomes increasingly important. Without this protection, veterans may lack the confidence to use the electronic services, and VA in turn may not be able to fully realize the benefits its Internet-based services can provide.

To ensure that individuals are informed about how their personal information is handled when they visit federal Web sites, in June 1999 OMB issued a policy memorandum requiring federal agencies to post privacy policies on their Internet Web sites<sup>17</sup>. The memorandum requires agencies to post easily accessible and clearly labeled privacy policies to their department or agency principal Web sites and to any other known, major entry points to their Web sites, as well

---

<sup>15</sup>General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data and programs is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

<sup>16</sup>A Web site is a collection of files that covers a particular theme or subject and is managed by a particular person or organization. These files are called Web pages and are usually based on hypertext markup language that may contain such elements as text, graphics, on-line audio, or video. As of February 21, 2001, VA reported having 395,587 Web pages on its Internet Web site.

<sup>17</sup>OMB Memorandum M-99-18, June 1999.

as any Web pages where they collect substantial personal information from the public. These policies must clearly and concisely inform visitors to the Web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it. In addition, a June 22, 2000, memorandum from OMB regarding privacy policy and data collection on federal Web sites states that federal agencies and contractors should not use persistent cookies<sup>18</sup> on their sites unless they provide "clear and conspicuous notice" of those activities and meet certain specified conditions.<sup>19</sup> Put simply, a persistent cookie is a short string of text sent from a Web server to a Web browser that is often used to recognize returning users and track Web site browsing behavior.

VA's Web sites provide a variety of information and services to its visitors. For example, table 1 provides information on VA Web sites where individuals can electronically access and complete ten specific application forms on-line. In accordance with OMB's Web privacy requirements, VA has developed a privacy and security statement for its primary Web site, [www.va.gov](http://www.va.gov). In addition, VA requires its administrations and staff offices to link their individual Web sites to the primary site or to post privacy policies on their individual sites that are consistent with OMB's guidance. The privacy and security statements posted on VA's primary and related Web sites are consistent with OMB's requirements for being clear, concise, clearly labeled, and easily accessed.

---

<sup>18</sup>Persistent cookies specify expiration dates, remain stored on the client's computer until the expiration date, and can be used to track users' browsing behaviors by identifying their Internet addresses whenever they return to a site.

<sup>19</sup>These conditions are (1) a compelling need to gather the data on the site, (2) appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (3) personal approval of the agency head

Table 1. VA Application Forms on the Internet.<sup>a</sup>

VA Administration <sup>b</sup>	VA form number	Application form	Description	VA Web address
VHA	10-10EZ	Application for Health Benefits	Application to enroll for health benefits	<a href="http://www.1010ez.med.va.gov/sec/vha/1010ez/">http://www.1010ez.med.va.gov/sec/vha/1010ez/</a>
VHA	10-2850	Application for Physicians, Dentists, Podiatrists, and Optometrists	Application for employment	<a href="http://www.vacareers.com/pages/3.b.3.x.htm">http://www.vacareers.com/pages/3.b.3.x.htm</a>
VHA	10-2850a	Application for Nurses and Nurse Anesthetists	Application for employment	<a href="http://www.vacareers.com">Http://www.vacareers.com</a>
VHA	10-2850c	Application for Associated Health Occupations	Application for employment for occupational therapists, pharmacists, etc.	<a href="http://www.vacareers.com">http://www.vacareers.com</a>
VBA	21-1900	Veterans Online APPLICATION (VONAPP)	Applications for compensation and pension benefits and for vocational rehabilitation benefits	<a href="http://www.vabenefits.vba.va.gov">http://www.vabenefits.vba.va.gov</a>
VBA	22-1999 22-1999b	VA Online Certification (VAnetCert)	Application for school officials to certify eligibility for educational benefits	<a href="http://www.gibill.va.gov">http://www.gibill.va.gov</a>
VBA	22-8979	Web Automated Verification of Enrollment (WAVE)	Application for education enrollment reporting	<a href="http://www.gibill.va.gov">http://www.gibill.va.gov</a>
VBA	26-1805	Request for Determination of Reasonable Value (via VA Assignment System)	Application requesting a determination of reasonable value for realty used as security for VA mortgages	<a href="http://vaas.vba.va.gov/prod/vaas/indexnew.cfm">http://vaas.vba.va.gov/prod/vaas/indexnew.cfm</a>

<sup>a</sup> Two of the on-line applications—VAnetCert and WAVE—are not currently accessible via the Internet and thus were not available for our evaluation.

<sup>b</sup> NCA does not provide on-line applications for public use.

In addition, we confirmed that other VA Web sites providing forms that may be downloaded<sup>20</sup> also contain links to the privacy and security statement posted on VA's primary Web site. And as further evidence of the department's attention to privacy policies, VA Web sites containing the applications for health benefits and for compensation and pension and vocational rehabilitation require users to acknowledge that they have read additional privacy notices prior to providing personal information.

While VA has adhered to Web privacy requirements, it has not consistently adhered to OMB's requirement limiting the use of persistent cookies. In interviews with VA Privacy Act officials and Webmasters, we were told that the department was in compliance with the OMB policy and did not use persistent cookies on its Internet Web sites. However, during the course of our work, we identified and informed VA of persistent cookies on two Web pages used to access VBA on-line applications. In discussing this finding, VA's Privacy Act officer said that VBA did not have departmental approval to use these cookies, and stated that the department would look into the matter.

**IMPROVEMENTS MADE IN VA'S IT INVESTMENT MANAGEMENT,  
BUT CHALLENGES REMAIN**

IT investment management processes provide a systematic method for agencies to minimize risks while maximizing their return on IT investments. Our September 2000 testimony<sup>21</sup> pointed out that while VA had improved its processes for selecting, monitoring, and managing Capital Investment Board (CIB)-level projects, a more structured decision process was needed for IT projects below the CIB threshold. Moreover, we noted that VA needed to conduct more timely in-process reviews and provide lessons learned from post-implementation reviews to key decisionmakers, such as investment panel members. In-process reviews are essential because they enable management to make informed, data-driven decisions about the progress of IT

---

<sup>20</sup>VA administrations' Web sites contain 114 public-use forms that individuals can download and submit to the department through means other than these Web sites.

<sup>21</sup>GAO/T-AIMD-00-321, September 21, 2000.

projects at key milestones in their life cycles, including whether to cancel, modify, or continue the projects. In addition, post-implementation reviews at the conclusion of key project phases provide critical information that management can use to validate projected savings and identify needed changes in systems development and IT management practices.

Subsequent to our September testimony, VA provided us its *Information Technology Capital Investment Guide*. Intended as departmentwide guidance for use in each of VA's components, it provides comprehensive guidelines for processes to be used in managing the department's IT investments. The guide addresses a number of shortcomings we previously identified with VA's investment management process and reflects the attention that the department has devoted to improving the process.

Let me mention a few of these positive changes. Specifically, for projects below the CIB dollar threshold, VA now requires its administrations and offices to evaluate and report on the progress of its IT projects at predetermined intervals. For example, organizations are to submit to the director of VA's Information Resources Management Planning and Acquisitions Service quarterly project status reports summarizing accomplishments, problems encountered, and corrective actions taken. In addition to these reports, organizations are to notify the director of any significant changes to the overall project, plan, schedule, or benefit-cost information at the time those changes are made. The guide also requires administrations and staff offices to manage smaller IT projects, and to track IT expenditures and other data. Further, consistent with our prior recommendations, VA has stipulated in the guide that completion dates be included in in-process review plans and that the results of post-implementation reviews of CIB-level projects be provided to VA's CIO Council.

Nevertheless, VA has not yet demonstrated that it is implementing key parts of its investment guidance. For example, since September 2000, it has not scheduled or conducted any in-process or post-implementation reviews. VA has indicated that it intends to conduct one in-process review (of its E-Commerce system) and three post-implementation reviews. However, at the

conclusion of our work last month, VA had not established plans or schedules indicating when they would be conducted. In addition, although the guidance requires VA to conduct quarterly execution reviews of approved IT capital investments to help identify projects experiencing cost, schedule, or performance problems (and thus candidates for in-process reviews), the Director of VA's IRM Planning and Acquisition Service stated that VA has not conducted an IT execution review since June 2000.

We also testified last September<sup>22</sup> that VA had not implemented a uniform mechanism for collecting, automating, and processing data on IT costs and performance across the department. At that time, VBA tracked IT expenditures centrally, while VHA delegated responsibility for tracking approximately 80 percent of its IT expenditures to the 22 VISNs. Further, neither of these administrations tracked personnel costs associated with their IT projects because of the limitations of VA's financial management system.

A uniform cost-tracking mechanism should provide data needed to monitor and evaluate investments individually and strategically, provide feedback on the project's adherence to strategic initiatives and plans, and allow for review of unexpected costs or benefits that resulted from investment decisions.<sup>23</sup> An expenditure tracking mechanism would also aid the department in meeting the requirements of its own Directive 6000, which requires officials to maintain complete and accurate data on all personnel and nonpersonnel costs associated with IT activities.

According to the director of IRM Planning and Acquisition Service, VA will begin using a numbering system within the financial management system to track IT capital investment costs beginning with the execution of fiscal year 2002 projects. Using this numbering system, the Information Resources Management Planning and Acquisitions Service will run special reports on project expenditures on an as-needed basis. However, the system will not allow VA to track personnel costs for IT projects automatically. VA plans to extend the numbering scheme to other

---

<sup>22</sup>GAO/AIMD-00-321, September 21, 2000.

<sup>23</sup>GAO/AIMD-10-123.

projects once its new financial management system is implemented in October 2004. In the interim, the VA CIO Council is investigating the use of a universal project management tool with personnel tracking capability.

VA REMAINS WITHOUT AN  
ENTERPRISEWIDE ARCHITECTURE

The Clinger-Cohen Act and Office of Management and Budget guidelines direct agency CIOs to implement an architecture to provide a framework for evolving or maintaining existing IT and for acquiring new IT to achieve the agency's strategic goals. Leading organizations both in the private sector and in government use enterprise architectures to guide mission-critical systems development and to ensure the appropriate integration of information systems through common standards.<sup>24</sup> Further, in recently issued guidance,<sup>25</sup> the CIO Council has emphasized the importance of enterprise architectures for evolving information systems and developing new systems that optimize an organization's mission value.

In previous testimony, we noted that VA had adopted the National Institute of Standards and Technology (NIST) five-layer model<sup>26</sup> as the framework that it planned to use for its departmentwide IT architecture. VA also published a departmentwide technical architecture<sup>27</sup> which described one layer—the technology layer—of the NIST model. In response to a May 11, 2000,<sup>28</sup> hearing, the former Chairman of this Subcommittee requested that VA provide a plan and milestones for completing the logical portion of its departmentwide architecture within 60 days of that hearing. VA subsequently submitted a two-page plan to the Subcommittee that provided a high-level discussion of VA's approach to developing a departmentwide logical architecture and time estimates for various deliverables. The approach outlined in the plan called for each VA administration to develop its own logical architecture, but to avoid duplicating the

<sup>24</sup> *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology—Learning from Leading Organizations* (GAO/AIMD-94-115, May 1994).

<sup>25</sup> *A Practical Guide to Federal Enterprise Architecture*, February 2001, Federal Architecture Working Group and Federal Chief Information Officers Council.

<sup>26</sup> The five layers are business processes, information flows and relationships, applications processing, data descriptions, and technology. This provides a framework for defining an IT architecture.

<sup>27</sup> *VA Technical Architecture: Technical Reference Model and Standards Profile*, May 1999.

<sup>28</sup> GAO/T-AIMD-00-74, May 11, 2000.

administrations' efforts, VA planned to develop a departmentwide component that focused on crosscutting issues and interdependencies. However, as we noted in our September 2000 testimony,<sup>29</sup> this approach would not likely result in an integrated architecture but, rather, in at least three different architectures. Accordingly, we pointed out the need for VA to reassess its strategy and work together with the administrations to develop an integrated, departmentwide logical architecture, consistent with the Clinger-Cohen Act.

Developing an enterprise architecture requires a disciplined and rigorous approach that is endorsed by senior management. The CIO Council's enterprise architecture guide stresses that an enterprise architecture is a corporate asset that should be managed as a formal, long-term program, and that successful execution of the enterprise architecture process is an agencywide endeavor requiring management, allocation of resources, continuity, and coordination. In particular, the architecture development team needs to work closely with agency business line executives to produce a description of the agency's operations, a vision of the future, and an investment and technology strategy for accomplishing defined business goals.

After being confronted with contractor bids for developing the logical architecture for the department that exceeded available resources in October 2000, VA's acting CIO and the administration CIOs agreed to undertake an accelerated in-house effort to develop a draft departmentwide IT architecture by March 2, 2001. This effort was to combine the IT architectural work that had been completed by VA's administrations and offices into one draft IT architecture plan for the department.

As of the end of March 2001, VA had not yet completed the integrated, departmentwide architecture. According to the architecture project manager, the Secretary recently redirected efforts toward developing this architecture and requested that the architecture team prepare a plan detailing a new strategy for developing it. The Secretary was concerned, in part, that VA's business lines had not been adequately integrated in the prior effort to develop the architecture, and has requested that VA business managers be included in the new development effort.

---

<sup>29</sup>GAO/T-AIMD-00-321, September 21, 2000.

TWO SYSTEMS PROJECTS ARE PROGRESSING, BUT FACE CRITICAL CHALLENGES UNDERLYING SUCCESSFUL UTILIZATION

You also asked that we update you on VA's progress with two visible systems projects, VHA's Decision Support System (DSS) and VBA's compensation and pension replacement (C&P) project, one of the major initiatives under the agency's Veterans Service Network (VETSNET) strategy.

DSS is an executive information system designed to provide VHA managers and clinicians with data on patterns of patient care and patient health outcomes, as well as the capability to analyze resource utilization and the cost of providing health care services. In September 2000,<sup>30</sup> we testified that DSS had not been fully utilized since its implementation at all VA medical centers in October 1998. We noted that while cost reductions and improved clinical processes had been reported by some VISNs and medical centers using DSS, none of the ones we had contacted used DSS for all of the purposes VHA intended. At that time, the reasons given by VISNs and medical centers for not making greater use of DSS included (1) concerns about the accuracy and completeness of DSS data and (2) DSS staffing issues, including insufficient staff, staff with inadequate skills, and staff turnover.

Since last September, VHA has made moderate progress in increasing usage of DSS among its VISNs and medical centers. At the time of that testimony, 4 of 22 VISNs—VISN 6 (Durham, North Carolina), VISN 8 (Bay Pines, Florida), VISN 20 (Portland, Oregon), and VISN 21 (San Francisco)—had not provided examples of how they were using DSS. However, in recent discussions with the DSS coordinators at these VISNs, three of the four provided examples of their current use of DSS information or of initiatives underway to facilitate greater use.

For example, to facilitate clinical decisionmaking, these DSS coordinators told us they are using DSS to provide VISN-wide information on:

---

<sup>30</sup> GAO/T-AIMD-00-321, September 21, 2000.

- the pharmacy cost of hepatitis C, radiology utilization for preoperative chest x-rays among eye surgery patients, and the frequency with which pathology laboratory medical tests are administered;
- patient length of stay and cost per case, to help determine the extent to which medical centers are meeting an established performance measure of reducing the cost of chronic obstructive pulmonary disease by 5 percent; and
- a VISN-wide diabetes study to determine what percentage of patients with a primary or secondary diagnosis of diabetes had received certain required testing within a specified time frame.

However, VISN 20 (Portland) reports that it is still not using DSS. According to the DSS coordinator, because of differences in the structural organization of DSS among the VISN's facilities, DSS data maintained by the VISN's medical centers cannot be compared, and thus not readily useable for decisionmaking. For example, she explained that in maintaining primary care data in DSS, a community-based outpatient clinic may include data in its DSS primary care department that extends beyond just primary care work, while the medical facilities only include primary care work in their DSS primary care departments.

Our September testimony<sup>31</sup> also reported on the medical centers' use of DSS. At that time, 59 of 140 centers had not provided specific examples of DSS use.<sup>32</sup> Three of the 59 medical centers—Beckley (West Virginia), Anchorage Health Care System, and Boise (Idaho)—had explicitly stated that they did not use DSS. However, in contrast, two of the medical centers—Long Beach and Portland (Oregon)—reported extensive use of DSS. We met with physicians, nurses, and administrators at these two medical centers to better understand the reasons behind higher DSS usage at these centers. They pointed to numerous positive examples where DSS was useful:

- Changing the clinical practice of admitting elective surgery patients the day of surgery,
- Determining whether physicians are following accepted clinical guidelines for treating atrial fibrillation patients,

<sup>31</sup> GAO/T- AIMD-00-321, September 21, 2000.

<sup>32</sup> These 59 medical centers did not provide specific examples of DSS use in their response to the March 2000 memo. This does not necessarily mean that they were not using DSS. For example, none of the medical centers in VISN 13 provided examples; however, DSS data is used more extensively at the VISN level in that VISN than in any other.

- Determining the location of community-based outpatient clinics to provide service to the most veterans,
- Assessing the quality of care given to a certain cohort of patients,
- Evaluating the effectiveness of a case management model of nursing care delivery, and
- Determining staffing levels and the required mix of nurses for wards.

#### Factors Contributing to Successful Use of DSS

In on-site discussions with officials at the Long Beach and Portland medical centers, they pointed out several factors that had substantially contributed to the successful use of DSS:

- *Top management support*—Each center's director had set an explicit expectation that decisions would be made based on DSS data and that concerns about data quality would not be an acceptable excuse for not using the system.
- *Skilled DSS staff*—At each center, the director had assigned staff with adequate skills to use DSS, thus providing the necessary resources to ensure that it functioned properly and that proper assistance was available to administrators and medical staff in analyzing and using DSS data. Further, the DSS staff was knowledgeable in both the financial and clinical aspects of the centers' work, which substantially facilitated use of the system.
- *Familiarity with DSS and longevity of experience*—DSS had been implemented at the medical centers during the first phase of its implementation, and DSS site managers at both medical centers had been with DSS since its inception.

Efforts encouraging greater VA-wide use of DSS are continuing. Fiscal year 2000 DSS data are being used as part of the fiscal year 2002 resource allocation process; use and validation of DSS data are among the factors that will be considered in determining VISN director year-end performance appraisals; and VISN directors have been required to provide monthly examples of their reports and/or processes that rely on DSS data, and to ensure that the processing of DSS data by their medical centers is current (i.e., no more than 60 days old).

The new DSS program office—established March 11, 2001—is also developing project plans for priority initiatives, which are to be integrated into a business plan by the end of May. Later, through review of best practices and benchmarking, the program office plans to develop opportunities to export and apply measures derived from DSS data. In doing this, it remains critical that VHA continue to provide top management support to ensure that the system is fully utilized and benefits are being realized in both the financial and clinical areas.

THE COMPENSATION AND PENSION PAYMENT SYSTEM  
REPLACEMENT CONTINUES TO FACE CHALLENGES

The C&P project was intended to replace VBA's existing compensation and pension payment systems with one new, state-of-the-art system. The project, which began in April 1996, had an estimated cost of \$8 million and was originally scheduled for completion in May 1998.

Over the years, we and VA have reported on the problems that VBA has encountered in completing this project.<sup>33</sup> Our prior work found that the project had been delayed largely because VBA lacked an integrated architecture defining its business processes, information flows and relationships, business requirements, and data descriptions. Specifically, the project was begun before VBA had fully developed its business requirements and delays subsequently resulted from confusion over the specific requirements to be addressed. In addition, our prior work also attributed the project's problems to VBA's immature software development capability.<sup>34</sup>

Last September, we testified<sup>35</sup> that VBA had changed its strategy for developing this new system to one that utilized and built upon software products developed elsewhere in VBA. At that time, however, VBA did not have an integrated project plan and schedule detailing all of the areas that

---

<sup>33</sup>*Veterans Benefits Modernization: Management and Technical Weaknesses Must Be Overcome if Modernization Is To Succeed* (GAO/T-AIMD-96-103, June 19, 1996), *Veterans Benefits Computer Systems: Risks of VBA's Year 2000 Program* (GAO/AIMD-97-79, May 30, 1997), and *VETSNET Quarterly Review*, Office of Information Resources Management, Department of Veterans Affairs, March 1998.

<sup>34</sup>*Veterans Benefits Modernization: VBA Has Begun to Address Software Development Weaknesses But Work Remains* (GAO/AIMD-97-154, September 15, 1997).

<sup>35</sup> GAO/T-AIMD-00-321, September 21, 2000.

needed to be addressed in order to develop and implement the system but, rather, only short-term schedules for developing five key software components.

The C&P project has moved forward since last September. In November 2000, VBA completed implementation of a rating board automation tool and completed development and testing of the other four software products at the end of January 2001—about 1 month behind schedule. A small pilot test was conducted in mid-February to demonstrate VBA's ability to process and generate compensation and pension benefit payments and according to VBA, the test occurred without problems and successfully demonstrated that claims payments could be made using the new products. VBA has also taken steps to improve its planning and management of this effort. For example, VBA has created a project control board to provide day-to-day management and oversight for the project, and it has begun allocating staff to conduct work supporting key areas that had not been addressed previously, including data conversion, interfaces, batch processing, and synchronization. In addition, VBA has released a schedule that calls for deploying the compensation and pension replacement system in July 2002.

Nonetheless, VBA still needs to address several important issues before it can successfully implement the project. For example, although it has established a schedule for deploying the project, it has not developed an integrated project plan and schedule incorporating all of the critical areas of this system development effort, to be used as a means of determining what needs to be done and when, and of measuring progress. Instead, detailed plans and schedules exist only for portions of it, while other areas have yet to be fully addressed, including critical areas such as data conversion. As we reported in September, data conversion is considered by VBA to be the most difficult remaining part of the compensation and pension replacement project.

Furthermore, VBA's C&P pilot test only processed ten original claims that did not require significant claims development work. The current C&P payment system processes on the order of 3.2 million payments each month. Therefore, VBA must address scalability issues in order to move this software from the pilot stage to the deployment stage. The limited scope and nature of the pilot test puts VBA's millions of claims at risk should the C&P application not work as intended once it is put into an organizationwide operational setting.

In summary, Mr. Chairman, while VA has taken actions to improve many of its IT management processes, it continues to face substantive challenges which if left incomplete can disrupt existing progress and threaten the viability of its existing and future IT spending. VA has yet to fill its full-time department CIO vacancy since the position's creation 3 years ago. In addition, sustained leadership and commitment are necessary for improving VA's departmentwide computer security program, particularly effectively addressing and monitoring security risks as it takes steps to move some of its information and services to veterans onto the Internet. And while the department has done a good job of posting privacy and security notices on its Web sites, it should nevertheless increase its attention to compliance with OMB policies prohibiting the use of persistent Internet cookies. Further, until VA defines and begins to implement a departmentwide, enterprise architecture, it will continue to encounter costly difficulties in achieving its "One VA" vision. Finally, VA faces important decisions for making greater use of DSS and in ensuring that it is making an informed decision regarding continued development and wide-scale implementation of the compensation and pension replacement project. Continued attention and full implementation of past recommendations we and others have made are essential for achieving better IT management outcomes.

#### SCOPE AND METHODOLOGY

We performed this assignment in accordance with generally accepted government auditing standards, from December 2000 through April 2001. In carrying out this assignment we assessed the structure of and VA's efforts to fill its CIO position; improve the department's computer security; processes for selecting, controlling, and evaluating IT investments; complete a departmentwide integrated systems architecture; track its IT expenditures; utilize VHA's Decision Support System; and implement VBA's compensation and pension replacement project.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the Subcommittee may have at this time.

#### CONTACTS AND ACKNOWLEDGMENTS

For information about this testimony, please contact me at (202) 512-6257 or by e-mail at [mcclured@gao.gov](mailto:mcclured@gao.gov). Individuals making key contributions to this testimony include Mary Dorsey, Amanda C. Gill, Tonia L. Johnson, Dave Irvin, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, and Charles Vrabel.

(310406)

February 2001

# Maximizing the Success of Chief Information Officers

Learning From Leading  
Organizations



GAO-01-376G

---

**GAO**

Accounting and Information Management  
Division

---

May 1998

## Executive Guide

# Information Security Management

Learning From Leading  
Organizations

GAO

United States General Accounting Office  
Accounting and Information  
Management Division

November 1999

# Information Security Risk Assessment Practices of Leading Organizations:

A Supplement to GAO's May 1998  
Executive Guide on Information  
Security Management



GAO

Accountability • Integrity • Reliability

GAO/AIMD-00-33

**Statement and Supporting Documents**

**Hearing by Subcommittee of Oversight and Investigations,  
Department of Veteran Affairs**

**Karl Ware  
Co-Founder and Executive Vice President of Operations  
BioNetrix**

**April 4, 2001**

## Introduction

Today's rapid advancement and adoption rate of technology is accelerating the evolution of business processes into a completely digital environment. This means that internal and external users, external partners, suppliers and vendors, customers and consumers are given 24x7x365 access to sensitive, critical and often confidential information electronically, and in most cases given significant authority to conduct materially affecting transactions in a digital form. What was once a digital evolution within the confines of an enterprise or organization has transformed into ubiquitous access over multiple channels – the enterprise network, the Internet, mobile palm-based devices and wireless phones. These dynamic environments are forcing organizations to evaluate traditional approaches to internetworking and network security.

Organizations need to be able to verify the identity, authority and access privileges of individuals and entities to allow them to access confidential information or conduct transactions electronically. Additionally, as the ubiquitous environment becomes pervasive, organizations have to protect their resources from crimes such as malicious attacks, corruption of critical data and theft of sensitive information. It is no longer sufficient to solely trust the security of the core network; organizations must be able to trust both the network and the user at the edge of the network.

## Passwords – A Weak Link in the Secure Digital Environment

Applications and network resources today are protected by password systems that are just surrogates for a user; they do not provide conclusive authentication. In short, passwords don't prove that users really are who they say they are. As the digitally ubiquitous environment grows, reliance on passwords alone will further weaken security and trust models. As the channels of access increase, the environment presents a serious security threat and an expensive, cumbersome management problem. This scenario is becoming increasingly troublesome as evidenced by recent press reports (Table 1).

**Table 1.**

*"On January 29 and 30, 2001, Verisign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not" - ZDNET March 2001*

*"A restaurant worker allegedly masterminded the largest theft of identities in Internet history and is suspected of stealing millions of dollars from celebrities, billionaires and executives such as Steven Spielberg, Warren Buffet, and Ted Turner" - Reuters March 2001*

*"Michael Bloomberg's personal computer passwords were stolen and the inner walls of security at Bloomberg were penetrated." - London Times, August 20, 2000*

*"Fortune 1000 companies sustained losses of more than \$45 billion in 1999 from the theft of proprietary information" - American Society for Industrial Security (ASIS) and PricewaterhouseCoopers Survey*

The problems with passwords have been well documented. Some of the issues include:  
(Source: The Gartner Group)

- Users might share passwords with colleagues to shortcut access controls request procedures. This might not expose the system to an attacker, but it does destroy accountability.
- Users tend to choose passwords that are easily remembered and so easily guessed or vulnerable to a "dictionary attack," an attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.
- Users write down passwords where they can be found by an attacker, in the worst case, on notes stuck to workstations.
- An attacker might use social engineering, employing some kind of confidence trick to persuade the user to reveal the password or a help desk operator to reset the user's password.
- An attacker might simply observe a user keying in a password. This is known as shoulder surfing.

- An attacker can intercept passwords that are sent over networks in clear text. This is a high risk in open, unencrypted, public networks such as the Internet.
- If an attacker can place malicious software on the user's workstation or the organization's network, this can discover usernames and passwords and e-mail them to the attacker.
- Users forget passwords, leading to a potentially high administrative overhead (as high as 40 percent of help desk calls in some organizations) or costly self-service password reset solutions
- Finally, with most of these vulnerabilities, it is difficult to detect if or when a password has been compromised.

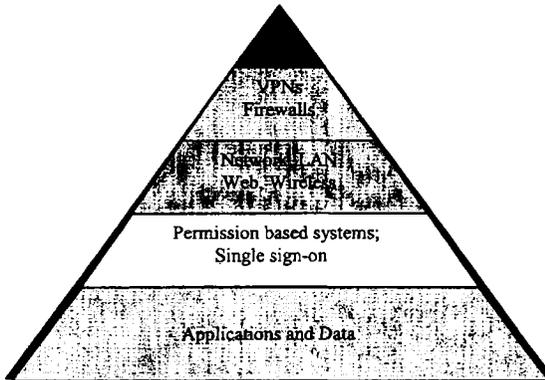
### Need for Strong Authentication at the Network's Edge

To gain an understanding of the need for a stronger and more conclusive user authentication management system at the network's edge requires an examination of the current solutions that address information and transaction security (Figure 1).

The core of an organization's computing infrastructure is applications and data. Over the last few years, the trend has been to move from centralized assets to a more distributed form where applications are distributed across servers, geographic locations and business units. Traditionally, the security for access and authorization has been built into each application separately. As the number of applications has grown and the channels of access have expanded, it has become increasingly complex and expensive to include security components on an application-by-application basis.

Protecting network applications from unauthorized access and, at the same time, supporting the growing number of applications, users, and channels of access has led to privilege or permission-based management systems. Such systems provide authorized users with the appropriate access to specific applications and network resources based on user profiles. Providing a way to manage user access privileges means that it is possible for authorized users to move between applications without logging on to each application. This function, known as single sign-on, has the potential benefit of remembering and using a single password to gain authorized access to multiple applications. The downside of using passwords for single sign-on is that a compromised password is a single, and critical, point of vulnerability.

Figure 1.

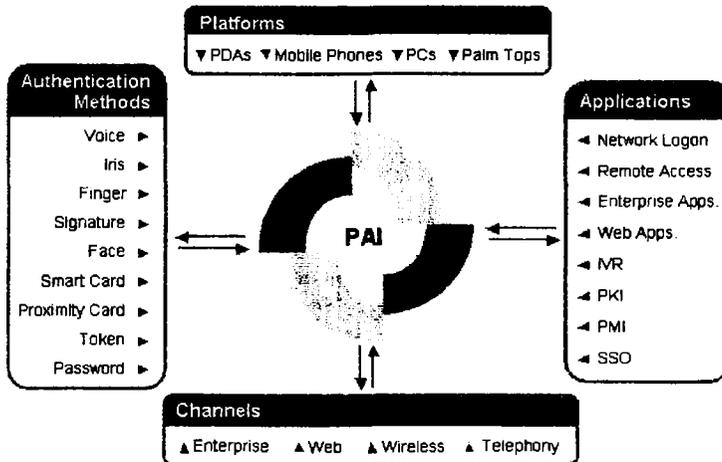


The need to provide cost efficient but secure network access to distributed applications over the intranet, extranet and the Internet has given rise to widespread deployment of firewalls and Virtual Private Networks (VPNs). Firewalls are used to secure sensitive portions of an organization's network and ensure that all communications across it conform to the organization's security policy. Firewalls are essential gateways, which are usually positioned between a LAN and the Internet. They intercept all communications before entering an organization's private network and decide whether to pass or reject these communications based on predefined rules. VPNs typically use the Internet as the transport backbone to establish secure links, via authentication, encryption and secure tunneling. A VPN is usually installed on the existing network infrastructure such as a firewall. VPNs provide the ability to secure and trust the network when remotely accessed by mobile users or when networks connect multiple locations.

As we review the security stack from the applications and privilege management systems all the way to the firewall and VPNs at the edge of the network, it is evident that these systems provide acceptable authentication at the machine-to-machine and application-to-application level. The problem is that in this "security chain," applications and network resources are compromised at the very edge of the network because password systems serve as surrogates for a user and do not provide personal, conclusive authentication. A system that provides privilege-based access to users assumes that the user is who he says he is. A robust personal authentication infrastructure (PAI) relies on strong authentication at the edge of the network to conclusively identify the user before the user is authorized for access to information and transactions. Furthermore, authentication cannot be considered in isolation. There is little point in requiring a user to authenticate to a firewall using a challenge-response token if all subsequent authentication events to services behind the firewall use memorized passwords transmitted without encryption. A PAI can ensure that an organization deploys strong authentication for all services within the security infrastructure.

### Personal Authentication Infrastructure

A Personal Authentication Infrastructure (PAI) enables organizations to deploy personal authentication at the network's edge – and know for certain who is accessing sensitive information, applications and transactions. A PAI deploys and manages multiple advanced authentication methods – biometric (fingerprint, voice, face, iris and signature recognition) and non-biometric (token and smart card) – to protect access to any application or resource. A PAI extends the organization's existing security infrastructure and supports the adoption and migration to advanced authentication methods. It should be flexible enough to enable dynamic, multi-factor authentication, allowing organizations to dial up the appropriate level of security without sacrificing convenience.



## Benefits of Deploying a Personal Authentication Infrastructure (PAI)

When it comes to deploying security measures even within one organization, it is likely that one authentication method or combination of methods will suit some users, and another will suit other users, depending, for example, on what information or services they are authorized to use. Furthermore, different authentication methods might be appropriate to the same user at different times – or, rather, in different locations, such as in the office or dialing in from home.

### 1. Flexibility to Choose Authentication Methods

A PAI provides the flexibility of selecting from various means of user verification. Authentication by its very definition verifies an identity claimed by or for a user or other system entity by demanding proofs and credentials. The means of identification supported may be classified as:

*Identification based on something the user is*



Iris/Retina



Fingerprint



Face



Hand

*Identification based on something user does*



Signature



Voice



Keystroke

*Identification based on something user has*



USB



Sync



Smart Card

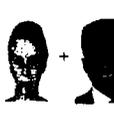
*Identification based on something a user knows*

USER ID/ PASSWORD/PIN

### 2. Ability to Implement Strong Authentication Policies

Through a policy-based infrastructure, a PAI allows an organization to deploy varying methods and levels of security throughout its computing environment. Policies are defined and managed based on individuals, groups, applications, channels or entry points. When necessary, they enable multi-factor authentication, requiring any desired number and combination of biometric and non-biometric verification methods.

**Table 2.**  
Examples of Multi-Layered Authentication Policies

<p><b>Policy Assigned</b></p>				
<p><b>Application or Environment</b></p>	<p>Standard Remote Access</p>	<p>Standard Desktop Access</p>	<p>Access to mission critical information</p>	<p>High value transactions (Wire Transfers)</p>

### 3. Fraud Prevention and Ability to Enforce Policies

A PAI provides real-time logging of authentication activity and detailed auditing reports to prevent fraud and to monitor and enforce policy. Detailed reports can allow administrators to know who, what, when and where – who is attempting to gain access to what applications; when the attempts occur; and from what platform the attempts are made. In addition, they specify whether the attempt is successful and what authentication policy is governing user access. Costs saved through fraud prevention and non-repudiation of fraudulent transactions alone can return the investment on a PAI deployment in less than one year.

### 4. Increased Security with Increased Convenience

Implementing security measures has always come at the cost of convenience. A PAI enables organizations to choose from various authentication methods to implement the technology that is best for the user population. The ability to apply flexible policies to meet specific needs rather than implementing a "one-size-fits-all" solution accelerates the user adoption and compliance of security measures deployed.

### Summary

As organizations move to a completely digital environment, users are given 24x7x365 access to sensitive, critical and often confidential information electronically and in most cases given significant authority to conduct materially affecting transactions in a digital form. What was once a digital evolution within the confines of an enterprise or organization has transformed into ubiquitous access over multiple channels – the enterprise network, the Internet, mobile palm-based devices and wireless phones.

Organizations need to be able to conclusively verify the identity of individuals and entities before providing the authority and access privileges to allow them to access confidential information or conduct transactions electronically. It is no longer sufficient to solely trust the security of the core network; organizations must be able to trust both the network and the user at the edge of the network.

Organizations should consider deploying a personal authentication infrastructure (PAI) that integrates with and manages all components of existing security systems that may include any combination of user authentication – biometric or non-biometric. It mitigates interoperability problems between multiple applications, authentication methods, channels and platforms, driving cost savings, convenience and security.

## Appendix 1.

**\*\*Note:** BioNetrix and Karl Ware have not received any Federal grant or contract relevant to the subject of this testimony.

### **Biography of Karl Ware, Co-Founder, Executive Vice President of Operations, BioNetrix**

Karl Ware co-founded BioNetrix in 1997 and launched the company's flagship product, the BioNetrix Authentication Suite. As executive vice president of operations, Ware now oversees the company's day-to-day operations. Before founding BioNetrix, Ware worked in various capacities at Dow Jones Teletate and Motorola, creating and executing successful marketing initiatives. He launched more than 18 different products for the two companies into both domestic and international markets.

Ware started his career in Washington, D.C., where he obtained an expertise in information security working for the Central Intelligence Agency (CIA). He later served as vice president of information/communications security for JP Morgan, where he defined technical and user security policies for the organization. Ware has worked extensively in England, Hong Kong, Singapore and Indonesia.

### **BioNetrix Company Overview**

BioNetrix delivers information security at the network's edge – the intersection where people access information – through an authentication software platform that allows organizations to control who accesses their critical applications, transactions and data.

The BioNetrix platform deploys and manages a host of personal authentication technologies, including biometrics (fingerprint, face, iris, voice and signature recognition), smart cards and tokens. Through the deployment of these advanced authentication technologies, BioNetrix provides conclusive identity verification of employees, customers and partners, strengthening security for enterprise computing and Internet transactions. With BioNetrix, organizations can authenticate people, not just machines, and as a result, deliver trusted, higher-value electronic business.

Recent industry accolades for the BioNetrix product include Network Computing's "Well-Connected" and "Editor's Choice" awards, and Network World's "World-Class" and "Best of the Tests" awards.

Now led by CEO John Ticer, BioNetrix was founded in 1997 by Peter Bianco, Vice Chairman, and Karl Ware, executive vice president of operations. BioNetrix is headquartered in Vienna, Va., in the heart of the area's high-tech corridor. The company's management team and board of directors have successfully built companies that dominated their markets. The BioNetrix team is made up of proven, driven individuals who have done it before.

### **The BioNetrix PAI**

BioNetrix extends information security to the network's edge – the intersection where people access information – through a centrally managed authentication platform that allows organizations to control who accesses their critical applications, transactions and data. The BioNetrix platform deploys and manages a host of personal authentication technologies, including biometrics (fingerprint, face, iris, voice and signature recognition), smart cards and tokens. Through the deployment of these advanced authentication technologies, BioNetrix provides conclusive identity verification of employees, customers and partners, strengthening security for enterprise computing and Internet transactions. With BioNetrix, organizations can authenticate people, not just machines, and as a result, deliver trusted, higher-value electronic business.

The BioNetrix Authentication Suite is the industry's first multi-channel PAI, providing a single identity verification management system for both enterprise and Web-based applications. With one universal management platform, an organization can manage authentication throughout its entire computing environment, streamlining administration functions and reducing complexity.

The Authentication Suite integrates with and manages all components of existing security systems that may include any combination of user authentication, biometric or non-biometric. It mitigates interoperability problems between multiple applications, authentication methods, channels and platforms, driving cost savings, convenience and security.

The BioNetrix solution includes the most extensive authentication method and application libraries in the industry. The product's open architecture ensures that methods and applications not supported in the core product are easily integrated using BioNetrix's suite of toolkits.

## The Weak Link

Passwords weaken the trust model in the electronic transaction world. Users expect e-commerce to be available 24/7/365... and secure.

*"Fortune 1000 companies sustained losses of more than \$45 billion in 1999 from the theft of proprietary information..."*  
*American Society for Industrial Security (ASIS) and PricewaterhouseCoopers Survey*

---

*"On January 29 and 30, 2001, Verisign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not"*  
*ZDNET March 2001*

---

*"Michael Bloomberg's personal computer passwords were stolen and the inner walls of security at Bloomberg were penetrated."*  
*London Times, August 20, 2000*

---

A restaurant worker allegedly masterminded the largest theft of identities in Internet history and is suspected of stealing millions of dollars from celebrities, billionaires and executives such as Steven Spielberg, Warren Buffet, and Ted Turner.  
*New York Post - Reuters - NEW YORK March 20, 2001*

**BIONETRIX**

## The Password Test

- Your Name
- Birthday
- Related Name
- Address
- Social Security #
- Phone Number
- Possession/Car
- Important Date
- Sports Team
- Pet's Name
- Favorite Pass-time
- Location Name
- Musical Reference
- Cinema Reference
- License Number
- Employee ID Number

This Test has a minimum 92% hit rate...  
**YOU HAVE JUST BEEN HACKED**

**BIONETRIX**

## Protecting Cyberspace

**Personal Authentication Infrastructure**

**Privacy/Integrity**

**Channel**

**Authorization**

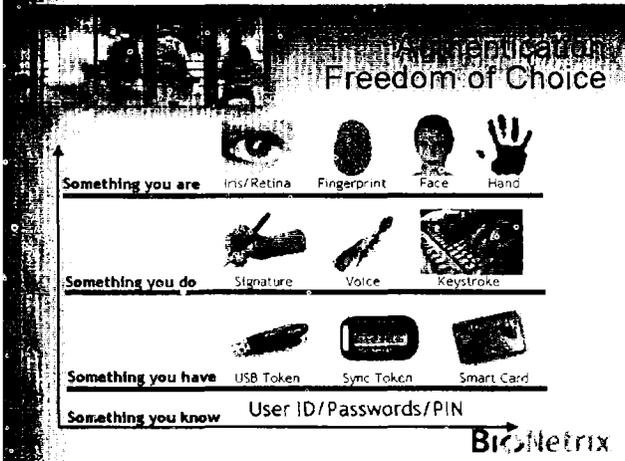
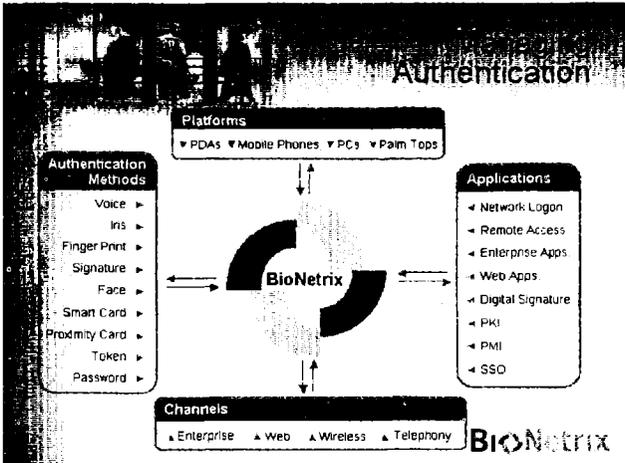
**Encryption, Firewall, VPN, E-Sign**

**Network, LAN, Web, Wireless, Telephone**

**Permission Management Systems, Single Sign-On**

**Digital Destinations - The Applications**

**BIONETRIX**



### Authentication Policies

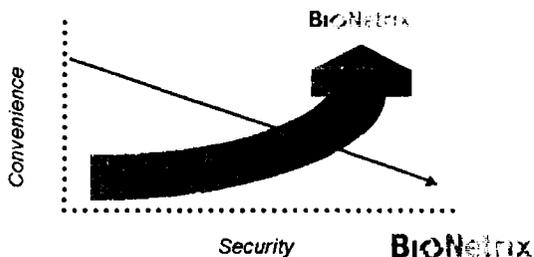
Policies enable assignment of authentication technologies based on the value of assets or operational environment.

<b>Policy Assigned</b>			
Application or Environment	Remote Access 	Standard Desktop Access 	Gov't Benefits/ Wire Transfer 

BioNetrix

Secure?

With BioNetrix convenience and security work together



Summary

- Benefits gained through the use of the **BioNetrix Authentication Suite™**
  - Fraud Reduction/Deterrent
  - Cost Reduction for maintenance of passwords/authentication
  - Augment the use of passwords
  - More security over any channel: web, voice, intranet, dial-in, wireless
  - Convenience/Flexibility is increased for users
  - Automated Policy Enforcement
  - Stronger Trust enables higher value transactions
  - Ability to use any authentication method(s) for access to any application

BioNetrix

BioNetrix

Providing Conclusive Authentication  
For Any Digital Environment

[www.bionetrix.com](http://www.bionetrix.com)

Pat. Ware

Pat. Ware, EVP

[pat@bionetrix.com](mailto:pat@bionetrix.com)

[www.bionetrix.com](http://www.bionetrix.com)

1-800-756-1173 x 9200

BioNetrix

# **TIGER TESTING**

**The Independent Computer Security Testing Specialists**

**What is Ethical Hacking,**  
**What are the Benefits,**  
**and**  
**How Should Ethical Hacking Be Done**

Testimony by  
Ken Brandt, Managing Director of Tiger Testing  
30 Wall Street, New York, NY 10005

Before the  
Subcommittee on Oversight and Investigation  
Committee of Veterans Affairs  
United States House of Representatives

April 4, 2001

I would like to thank the Subcommittee for the opportunity to testify today. The United States leads the Information and Internet Age, and as a result, must lead in resolving the associated Internet, system security, and privacy issues. This is a challenge for both the private and public sectors. The Subcommittee's highlighting of these issues today is a great example of Congressional leadership.

As leaders in the field of ethical hacking, we at Tiger Testing are honored and excited about providing the Subcommittee with this overview and explanation of ethical hacking.

**What is Ethical Hacking**

Ethical hackers test Internet security. They answer the question: how safe is your web site from computer hackers? Ethical hackers test everything related to the safety and security of a web site, including related services (FTP, Mail, HTTP, etc.), the associated IP addresses, and the underlying systems.

Ethical hacking is also known as vulnerability assessment, web site security testing, network security assessment, red teaming, and several other names. Ethical hacking allows system owners and operators to learn about security gaps and potential breaches of privacy, so that they can be corrected, rather than leave them open for potential abuse.

Ethical hacking is a key component of congressionally mandated risk assessment. Congress requires government agencies, financial firms, and health care organizations to develop and implement security policies to safeguard information and privacy, and then test to be sure that information and privacy are actually being safeguarded. By testing

- Page 1 of 6 -

**30 Wall Street, New York, New York 10005**  
**www.TigerTesting.com**  
**Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com**

# TIGER TESTING

The Independent Computer Security Testing Specialists

web site security, ethical hackers also answer the questions: Is information really secure and is privacy really protected?

The “ethical” part of ethical hacking means three important things: integrity, transparency, and independence.

- First and foremost “ethical” means integrity. Ethical hackers are not ex-hackers with criminal records or a past that includes breaking into systems or defacing web sites. Ethical hackers can pass very thorough background checks and have backgrounds in systems engineering, systems audit, and systems security.
- Second, “ethical” means a transparent non-invasive process. Ethical hackers don’t do anything to change, slow down, or damage their clients’ systems. An ethical hacker does not write to or modify clients’ computer code and never reduces their clients’ network response time. System security and privacy gaps (including Denial of Service vulnerabilities) can, and should, be identified without causing any damage.
- Third and equally important is independence. Ethical hackers don’t have any conflicts of interest. Ethical hacking is performed by firms that are not in the business of selling auditing, consulting, hardware, software, firewall, hosting, and/or networking products and services. An ethical hacking firm avoids the conflict of interest of testing system security measures that they recommend, install, or sell.

## The Benefits of Ethical Hacking

The benefits of ethical hacking are just as straightforward. A “virtuous cycle” of ethical hacking, fixing of system security holes, more ethical hacking, more fixing of system security holes, etc. results in greater information security and stronger privacy protection.

The ethical hacking / fixing the security holes cycle must be an ongoing cycle in order for it to work. Security gaps can open up as a result of system changes and/or advances in hacker technology. Testing and fixing on an ongoing basis is the only way to identify and fix security gaps that may be opening up. Hackers don’t try to access confidential and private information just once in a while, so testing and fixing shouldn’t take place just once in a while.

## How Ethical Hacking Should Be Done

The ethical hacking approach and deliverables outlined below were developed by Tiger Testing and used as the basis of industry standard best practices being published shortly for both the Internet legal field and the system security field.

- Page 2 of 6 -

30 Wall Street, New York, New York 10005

[www.TigerTesting.com](http://www.TigerTesting.com)

Phone (212) 898-9322 Fax (212) 361-2209 E-Mail [kbrandt@tigertesting.com](mailto:kbrandt@tigertesting.com)

# **TIGER TESTING**

**The Independent Computer Security Testing Specialists**

## **APPROACH**

Ethical hacking should utilize an eight step approach to both maximize the quality of the testing and minimize the need for client resources.

### **1. Test Remotely**

Testers do not have to come onsite at a client in order to test the client's web site security. Remote testing should not require any client: advance preparation, staff time, system changes, system time, or facilities space. The risk being tested is external, so the testing should be performed externally. A secondary advantage of remote testing is that the client does not need to incur any of the security risks associated with having outside consultants onsite.

### **2. Test Transparently**

Security vulnerabilities (i.e. the ability to cause a Denial of Service, gain root access to key systems, alter web pages, etc.) can, and should, be identified without doing any damage. Testing should not involve writing to or modifying client systems, and should not reduce client systems' response time.

### **3. Test Each Month, Not Once or Twice A Year**

Security gaps can open up as a result of system changes and/or advances in hacker technology. Testing on an on-going basis is the only way to know if new security gaps are opening up. Hackers don't try to penetrate systems just once, so testing shouldn't take place just once.

### **4. Test at Varying and Random Times Throughout Each Month**

Some security vulnerabilities are more likely to show up when network traffic is heavy (i.e. fragmented packet security gaps) and some are more likely to show up when network traffic is light (i.e. predictable TCP or IP sequences). Tests should be conducted at all different times: weekdays/weekends, days/nights, and holidays/non-holidays.

### **5. Use The Right Testing Tools and Use Them Correctly**

Both open source and proprietary software tools should be used. There are over 20 excellent open source testing tools, each of which has different strengths, so each should be utilized. Each of these tools should be continuously modified and retested prior to it's use. This optimization should be done at the operating system, configuration, and (if applicable) application level.

### **6. Use Testers With Integrity**

Giving an ex-hacker a paycheck or a consulting fee doesn't change his or her ethics. Penetration testing should be performed by systems engineers and security professionals,

- Page 3 of 6 -

**30 Wall Street, New York, New York 10005**

**[www.TigerTesting.com](http://www.TigerTesting.com)**

**Phone (212) 898-9322 Fax (212) 361-2209 E-Mail [kbrandt@tigertesting.com](mailto:kbrandt@tigertesting.com)**

# TIGER TESTING

The Independent Computer Security Testing Specialists

rather than ex-hackers. Organizations should not increase system risk by inviting ex-hackers to perform ethical hacking.

## 7. Use Independent Testers

When a firm tests the results of their own advice, products, or services, they always look good. Ethical hacking should be performed by a firm that is not in the business of selling: auditing, consulting, hardware, software, firewall, hosting, and/or networking products and services. Ethical hackers must be independent to avoid this conflicts of interest.

## 8. Use External Testers

Internal employees (people who work for the organization who's web site is being tested) may be reluctant to point out security flaws that they, their associates, their boss, and/or their system security strategy, may be responsible for. External penetration testers will be rewarded by their firm for finding security gaps, internal penetration testers are seldom so lucky. For full reporting, ethical hacking should be performed by an outside firm.

## DELIVERABLES

The client should provide the testing firm with the URL (web site name) or range of IP addresses to be tested. No additional information (network topology, architecture, configuration, vendors, versions, etc.) should be required. For each URL or range of IP addresses to be tested, the testing firm should provide the client with the following monthly deliverables:

### 1. Testing

Full high quality testing over the course of each month, as described in the Approach section.

### 2. Reporting

A concise monthly report suitable for both senior management and hands-on technologists. The report should contain:

- A. An executive summary explaining how the testing was performed, what was tested, how many tests were conducted, and the number of security gaps that were identified.
- B. An assessment of the client's risks. A risk rating should be provided for each of the major types of potential Internet vulnerabilities.
- C. An explanation of each of the client's system security vulnerabilities. Each explanation should include both the business risk as well as the technical details. The technical details should be very specific as to which machines, ports, and services, have which security gaps, and how each could be exploited. However,

- Page 4 of 6 -

30 Wall Street, New York, New York 10005

[www.TigerTesting.com](http://www.TigerTesting.com)

Phone (212) 898-9322 Fax (212) 361-2209 E-Mail [kbrandt@tigertesting.com](mailto:kbrandt@tigertesting.com)

# **TIGER TESTING**

**The Independent Computer Security Testing Specialists**

in order to maintain testing objectivity (see Independence portion of the Approach) the explanations should not include recommendations or consulting advice.

- D. A list of the client's hosts that are visible to hackers. This list should include all the machines that are visible, not just those that contain security gaps.
- E. An appendix defining the Internet vulnerabilities tested. This will provide a frame-work for reviewing the risk assessment and the explanation of each security gap.

### **3. REVIEW OF FINDINGS**

The client may wish to review some of the monthly reports with the testing firm. At the client's option, the testing firm should be ready to discuss any of the reports over the telephone.

#### Conclusion

I hope this overview has been helpful, appreciate Congress's interest and leadership in this area, and am prepared to answer any questions the Subcommittee may have.

- Page 5 of 6 -

**30 Wall Street, New York, New York 10005**

**www.TigerTesting.com**

**Phone (212) 898-9322 Fax (212) 361-2209 E-Mail kbrandt@tigertesting.com**

# **TIGER TESTING**

**The Independent Computer Security Testing Specialists**

**Ken Brandt**  
**Managing Director of Tiger Testing**

Ken Brandt is Tiger Testing's Chief Executive Officer and one of its two co-founders. Tiger Testing is the premier ethical hacking firm and has offices in New York, NY and Austin, TX. Tiger Testing tests the Internet security of financial, media, and technology giants in Asia, Europe, and the United States.

In addition to his internal responsibilities, Mr. Brandt represents Tiger Testing at two national Internet security organizations: the Partnership for Infrastructure Security and the Center for Internet Security. Tiger Testing has actively participated in the Partnership since it was formed by the President and the U.S. Chamber of Commerce. Mr. Brandt is a founding member of the Center for Internet Security.

Prior to co-founding Tiger Testing, Mr. Brandt was a technology executive with experience managing large system and security projects at major multinational and regional broker/dealers, trading system vendors, banks, investment companies, and market data providers.

- Page 6 of 6 -

**30 Wall Street, New York, New York 10005**  
**[www.TigerTesting.com](http://www.TigerTesting.com)**

**Phone (212) 898-9322 Fax (212) 361-2209 E-Mail [kbrandt@tigertesting.com](mailto:kbrandt@tigertesting.com)**

Testimony before the Committee on Veterans' Affairs  
Subcommittee on Oversight & Investigations  
United States House of Representatives

Submitted by

Scott C. Sherman  
Director of Advanced Technology Architectures  
EMC Corporation  
April 4, 2001

Chairman Buyer, Congressman Snyder, and distinguished members of the subcommittee, I am Scott Sherman, Director of Advanced Technology Architectures at EMC Federal Systems. It is an honor and a distinct pleasure to be here this morning.

EMC is the world leader in enterprise information storage systems, software, networks and services, and the leading provider of secure information storage infrastructure in the world. It is these information infrastructures that determine an organization's ability to deliver new services, and their ability to adapt to the explosive growth in information and revolutionary technologies. With revenues of \$9B in 2000, EMC stores two-thirds of the world's critical information, and has developed storage infrastructure solutions for the majority of the world's largest banks and financial institutions, airlines, telecommunication companies, transportation companies, Internet Service Providers, educational institutions, and regional and national government agencies.

EMC has revolutionized enterprise Information Technology (IT) strategies, and developed unprecedented interoperability with all information systems, sub-systems and emerging technologies, to deliver complete enterprise information frameworks that dynamically adapt to multiple, mission critical requirements. Based in Hopkinton, Massachusetts, EMC was founded in 1979, currently has over 16,000 employee's nation-wide (23,500 worldwide), and offices in 43 states.

We are in the midst of explosive information growth. A recent University of California-Berkley study indicated that we will create as much information digitally over the next two years as we have created in the entire existence of man-kind. Combine this with the revolution in technology and services, exponential capabilities in information storage, exploding bandwidth, wireless computing, and we have revolutionary new ways to leverage information in order to deliver services never before thought possible.

In the commercial sector, high performance organizations have shifted their IT architectures in response to these trends, and employed standardized, enterprise-wide IT infrastructure. These organizations have created consolidated corporate information databases which dramatically ease the sharing of data between different business functions, standardize and simplify data management processes, guarantee the protection of data against loss or corruption, and improve management decision-making. This same technology can be utilized by the VA to obtain an efficient and unified view of each veteran, to include all of the pertinent information regarding the healthcare and benefits that are provided to him or her by the VA: ONE VA.

One of the driving forces behind enterprise infrastructure is the recognition by the world's global 2000 companies that to stay competitive they must insure that all corporate activities are focused on ultimately

providing high customer satisfaction. This “customer-centric” business architecture must be matched by an IT architecture that puts information of the customer, and the business, at its center. This “information centric” approach makes possible efficient information sharing, data management and high-speed communication among diverse business systems. The promise of IT to deliver massive operational efficiencies is finally being realized in high performance organizations through an enterprise, information centric approach that enables a single, unified view of the customer, or business issue.

The ability to capture and integrate all customer data from anywhere in the organization, to analyze and consolidate it into standardized form, and then to distribute the results to various systems and customer contact points across the enterprise is the challenge that the VA faces. This challenge is made more difficult due to the advances made early on with the Decentralized Hospital Computer Program (DCHP), and later the Veterans’ Health Information Systems and Technology Architecture (VISTA). Although wonderful examples of integration and standardization, the ability to rapidly adapt these systems to changing health care technology and requirements is difficult.

Commercial organizations have demonstrated that this challenge is best met by implementing an enterprise architecture that integrates all of a company’s systems and places information at the center. Such architecture is based upon enterprise storage, which provides consolidated scalable support to multiple operating systems (mainframe computers, Unix systems, and Windows NT), on a single storage platform. Enterprise storage infrastructure can be centralized in the data center, or it can be distributed across the enterprise via an enterprise network; however, enterprise information storage is the technical foundation for an information-centric infrastructure.

This architecture eases information sharing across different business functions and fast communication across all enterprise systems. It provides better information protection by isolating the complexities of data management. It provides high availability as a result of online backup and disaster recovery. It provides cost-effective data management from centralized, cross-platform management tools. Finally, it provides a more flexible business environment that helps companies provide better customer service because they now have a complete, manageable view of all their information.

This architecture consolidates information from many systems within a centrally managed storage platform, reducing the need to extract and replicate data among many systems. The enterprise storage approach also creates tremendous efficiencies through the ability to “mirror” (a mirror is a real-time copy) all of the enterprise information. This “mirrored” copy can be created in the background to serve as an independently addressable physical copy, created for analysis, decision support, application development, or to run simultaneous tasks in parallel.

Enterprise storage’s powerful information protection capabilities also help avoid the costly impact of outages. By replicating information at the physical storage level, you isolate the complexities of data maintenance, online backup and disaster recovery. The “mirrored” data serves for instant back up and recovery in the event of a planned, or unplanned, outage.

The VA’s operational database for benefit information, for example, could be maintained in Kokomo, Indiana, and “mirrored” to a remote disaster recovery site in Little Rock, Arkansas. In the event of an interruption at the primary site, full operation can resume at the secondary site virtually instantaneously, as opposed to the days or weeks that are typically required from “tape-based” recovery solutions. Because enterprise storage consolidates heterogeneous systems at the storage system level, decoupled from platform-specific anchors, disaster management is centralized, and disaster restart can be accomplished for all platforms at once. This is far simpler than with server-centric storage, where backup and restore is at the application, database or server level. This is the Information Technology that has

enabled our nation to enjoy the extraordinary e-commerce revolution, by guaranteeing "24 x forever" availability of service.

Enterprise storage allows centralized information management across the organization through a common set of procedures. This is more cost-effective than IT staffs having to learn separate procedures for every database, operating system, or server. When new applications or platforms are added to an enterprise storage environment, existing staff are already trained and competent to manage the information. Administrators, then, are far more productive in managing enterprise storage. Such flexibility helps companies keep pace with rapid business changes, preparing them for virtually any challenge.

Finally, enterprise storage allows data movement from all systems into a central repository—the data warehouse, creating a single, uniform view of the customer that can be shared throughout the extended organization.

The Department of Veterans Affairs is currently utilizing some of the technology discussed today. The Austin Automation Center (AAC) has been using EMC hardware for several years. In the last few months, they have begun acquiring and utilizing the software tools that will allow the creation of an enterprise storage environment at the AAC. But the AAC is just one part of the VA's information technology infrastructure. In order to create a true enterprise storage infrastructure across the entire Department, the VA will have to create and implement matching enterprise storage standards throughout the rest of the Department (i.e. VHA, VBA, NCA). By doing so, the VA will be able to harness the information necessary to create a total continuum of care for the veteran. This means from the time each veteran begins realizing their VA benefits, information would be available whenever and wherever the information is required in order to efficiently provide service to the veteran.

Finally, the obstacles to achieving this enterprise, information centric, vision, are often times just as challenging culturally as they are technologically. The decision, authority and ability to develop an enterprise approach resides at the "CEO" level, and is typically met with significant opposition by departmental leadership who perceive the release of "their" information and supporting systems as encroachment into their domain. Commercially, it is EMC's experience that few, if any, high performance organizations achieve an enterprise approach without a dictator-like commitment, which departmental leaders must accept regardless of the organizational and cultural changes that result. This cultural hurdle is often times more limiting than available technology, and just as frequently holds organizations back from realizing the massive operational efficiencies that have for so long been the promise of IT. Secretary Principi's statements during his confirmation hearings earlier this year paint a very optimistic picture in this regard, and I am sure veterans across our nation are excited about the vision, experience and leadership that he brings to the VA.

EMC Statement of Financial Disclosure for Fiscal Year 2001  
 Before the Subcommittee on Oversight and Investigation, Committee on Veteran's Affairs  
 April 4, 2001

For Fiscal Year 2001, EMC Corporation has received, either through contract or subcontract with the federal government, the following amounts listed by agency:

Air Mobility Command	\$216,783
Army National Guard, Headquarters	\$913,039
Ballistic Missile Defense Organization	\$246,397
Bureau of Alcohol, Tobacco and Fire Arms	\$1,568,702
Central Intelligence Agency	\$9,170,280
DCMA	\$175,865
DCMC District Head Quarters	\$47,168
DECA	\$190,164
Defense Commissary Agency	\$2,965,00
Defense Logistics Agency	\$3,374,113
Department of Agriculture	\$649,708
Department of Commerce	\$62,370
Department of Energy	\$493,783
Department of Interior	\$1,143,790
Department of Justice/Office of Justice Programs	\$627,092
Department of Veterans' Affairs	\$4,145,373
Defense Finance and Accounting Service	\$1,019,300
Defense Intelligence Agency	\$1,664,502
Defense Information Systems Agency	\$2,626,073
Drug Enforcement Agency	\$5,040,655
Executive Office of the President	\$481,165
Federal Aviation Administration	\$2,298,062
Federal Bureau of Investigations	\$97,647
Federal Reserve	\$291,610
Health Care Finance Administration	\$73,000
Housing and Urban Development	\$2,219,696
IFMC/Balt/CSC	\$1,806,715
Internal Revenue Service	\$11,645,163
Library of Congress	\$283,897
LIWA	\$1,579,353
McChord Air Force Base	\$54,432
MSRC Aberdeen	\$740,586
NASA	\$3,240,706
National Institute of Health	\$41,000
National Security Agency	\$171,239
Naval War College	\$120,101
NOAA/National Weather Service	\$147,700
Office of Secretary of Defense/ITD	\$3,785,264
Pacific Air Force	\$42,663,102
Security and Exchange Commission	\$517,470
Smithsonian	\$140,669
Social Security Administration	\$1,567,953
Special Operations Command	\$350,953
SPAWAR	\$2,489,918
Tennessee Valley Authority	\$1,396,143
United States Postal Service	\$3,783,080
United States Army	\$63,000
United States Army Forces Command	\$223,320
United States Army, PERSCOM	\$799,130
United States Coast Guard	\$118,000
United States Navy, Pensacola	\$266,561
United States Central Command	\$13,000
US Geological Service	\$642,688
US Patent and Trademark Office	\$7,742,449
USFPO	\$13,940
United States Marine Corps, Personnel Management Support Branch	\$1,033,430

Statement of  
Anthony J. Principi  
Secretary  
Department of Veterans Affairs  
Before the  
Subcommittee on Oversight and Investigations  
Committee on Veterans' Affairs  
U.S. House of Representatives  
April 4, 2001

Thank you Mr. Chairman, Mr. Snyder, and members of the subcommittee for this opportunity to come here today to address the issues you have raised concerning VA's Information Technology (IT) program and specifically VA's integrated systems architecture, VETSNET, our information security posture, and the Veterans Health Administration's (VHA) Decision Support System. I would also like to take this opportunity to give you my personal commitment that we will reform the way we use information technology at VA.

I first want to restate my pledge that we will not spend any new funds on IT until we have defined an Enterprise Architecture that ends "stove-pipe" systems design, incompatible systems development, and the collection of data that do not yield useful information. I have instructed my staff to convene a panel of world experts in the area of systems architecture to team with key business unit decision makers in each of our Administrations and staff offices to develop a comprehensive Integrated Enterprise Architecture Plan. I am well aware of your concern about this serious problem. I have assigned it the highest priority, and I expect to be able to deliver this plan to you in a matter of months.

The other issue that has my immediate attention is our IT security posture. I want you to know that I take very seriously the privacy and security of the information that we use and collect. As we become more and more sophisticated

in the use of information technology, we must never lose sight of what is really at stake. Our veterans entrust us with the most private, the most sensitive information imaginable. Good medicine is dependent upon good communication. Our veterans must be assured that we will honor that trust by ensuring that no unauthorized person has access to this information. Similarly we must be able to ensure that financial transactions are scrupulously protected and that the networks and systems that we have come to depend on are secure and available.

I am pleased to be able to report that we have made significant strides recently in improving our overall IT security posture. But as the reports of the U. S. General Accounting Office and our own Inspector General demonstrate, in truth, we still have much to do. I have made it clear to my staff that I will hold all senior managers accountable for ensuring strict compliance with our security directives. I am pleased to report that we have created a Senior Executive Service level "Cyber-Security" Director position. We have selected a highly qualified candidate from a rich talent pool to fill the position. He will be an important member of my IT management team. We have also made a series of critical decisions to enforce our policies that will result in a more secure, a more private environment. We cannot afford to lose the trust of veterans concerning the privacy of their medical information or the Congress concerning our stewardship of the resources that have been provided. We appreciate that trust and we will not lose it.

In regard to the two specific programs, VETSNET and VHA's Decision Support System, as you are very aware, each of these programs has had a troubled history. Let me tell you what I currently know, and more importantly, how I intend to proceed with each program.

VETSNET has been under development for far too long. Its development was delayed as new technologies and technical approaches came and went. Over

time it has suffered from a lack of focus, the absence of clear goals, and at some points inadequate management. These problems are behind us. The current VETSNET management plan addresses these problems. What began as a modernization program to automate all of VBA's business lines has evolved into a replacement system for the Compensation and Pension (C&P) claims processing system that was developed in the 1960's and 70's. However, I am still concerned about critical issues of performance and effective systems integration. Therefore, I have directed that before we proceed to a fully operational status on VETSNET, we will conduct an independent audit of the overall system. This audit will provide us with the assurance that this system will meet all of the security, functional, and performance requirements we have set for it. If it passes these tests, we will go forward with its implementation on the current schedule. If not, we will develop a plan to extend the life of the current systems and immediately begin the development of a replacement system.

Let me make a few things clear. We will not throw good money after bad. If this current version of VETSNET doesn't meet our needs for the next several years, we will terminate its development. Conversely, if it does meet our needs, we will not hold past failures against it, and we will go into production with the system. I have been assured that VETSNET is being developed in an open architecture to facilitate eventual integration into a future system and that it should fit within the framework of the Enterprise Architecture I have previously discussed. That system will be part of an integrated, whole solution to the needs of our veterans.

As for VHA's Decision Support System (DSS), we have made a significant investment in both time and resources in the implementation of DSS. Since its implementation at the end of FY 1998, VHA has made significant strides to improve the data quality and access. A number of significant changes and applications of DSS are underway in VHA.

VHA has extended access to DSS data from beyond the production system by developing National DSS extracts. These enable users at both the Veterans

Integrated Service Network (VISN) and VA Medical Center (VAMC) levels to develop customized reports needed to manage costs and understand workload. DSS data are now being used for the development of FY 2002 VERA allocations. The DSS use for VERA allocations is a clear indication that VHA is committed to using DSS to support some of the most critical decisions that VHA makes. Also, the Practice Management Advisory Board is using DSS data in their work in practice profiling. VISN Directors now have two DSS performance measures and a total of 14 DSS-based performance measures are being used to ensure that facilities move towards data based decision making. Most importantly, to further integrate DSS use in financial management and day-to-day operations, the DSS program was transferred to the VHA Office of Finance on March 11, 2001.

To address concerns about the quality of DSS data, standardization audits have been developed and will be deployed to ensure that a standard structure is used at all levels. Additional efforts are underway to improve access and use of DSS data. While many of the implementation issues that once faced VHA have been addressed and resolved, I believe our focus must be on the future and on better use of DSS in our day-to-day business and management decision processes. DSS still faces challenges to full implementation and significant efforts will be necessary to ensure an appropriate return on our investment.

Thank you for this opportunity to discuss these very serious IT issues. I will be happy to answer any questions I can.

## WRITTEN COMMITTEE QUESTIONS AND THEIR RESPONSES

**Post-Hearing Questions  
Concerning the April 4, 2001, IT Hearing****For  
The Department of Veterans Affairs****From  
The Honorable Steve Buyer  
Chairman, Subcommittee on Oversight and Investigations  
Committee on Veterans Affairs  
U.S. House of Representatives**

*1. Please describe technological, organizational, and cultural challenges the VA faces in implementing an Enterprise IT Architecture.*

The technological challenges that VA faces in implementing an Enterprise Architecture are integrating VA's legacy, stovepipe systems that have been developed over many years and assuring that VA's infrastructure and telecommunications wide area and local area networks have the capabilities needed to make business information available to all who need it. The organizational challenge is to have the three Administrations with their specific and diverse missions develop the business processes that will ensure common information and business needs are shared across VA's business lines. The cultural challenges derive from VBA's centralized management style and VHA's decentralized form of management and heavily ingrained professional biases and traditions. An additional challenge arises from the need for reaching agreement on standard data definitions.

*2. Until a candidate for the Department CIO is confirmed by the Senate, who will ensure that the requisite VA IT leadership and management will be carried out to address IT management issues raised by GAO?*

An Acting CIO has been appointed who has as his only function the management of the Department's information technology assets, both existing and proposed. This individual reports to the Secretary on all matters involving information technology (IT), in full spirit of the Clinger-Cohen Act. The day-to-day management of the Department's information technology is being administered and carried out by a fully dedicated staff that answers to the Acting Chief Information Officer. This is the same staff that will provide support to the VA CIO, when he or she is confirmed by the Senate.

Page 2  
Honorable Steve Buyer

***3. What will the reporting relationships be between the Department Chief Information Officer and the Administrations' Chief Information Officers?***

The VA's CIO determines and sets IT policy for the entire Department; policy the Administrations are obliged to follow. The Administrations' CIOs take their technical direction from the Departmental CIO. Currently, the Administration CIOs report to their respective Administration management. They serve their Administration by representing their needs and best interests to the Departmental CIO while they carry out IT policy as determined by the Departmental CIO. If at any point the best interests of the veteran or the Department of Veterans Affairs are not being served I am prepared to change this reporting mechanism.

***4. What will be the roles and responsibilities of the VA cyber security executive and to whom will he report? Will he have responsibility for Department-wide security issues?***

The VA Associate Deputy Assistant Secretary for Cyber Security has overall responsibility for information security in the Department and reports to the Chief Information Officer. His role is primarily that of VA Information Security Officer empowered to issue and enforce policy, procedure, and guidance. In addition, his tasking is to manage those activities, which for reasons of efficiency and cost-effectiveness, are best performed at the highest level. Examples include security training and education, public key infrastructure (PKI), virus defense, intrusion detection, incident handling, risk assessment, security architecture, and certification/accreditation. He is also tasked with the leadership role in VA's information security community, ensuring cooperation of Administrations and Staff Offices.

***5. What is your plan to ensure that VA's security policies, procedures, and guidance are up-to-date, comprehensive, and well communicated throughout VA's administration?***

The Cyber Security Office (CSO) has issued overall information security policies and procedure handbooks. In addition, specific policies for the security of external connections, account and password management, and for limited personal use of government resources have been issued. Two additional policies will soon be issued: Public Key Infrastructure (PKI) and security certification and accreditation.

Page 3  
Honorable Steve Buyer

The project to revamp VA's security policies is in process already. All directives, handbooks, and procedures under the purview of the CSO are currently under review. Based on current laws, executive policies, input from oversight organizations, and VA's risk posture, all will be prioritized, created or revamped, and issued over the next six months. Security enforcement procedures and policies are also included in the comprehensive review.

In addition, the CSO will work with their Administration and Staff Office security colleagues to ensure that policies, procedures, and guidance are understood and disseminated to all employees. The mechanisms for these communications are the Security Subcommittee of VA's CIO Council and the lower-level VA Information Security Working Group. Further, the CSO has a training and awareness program that includes an on-line security awareness course required for all VA employees, contractors, and volunteers. The Department awareness program also includes brochures, posters, and log-on bulletins. The program also provides on-line training for VA's Information Security Officers (ISOs). A VA Critical Incident Response Capability (VA-CIRC) ensures that warnings of potential threats are communicated to VA offices and that local incidents are reported and analyzed.

*6. How do you plan to ensure that policies, procedures, and guidance for the performance of risk assessments on a continuing basis or when significant changes occur as well as on how these risk assessments should be conducted are developed and communicated throughout VA's administrations.*

One of the first orders of business in the Cyber Security Office is to establish a formal process for identifying Department security assets and for recording their security status. A continuous and periodic process of facility and system review, as established under the Government Information Security Reform Act (GISRA), will provide the metrics to determine the effectiveness of the Office's plan. This continuous review will determine if adequate risk assessments are conducted by Department "systems' owners". If the reviews indicate that inadequate risk assessments are being performed, the Cyber Security Office will work with their Administration or Staff Office counterparts to resolve the problems. Issues of chronic problems with risk assessments, or any other security program component, will be brought to the attention of the respective Administration or Staff Office leadership for resolution.

*7. VA has a computer security incident reporting and response system. However, there is no mechanism for routinely analyzing security incident records.*

Page 4  
Honorable Steve Buyer

*Do you plan to establish policies and procedures for the routine analysis of the incident reports generated by the reporting system? How will you ensure that these analyses are done on a regular basis?*

The Cyber Security Office has already noted your concerns with the VA Critical Incident Response Capability's (VA-CIRC) active response to incidents. The office will establish an active process for analyzing incidents and potential incidents. These analyses will be undertaken on a regular basis as well as in response to real-time events. We think that analyzing incidents is merely the second step in responding to them. Our CIRC will soon feature policy and procedure to detect incidents, analyze them, and mount an appropriate defense.

*8. How will the VA ensure that general access control and operating system weaknesses are reviewed and analyzed?*

As previously noted, a continuous and periodic process of facility and system review, as established under Government Information Security Reform Act (GISRA), will provide the metrics to determine the security status of VA's access controls and operating systems.

*9. GAO testified that no in-process reviews or post-implementation reviews have occurred since September 2000. Why hasn't the VA performed these reviews? More specifically, why didn't VA do any in-process or post-implementation reviews on projects that have had problems before, such as the VETSNET/C&P Replacement Effort?*

The guidelines for conducting an in-process review are specified in VA's *Information Technology Capital Investment Guide*. This guidance states that an in-process review (IPR) is initiated when the CIO Council wants to answer specific questions relative to an ongoing project's performance; the Department's CIO requires additional information; or management from an Administration or a Key Staff Office requires additional information concerning an IT initiative. During Fiscal Year (FY) 2001, when specific information was required on an IT investment by either the CIO Council or the Department's CIO, a briefing was requested from the Administration or Key Staff Office. Based on the outcome of this briefing, a decision would be made as to whether a formal IPR was required. In FY 2001, the CIO Council and the Department's CIO decided that the information provided during each briefing adequately addressed all concerns about the IT investment. One exception was an IPR requested on VA's E-Commerce IT investment. The Office of Information and Technology (OI&T) still plans to execute this review during FY 2001. VA also initiated in FY 2001 an

Page 5  
Honorable Steve Buyer

expanded Capital Investment Review Program. This program integrates the use of contractors and VA staff. The contracted support will concentrate on conducting In-Process (IPRs) and Post-Implementation Reviews (PIRs) for approved capital investment proposals. VA staff will conduct PIRs from a random sampling of those IT investments approved by the Department's CIO. Three IT investments have been scheduled for a PIR. OI&T plans to execute these reviews in FY 2001. Two of these PIRs (The Image Management System (TIMS) and Compensation & Pension Training Performance Support System (TPSS), specifically address components of VETSNET, and one addresses a major IT investment (National Enrollment) being executed by the Veterans Health Administration.

*10. When will we see the plan for VA's enterprise architecture? What steps will you take to ensure that this plan is completed? When will the plan be forwarded to Congress?*

VA's Enterprise Architecture Plan is currently scheduled to be completed by August 1, 2001. Developing this plan has highest priority. VA will bring in world-renowned experts to work with the key business people to do this. In addition, top level staff will be assigned to the project to assure its completion. The plan will be forwarded to Congress as soon as it has the Secretary's approval.

*11. Mr. Secretary, do you support the use of the Decision Support System at VHA? If so, how will you ensure that VHA achieves a full return on its investment in DSS? If not, why do you not support DSS use?*

I fully support the use of DSS by VHA as a systems tool for aiding improvement in management of VHA. I have testified to the Committee on Oversight and Investigations that it is necessary to increase the accountability of VHA management to ensure that the resources provided by the Congress and this Administration are effectively and efficiently used. This can only be accomplished if VHA becomes more data-driven in its decision-making and commits itself to detailed analysis of its patient care and administrative systems. The same commercial software that supports DSS, which VHA has implemented, is used by management in over 1,400 hospitals and health care systems worldwide.

I will require the Under Secretary for Health to provide me a semiannual progress report on the utilization of the DSS. In this report, I will require that auditable evidence be provided showing progress made in achieving standardization within the DSS.

Page 6  
Honorable Steve Buyer

Additionally, I will require detailed evidence that increasing use of the system is being made to improve patient care and administrative practices. I will expect that within two years the system will have only small variances in compliance with the published system standardization guidance and that all VISNs can demonstrate substantial and material use of DSS' information.

*12. GAO says that DSS use at your medical centers continues to vary despite the benefits demonstrated by those sites that now use DSS. How do you plan to improve DSS use throughout VHA?*

We acknowledge that despite the demonstrated benefits that many sites currently enjoy as a consequence of using DSS, a number of sites across the system have been lagging in their use of DSS. The successful integration of DSS into the daily decision making processes of networks and medical centers will require two distinct, but not separate, lines of action. These actions will focus on communication and education and upon the integration of DSS data into the ongoing business decision processes within VHA.

The communication and education effort will focus on the successes, benefits and processes employed by DSS users both within and outside the VA health care system. We will benchmark and highlight successful applications of DSS data in patient care delivery and health care administration venues. Our focus will not only be on health care administration managers at the VISN and facility levels, but also on the clinicians involved in the direct delivery of health care.

In addition, we are identifying a variety of internal business processes which will benefit from the use of DSS data. Understanding which business processes will benefit from the use of DSS data and redesigning these processes to incorporate DSS data will send a clear message to all VHA management that we expect DSS to meet our information needs. Some examples of work currently in progress include the conversion from VHA's Cost Distribution Report to DSS data and the introduction of DSS data in the VERA allocation model. Other areas under review include the use of DSS data for sharing agreement negotiations, the use of DSS data as variables in development for local billing charges, and the use of DSS cost and workload data for VA's annual enrollment level decision analysis process.

Page 7  
Honorable Steve Buyer

*13. Since top management support is critical to successful DSS implementation and use, how will you set the expectation that DSS will be used throughout VHA?*

I agree that top management support is the key to success in all-important initiatives. Let me assure you that the Under Secretary for Health and I are in agreement about the potential benefits of DSS. For this reason, the Under Secretary for Health is preparing a plan for meeting the expectations he and I have with regard to DSS information use. The objective of this plan is to define and use measurable criteria to evaluate individual senior managers in their support and use of DSS.

*14. Mr. Secretary, has the VETSNET pilot given you sufficient confidence in the new system to proceed to full implementation? If so, what steps will you take to ensure that VETSNET does successfully proceed to implementation?*

I have directed that we will conduct an independent audit of the overall system before VETSNET becomes fully operational. This audit will provide me with the assurance that this system will meet all the security, functional and performance tests we have set for it. If VETSNET passes this audit, we will go forward with its implementation on our current schedule.

*15. VBA Systems Modernization began in 1986 and has spent at least \$400 million to date with few benefits. How can long-term efforts with such limited results efforts be avoided in the future?*

I have pledged not to spend any new funds on information technology until an Enterprise Architecture has been defined that ends "stove-pipe" systems design, incompatible systems development and data collection that does not yield useful information. I believe that developing this plan, which has my highest priority, will help us avoid efforts that offer only limited results.

**Post-Hearing Questions  
Concerning the April 4, 2001, IT Hearing**

**For  
The Department of Veterans Affairs**

**From  
The Honorable Vic Snyder  
Ranking Democratic Member,  
Subcommittee on Oversight and Investigations  
Committee on Veterans Affairs  
U.S. House of Representatives**

*1. According to various documents you provided, all status reports on VETSNET since July 2000 reported "Problems: Project in Trouble." As of January 5, 2001, only Project Management had improved to "Significant Issues Exist." Given the length of time this project has been in development, please explain why a "Project in Trouble" should be continued.*

As a result of the use of the Project Management Methodology and the associated terminology such as "Problems: Project in Trouble," VETSNET has received a greatly improved management focus. I believe that the current VETSNET management plan addresses many of the past problems that resulted in such evaluations. In addition to these successes, which we believe validate our approach, ratification of the VETSNET strategy was obtained last year through an independent verification and validation of the VETSNET approach and technology by an outside contractor.

VBA is working to transform its methodology for development of new information systems, and to institutionalize those processes that will enhance the likelihood of success. VBA's Office of Information Management was recently reorganized to align the applications architecture function with the ongoing VETSNET and related development work at the St. Petersburg Regional Office. This will ensure that the VETSNET architecture will be adhered to as the standard development platform for all applications utilizing the VBA corporate database. Additionally, VBA is implementing configuration management technology throughout its major development projects. Configuration management enables more efficient software development through management and reuse of software code components, resulting in better software products. Finally VBA OIM is participating in a Department-wide effort to analyze and describe a VA Enterprise Architecture. This will result in better management of information

Page 2  
Honorable Vic Snyder

system and coordination of information technology efforts throughout the agency. A developmental task force has been appointed and is investigating project management software that all components of the Department can use to share information.

*2. In the VETSNET Pilot, approximately 10 "handpicked, vanilla" original compensation award cases were to have been established in the St. Petersburg Regional Office. Our understanding is that small number was too large. Also, what do you mean by "handpicked" and "vanilla", and what is the status of the VETSNET pilot?*

In February 2001, the Veterans Benefits Administration (VBA) successfully piloted the processing of claims utilizing the VETSNET system. Ten veterans were paid using the pilot version of the VETSNET award and accounting system. This pilot effort tested all phases of VETSNET processing from claims establishment through Rating Board action to award payment and accounting. These veterans will continue to receive their monthly benefit checks through the VETSNET system. These successes have demonstrated that VETSNET is a viable system for processing C&P claims.

Ten veterans consented to be a part of this "pilot." The claimants were veterans of the Army, Navy and Air Force. Collectively, their service covered World War II, the Vietnam era and the Gulf War. The age range of the claimants is 23 to 79 years old. Disability evaluations ranged from 10% to 50%. Two of the awards included additional benefits for dependents. Nine veterans were entitled to retroactive payments totaling \$12,998. The total monthly recurring payment is \$2,782.

The ten pilot cases were "handpicked" in that they were called and asked to participate in the new payment system, and they had to elect Electronic Funds Transfer (EFT) for their payment. The status of the pilot is that it is operational and every month these 10 veterans are receiving their payment through VETSNET.

*3. Why will the pilot only use "original award cases"?*

The pilot "original award cases" were completely and successfully processed using the new software. The conversion process from the Benefits Delivery Network (BDN) to VETSNET is not yet complete. We used "original award cases" because they would not require a conversion from BDN to VETSNET.

Page 3  
Honorable Vic Snyder

*4. After so many years and so many millions of dollars, what is this pilot supposed to prove?*

The most significant aspect of the pilot is that it proves we can pay successfully using a system other than the BDN methodology. As a result, we are confident that we can run in parallel until the new methodology is completely tested and the conversion process is complete. Therefore, the pilot has already successfully proved that the software that will be used to generate ratings, record decisions, generate and authorize the awards and make payment is completely functional.

*5. VA cannot tell us how much money it has spent on VETSNET. Can you tell us how many employees have worked only on VETSNET since they started work at VA?*

Since inception of the effort in 1996, VA has expended approximately \$20 million on VETSNET. Included in this amount are payroll funds to support an average of 14 full-time employees. None of these employees have worked only on

VETSNET since they started work at VA. All have been reassigned to VETSNET, having been previously employed throughout VBA in other capacities.

*6. Describe the VETSNET responsibilities currently being handled by Hines.*

Hines is responsible for the database conversion from Benefits Delivery Network to VETSNET, and for defining and developing batch and interface processing. Hines also has responsibility for operational management of the VETSNET hardware. Additionally, and more significantly, a core group at Hines is learning the new software language and methodology.

*7. The institutional expertise resident at Hines is essential to maintain the current payment systems for 3.2 million veterans per month, but for further development of VETSNET also. It would appear after so many years of work, VETSNET continues to be a drain on the remaining staff at Hines. It appears that a significantly diminished staff at Hines has been assigned significantly more responsibility, not just for paying benefits to America's disabled veterans, but for VETSNET as well. Is the VA doing anything to support Hines with its responsibilities?*

Hines is and will continue to be an important resource. Therefore, we have taken several steps to ensure Hines continues to fulfill its assigned responsibilities. For example, we have merged the Hines Benefits Delivery Center and System

Page 4  
Honorable Vic Snyder

Development Center into one organization. One benefit of this measure is increased flexibility to assign resources to tasks performed by Hines. We have also prioritized the workload consistent with resources available at Hines. We have also committed to providing Compensation and Pension (C&P) business staffing support to Hines to ensure the development of functional requirements for the conversion and transfer from BDN to the new system.

*8. In a November 1, 1993 hearing before the Subcommittee on Compensation, Pension, and Insurance, VA said VETSNET would "replace the existing BDN (Benefits Delivery System)." It has not done so. In a June 8, 1998 report, the SRA consulting firm worried that "conversion of BDN data" for VETSNET may corrupt the database". If VETSNET does not, "meet all of the security, functional, and performance requirements" you have set for it, will this be the final evaluation?*

As I indicated in my testimony, I will not throw good money after bad. If VETSNET does not pass the independent audit I have ordered, we will develop a plan to extend the life of our current systems and immediately begin to develop a replacement system.

*9. How many dedicated information security officers does the VA have now? How many are you planning to hire?*

VA has an extensive community of information security staff. These include facility and Staff Office/Program Office Information Security Officers (ISO), their respective Alternate ISOs (sometimes multiple at facilities), security program office staff, and contractors. Every VA facility is required to have a full-time or primary-time ISO. The approximate number of ISOs and Alternate ISOs is 580. The overall security community is larger when security program offices are considered. Note that with the exception of ISOs, many of these positions are part-time. Our GISRA review process will identify the prevalence of full-time ISOs at VA facilities. Based on these analyses, the Cyber Security Office will provide direction to those facilities not having full-time ISO positions to establish the position.

*10. Will the new Security Czar have only the authority to promulgate policies, or also be able to enforce them?*

The VA Cyber Security Office plans to work with all levels of VA to enhance our enforcement capabilities. Specifically, it will work closely with VA's Office of the Inspector General (OIG) and with high-level VA staff officials and Administration

Page 5  
Honorable Vic Snyder

leaders to use existing enforcement capabilities in the interest of information security. The Cyber Security Office will have the ability not only to promulgate policies but also to determine compliance therewith. Where non-compliance is found, appropriate action will be taken.

*11. How seriously do you take the IG's Penetration Review, which seems to indicate considerable vulnerability and possibility of fraud and tampering?*

The VA Cyber Security Office recognizes and respects the OIG's work in the information security arena and specifically their penetration studies. We take their Reviews as primary evidence for the development of our overall security plan. In fact, OIG's studies validate our own findings and experiences. We look forward to working closely with OIG in the interest of protecting the Department's information assets.

*12. What level of confidence do you have that a new system at Austin will act as well as what you now have in Hines?*

We currently have a high level of confidence that Austin can successfully perform the operational part of this new system. The decision to do this at Austin is consistent with our efforts to accomplish data center consolidation. However, we will not become dependent on this arrangement until we have conducted extensive testing and run the new system in parallel with the old. Also, Hines will continue to perform functions that ensure the successful applications payment process and other necessary activities such as configuration and data base management.

*13. Austin uses a computer tape backup system that major corporations have considered obsolete for 5 or more years. Today, major corporations use remote mirroring technology, which provides simultaneous backup on a parallel system. Until Austin can get up-to-date, shouldn't the VA plan to use Hines for backup?*

Many corporations do use remote mirroring technology for mission-critical applications requiring near 100 percent availability, data mirroring, and data replication. However, many corporations also still utilize the same or similar computer tape backup systems that are utilized at Austin and other VA computing centers. There are significant cost considerations to be weighed when deciding upon an enterprise-wide backup and storage approach. Remote mirroring and/or replication require significantly higher investments in hardware, software, and telecommunications. This may be appropriate in some cases, while tape technology may meet business requirements for other business applications. As a fee-for-service provider under the VA's Franchise Fund, the

Page 6  
Honorable Vic Snyder

Austin Automation Center (AAC) provides services to VA and other government agencies through the execution of customer agreements, accompanied by performance service level agreements (PSLAs). Current customer agreements and PSLAs do not contain requirements that necessitate remote mirroring or replication services. However, the AAC is strategically positioned to provide such services should they be required. The AAC has the technology that can easily support data mirroring and replication, either locally or remotely.

CHAIRMAN BUYER TO RICHARD GRIFFIN, INSPECTOR GENERAL,  
DEPARTMENT OF VETERANS AFFAIRS

SUPPLEMENTAL INFORMATION ON VA's INFORMATION TECHNOLOGY

This enclosure presents your questions and our responses, to supplement information provided in our testimony before the Subcommittee on April 4, 2001.

Post-Hearing Questions from Mr. Buyer:

1. Was computer security vulnerability an issue in regard to the recent indictment of a VBA employee at the Houston Resident Office?

The indicted employee was able to take advantage of a Regional Office (RO) violation of information security procedures. The RO believes that she established the false veteran during a brief six-week trial/experiment period, from August - September 1997. During this time, Veteran Service Officers were permitted to have two passwords to speed up the processing of veterans claims. Specifically, this was the "entry of data" password and the "authorization" password. This allowed the employee to establish, adjudicate, and authorize benefit payments. Once this account was established, adjustments could be made without oversight from a supervisor.

The other genuine account the employee accessed in late 1999 and 2000 was simply an entry that "recouped" funds for final payment to an authorized payee after a veteran is deceased. These funds would go to heirs or "other designated payee." Apparently there is no way to find this illegal action in the system, especially if the paid amounts are less than \$10,000.

2. Your information security survey identified significant security weaknesses. In your opinion, which of these should the Secretary address immediately, and, in the next six months?

The following issues should be addressed immediately:

- Appointment and confirmation of a Chief Information Officer for VA.
- Empowerment of the VA Cyber Security Officer to enforce standards already issued by the Assistant Secretary for Information and Technology.
- Centralize the management of the VACO network.
- Staffing effective Information Security Officer (ISO) positions to provide adequate oversight and implementation of necessary security control measures at the local facility level.
- Evaluation and correction of the potential vulnerabilities identified in our probes of VACO networks, data center networks, and selected field stations.
- Correction of the physical security weaknesses identified at the VACO data center and the Austin Automation Center.

The following issues should be addressed within the next six months:

- Implementing department-wide intrusion detection to reduce VA's vulnerability to inappropriate and undetected access to its systems and data.
- Deploying department-wide antivirus regime to better prevent/contain virus outbreaks that continue to occur in VA and cause disruption of services, adversely affect staff productivity, and divert technical staff efforts.
- Upgrading to VA-standard external electronic connections to reduce the vulnerability of VA's systems to penetration because of weaknesses in its external connections.
- Upgrading of all VA Desktop computers used in VA's automated systems to meet minimum acceptable security standards.

3. What computer security weaknesses have your Combined Assessment Programs Reviews identified in the VA?

The following is a list of the issues the CAP reviews have identified:

- A full-time ISO position had not been established.
- Strong password controls had not been implemented to reduce the risk of unauthorized access to VA systems.
- User access levels needed to be promptly updated to reflect current access requirements.
- Physical security of computer room and equipment needed to be strengthened.
- Annual AIS security awareness training had not been provided.
- Facility information system risk assessment and contingency plans needed to be developed to help ensure continuity of operations.

Some of these are repeated in our National Audit. However, I believe that the identification of these weaknesses at repeated sites is indicative of the systemic nature of the problems.

Post-Hearing Questions from Dr. Snyder

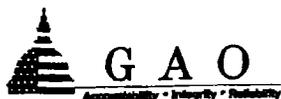
1. Is the VBA too overwhelmed by reform and redesign efforts that it cannot manage to resolve the system penetration threat at this time? Can VBA address the security issue in a series of steps that will not undermine the rest of its agenda? Could you propose steps to do so?

VBA has been reforming and redesigning its benefits delivery system for more than 10 years. The current task, VETSNET, is only the most recent of a series of projects. I do not believe that VBA is 'overwhelmed' with the task. The application of security should be a part of the process not another task. The

'retrofitting' of security to existing applications is one of the main reasons that VBA is in the state it is in regarding security.

Steps that should be taken to address the security vulnerabilities include:

- Each VBA facility should have an Information Security Officer (ISO). Information security should be the primary, if not exclusive, assignment for this person. Implementation of information security should be a critical factor in evaluations for the ISO.
- Each VBA facility director Performance Standards should include Information Security.
- Empowerment of an Information Security Officer at the Central Office level to enforce standards already issued by VA security offices and VBA security offices.
- Upgrading of all equipment to support a more stringent standard of security than is currently possible with Windows 95/98 machines currently in use.



United States General Accounting Office  
Washington, DC 20548

May 2, 2001

The Honorable Steve Buyer  
Chairman, Subcommittee on Oversight and Investigations  
Committee on Veterans' Affairs  
House of Representatives

Subject: Veterans Affairs: Subcommittee Questions Concerning the Department's  
Information Technology Program

Dear Mr. Chairman:

This letter responds to your April 12, 2001, request that we provide answers to questions relating to our testimony of April 4, 2001.<sup>1</sup> During that testimony, we discussed the status of the Department of Veterans Affairs' (VA) efforts to address numerous information technology challenges, including filling its chief information officer (CIO) position, improving computer security, and refining its processes for selecting, controlling, and evaluating its information technology investments. Your questions, along with our responses, follow.

*1. What has been the impact for the VA lacking a dedicated CIO?*

Appointing a permanent CIO is critical to the success of VA's information technology (IT) program. CIOs play an essential role in driving management processes to help control system development risks, better manage IT spending, and succeed in achieving real, measurable improvements in agency performance. Without such an official, VA lacks the level of leadership and focus needed to assist the Secretary and his executive management team in effectively identifying and responding to departmental IT challenges and in using IT to help realize improvements in the department's programs and operations.

VA faces long-standing and critical IT challenges and concerns. Our prior reports and testimonies have highlighted weaknesses in the department's efforts to develop an enterprise architecture, improve computer security, improve IT investment management, and implement and use key information systems. Each of these weaknesses has significant implications for the department, and when considered collectively, they reflect a critical need for the immediate and sustained attention of a CIO.

<sup>1</sup>VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist (GAO-01-550T, April 4, 2001).

In particular, as a key figure in applying technology to improve fundamental business processes and operations, a CIO can play an essential role in facilitating VA's implementation of an enterprise architecture. Without such an architecture, the department lacks fundamental guidance for developing mission-critical systems and achieving the appropriate integration of systems through common standards—which are necessary if VA is to successfully realize its "One VA" vision.

Further, a CIO is vital to the success of VA's information security management program. Despite taking constructive steps to address recognized computer security weaknesses, the department nonetheless needs a stronger management focus to resolve lingering departmentwide security problems. Dedicated CIO and other senior management attention is needed to help ensure that policies and guidelines adequately address the security of the department's interconnected computer environment and other key components of security management, such as risk identification and mitigation. Sustained management attention is also necessary to confirm that security-related activities are periodically monitored, tested, and evaluated, and that appropriate corrective actions are taken, when called for.

VA has also been challenged in managing its IT investments. To its credit, the department has improved its processes for selecting, monitoring, and managing its investments; however, the lack of demonstrated performance in implementing key parts of its investment guidance—such as reviewing on-going and completed IT projects through in-process and post-implementation reviews—deprives VA's top management of vital information needed to evaluate the effectiveness of these efforts and to make critical decisions regarding their development and implementation. Given VA's substantial IT budget and resources, the CIO should have a major role in ensuring that the department's processes for leading, managing, and controlling IT investments are fully instituted and adhered to throughout the department.

*2. In GAO's opinion, which Departments have effective CIOs? What makes them effective? How are these CIOs empowered?*

Our work to date has not included specific reviews of the effectiveness of other departments' CIOs. However, we have recently issued a report on the effectiveness of CIOs in several leading private and public organizations, which highlights a number of factors contributing to CIO successes.<sup>2</sup> Among these critical success factors are the following:

- Senior executives in the organizations embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making. The top executives of these organizations determine how a CIO best fits within existing or new management tiers to guide technology solutions, and CIOs are chosen to match the organizations' needs.
- Effective CIOs have legitimate and influential roles in partnering with top managers to apply IT to business problems and needs. While the placement of the CIO position at an executive management level in the organization is important, successful CIOs earn

<sup>2</sup>*Maximizing the Success of Chief Information Officers: Learning from Leading Organizations* (GAO-01-376G, February 2001).

credibility and produce results by establishing effective working relationships with business unit heads.

- CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy structures, and available IT skills; this structure is necessary to ensure that the CIO's office is aligned to best serve the needs of the enterprise.
- CIOs work effectively with their executive peers to jointly produce a vision that encompasses educating senior managers on the strategic value of IT, providing advice and direction, and setting expectations of what can be achieved. CIOs also participate on executive committees and boards that provide forums for promoting and building consensus on IT strategies and solutions.

These success factors and their underlying principles illustrate the extent to which the work of a successful CIO must extend throughout the enterprise. In particular, they highlight the role that senior executives play in creating an effective management context for their CIOs, as well as the CIOs' responsibilities for building credibility and organizing information technology and management to meet business needs. While the CIO has specific responsibilities that he or she must execute, it is clear from our studies of these organizations that successful CIOs rely extensively on both vertical and horizontal relationships within the enterprise to ensure that their duties are carried out most effectively.

*3. GAO's testimony addressed the vulnerability and weaknesses of VA's IT security. What are the five most important issues the Secretary must instruct the new IT security czar to fix or begin to address in the next 60 days? How about in the next 180 days?*

There are a number of critical IT security issues that VA must address to safeguard its assets, maintain the confidentiality of sensitive information, and ensure the reliability of its data. Consistent with our prior recommendations, the most important issues that the Secretary of Veterans Affairs should instruct the new IT security executive to begin addressing within the next 60 days include the following:

- Assess the status of actions taken to correct security weaknesses identified by VA's inspector general, GAO, VA management, consultants, or other external organizations. For those weaknesses reported as closed, independently validate that the actions taken have corrected the weaknesses. For those that remain open, take steps to implement a plan that sets priorities and requires corrective action within a reasonable timeframe.
- Review progress in implementing the actions in VA's departmentwide information security management plan. Assess all planned near- and long-term actions to ensure that they continue to be valid and monitor the progress of each action against established milestones.
- Meet with the security officers for each of the administrations and their key components, as appropriate, to (1) begin to develop communication lines and coordination efforts

between security functions, as a means of integrating security across all VA component organizations, and (2) assess opportunities to build on existing computer security initiatives. In September 2000,<sup>3</sup> we reported that VA organizations had independently acted to improve computer security, but these efforts were not coordinated as part of a departmentwide program. We noted that these organizations had developed certain guidance and oversight processes relating to key security management areas that could provide VA a starting point to expedite the development of departmentwide policies and procedures for assessing risk, monitoring access activity, and evaluating the effectiveness of information system controls.

- Review the computer security management of VA's wide area network. Currently, authority over operation of parts of the network is decentralized among 10 system administrators, providing the opportunity for security vulnerabilities to arise through the practice of implementing varying levels of security controls. Verify that overall network security is tested, including network security for each administration and central office. To complement this effort, implement a departmentwide intrusion detection program to better protect the network from unauthorized access.
- Require each of VA's key facilities to assign a full-time security officer. In our prior reviews at VA, we noted that most medical facilities did not have full-time security officers.

Beyond these near-term issues, there are other security weaknesses that VA should address within the next 180 days. We have previously reported on and made recommendations related to these weaknesses.<sup>4</sup> Actions needed to address these weaknesses include:

- Developing policies and guidance on how and when risk assessments should be conducted, and defining the level of risk assessment required for system changes.
- Updating the department's security policies and guidance to adequately address the security of its interconnected computer environment and developing technical security standards for VA's system and security software.
- Establishing a mechanism for routinely analyzing security incident records. Such a practice could provide VA with an additional process for proactively identifying and responding to other system security vulnerabilities. In addition, the information could be used to enhance security controls.

<sup>3</sup>VA *Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration* (GAO/AIMD-00-232, September 8, 2000).

<sup>4</sup>GAO/AIMD-00-232, September 8, 2000, and *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4, 1999).

4. *What are the major obstacles the VA faces in coming up with an integrated, department-wide enterprise architecture? Why is this so difficult for the VA?*

The major obstacle that VA faces in its attempts to develop an enterprise architecture is the lack of business and senior management involvement in and support for such an architecture, coupled with each administration believing that it needs its own. VA's CIO organization has not yet gained business-level and senior management support for the enterprise architecture development effort. Doing so is critical since the architecture will serve as a roadmap to achieving the agency's mission and performing core business functions within an efficient technology environment. Not only does VA's CIO organization need senior management to articulate its vision, and the business lines to document their business processes, information flows, and data needs, but it also needs senior management support to institutionalize the use of the enterprise architecture once developed.

However, VA's efforts to develop an architecture have, to date, been limited mostly to CIO and IT staff. As we testified in May 2000,<sup>5</sup> VA's previous efforts to develop an integrated, departmentwide architecture resulted only in the development of a technical architecture. We further stated that VA should initiate a new architecture development effort that incorporates the business lines as well as the IT components. The subcommittee agreed with our recommendation and requested that VA develop a plan, with milestones, for completing that architecture.

Despite VA's statement in its August 2000 Enterprise Architecture Plan that the cross-agency effort would involve both business and IT staff, its subsequent efforts were handled almost exclusively by IT staff. Concerned that VA's business lines were not adequately integrated in prior efforts to develop the architecture, VA's Secretary has now requested that business managers be included in any new development efforts.

5. *VETSNET has taken over 10 years to conduct a pilot test to process 10 pre-selected "vanilla" claims. In GAO's opinion, how long will it take VETSNET to get up to speed on 3.2 million claims payments?*

At this time, it is not possible to state when the Veterans Service Network (VETSNET) will be capable of processing the approximately 3.2 million compensation and pension payments made to veterans and their families each month. The project has progressed in some areas; for example, the Veterans Benefit Administration (VBA) completed implementation of the rating board automation tool in November 2000, and completed development and testing of four other key software components at the end of January 2001. However, the department needs to address several important issues before the compensation and pension replacement system can be successfully implemented.

Although VBA has established a schedule that calls for deploying the compensation and pension replacement system in July 2002, it has not yet completed an integrated project plan and schedule incorporating all the critical areas of this system development effort. Such a

<sup>5</sup>Information Technology: Update on VA Actions to Implement Critical Reforms (GAO/IT-AIMD-00-74, May 11, 2000).

plan is necessary for determining what project activities need to be accomplished and when, and for measuring VBA's progress in meeting the development milestones. Moreover, given previous delays in developing this project, such a plan is essential to helping VBA earn confidence in its ability to successfully proceed with this development effort.

Further, VBA still has to define a strategy for its most complex remaining effort—converting data from the old system to the new compensation and pension replacement system. According to project officials, successfully converting the data will require the involvement of compensation and pension business-line staff who have significant knowledge of the business processes and data needs and can provide necessary input into decisions regarding the system's design, development, and implementation. However, the data conversion effort has already encountered delays due in part to the lack of business-line support.

6. *GAO's testimony indicates that weak management has allowed lingering department-wide security problems. Which management team is accountable for not addressing this issue? What vulnerability issues must the Secretary address with specific instruction within the next 60 days?*

Responsibility for managing the security of VA's computers and data has resided with the department-level CIO, in coordination with administration heads, assistant secretaries, and other key officials. In addition, the Veterans Health Administration's (VHA) medical centers also have responsibility for securing their local systems. However, VA's difficulty in selecting a permanent CIO restricted its ability to effectively deal with departmentwide security issues. The senior executive recently installed to oversee the department's security program will now have a critical role in addressing VA's security challenges.

Issues that VA's Secretary needs to address within the next 60 days include

- defining the role and responsibilities of the security czar and empowering this official with the authority to ensure that the overall security management program is fully implemented departmentwide,
- requiring the security czar to periodically brief the Secretary on plans for improving information security and on progress in implementing these improvements,
- holding all senior managers accountable for ensuring strict compliance with security directives, as the lack of line management accountability is one reason security has not received adequate attention within VA, and
- ensuring that adequate resources are available to implement the actions necessary to improve security.

7. *VA published an updated guide for capital investment in information technology in October 2000. Is the VA following its own guidelines in its IT investments?*

VA's information technology capital investment guide addresses a number of shortcomings that we previously identified with the department's investment management process. Nevertheless, VA has not yet demonstrated that it is implementing key parts of this guidance. For example, the department has included guidance for conducting in-process and post-implementation reviews. These reviews are essential for aiding the department in controlling and evaluating IT investments. Consistent with our prior recommendations, the guidance stipulates that completion dates be included in VA's in-process review plans and that the results of post-implementation reviews of capital investment board-level projects be provided to VA's CIO Council. In addition, the guidance requires VA to conduct quarterly execution reviews of approved IT capital investments to help identify projects experiencing cost, schedule, or performance problems.

However, since September 2000, the department has not scheduled or conducted any in-process or post-implementation reviews, and the director of VA's Information Resources Management (IRM) Planning and Acquisition Service told us that the department has not conducted an IT execution review since June 2000. At the time of our testimony, the department indicated that it intended to conduct one in-process review and three post-implementation reviews. However, it had not established plans or a schedule showing when these reviews would be performed.

VA's IT investment guide reiterates the department's Directive 6000 requirement to maintain complete and accurate data on all personnel and nonpersonnel costs associated with IT activities. However, the department lacks a uniform process for tracking its IT expenditures. Without such a cost-tracking mechanism, VA may lack data needed to monitor and evaluate investments individually and strategically, provide feedback on the projects' adherence to strategic initiatives and plans, and allow for review of unexpected costs or benefits resulting from investment decisions. The director of VA's IRM Planning and Acquisition Service indicated that the department will begin using a new numbering system within its current financial management system, which should enable the department to compile reports on approved capital investment expenditures beginning in fiscal year 2002. However, until its new financial management system is implemented—estimated in October 2004—the department may continue to lack the capability to track complete personnel costs for capital investment projects and all expenditures for smaller IT projects.

8. *In May 2000, the former Chairman of this Subcommittee requested that the VA provide a plan with definitive milestones for completing an integrated department-wide information systems architecture. I understand this has been accomplished. Has the GAO seen this plan?*

We have neither received nor reviewed a plan from VA containing definitive milestones for completing an integrated, departmentwide information systems architecture. Rather, in August 2000, VA provided us with a document that contained high-level estimates of the time required to complete certain elements of the departmentwide architecture. However,

this document did not contain any definitive dates for completing the various elements or the departmentwide architecture as a whole. Moreover, the document stated that a contractor chosen to develop the architecture would be expected to deliver a work plan that identified the methodologies and milestones for completing the development tasks. At this time, we are not aware that this effort has been performed.

9. *How much money has the VA spent on VHA's Decision Support System? How many VISNs still do not utilize DSS? Which ones? How many medical centers do not use DSS? Which do not? Why haven't they implemented DSS?*

According to VA estimates, it has spent approximately \$261 million to develop and operate DSS from fiscal year 1992 through fiscal year 2000. Additionally, VA has reported that it expects to spend about \$50 million to operate DSS in fiscal year 2001.

In following up with DSS coordinators for those VISNs that previously reported not using DSS, we were told that VISN 20 is the only veterans integrated service network that is still not using the system to support its decision-making—although some of its facilities (i.e., medical centers and clinics) do currently use the system. For a VISN to use DSS, all of its medical centers must process their clinical and financial data in the system in a similar manner. However, the VISN 20 DSS coordinator indicated that because DSS data are organized and maintained differently by that VISN's various facilities, the data cannot be compared and thus are not readily usable for decision-making at the VISN level. For example, the coordinator explained that in maintaining primary care data in DSS, the medical centers within VISN 20 will only include data in their DSS primary care departments that pertain to primary care work, while a community-based outpatient clinic may include data that extend beyond primary care work.

DSS has been implemented in all of VA's medical centers since October 1998. Nonetheless, as we testified in September 2000<sup>6</sup> and last month, the medical centers were not using the system for all the purposes that VHA intended. Our most recent work did not include assessing all medical centers' current uses of DSS. However, we did review a DSS processing report, dated March 31, 2001 (the most recent report available), which indicated that all medical centers except the Anchorage Health Care System have completed their processing of fiscal year 2000 data.<sup>7</sup> Further, according to the VISN 20 DSS coordinator, the Anchorage Health Care System does not currently use the system. She explained that the medical center records about 50 percent of its costs (i.e., those costs associated with its fee-for-service program) in a health system module that does not feed data into DSS. As a result, capturing these costs in DSS requires two separate data entries—one that feeds data into DSS and another that records costs in a fee-based category. The official stated that these data entry requirements resulted in the medical center falling behind in processing DSS data.

<sup>6</sup>VA Information Technology: Progress Continues Although Vulnerabilities Remain (GAO/T-AIMD-00-321, September 21, 2000).

<sup>7</sup>The report further indicated that only three DSS sites—the Erie, Pennsylvania, and Tomah, Wisconsin, medical centers and the Chicago Health Care System—had not begun processing fiscal year 2001 data.

Dr. Snyder's questions, along with our responses, follow.

*10. What must the VA do to provide effective, seamless "One-VA" service to America's veterans and their families?*

Information technology is essential to VA's ability to effectively serve the veteran population and is the cornerstone of the department's vision of providing seamless services to veterans and their families. Integral to this vision is the effective and efficient use of current and emerging technology to support the department's business operations and improve overall customer service delivery. Despite its numerous investments, however, the department's IT infrastructure continues to include many standalone and stove-piped systems that do not interface or share information across the department, and thus are inconsistent with the premise of "One VA."

To provide the "One VA" services that it envisions, the department will need to immediately focus on two critical areas. First, as we have previously discussed, VA must complete the process of hiring a permanent CIO. Having a permanent CIO is essential to ensuring that the department's IT resources are effectively managed and that the benefits of its investments are fully realized. Second, the department must ensure that sustained attention is given to implementing an enterprise architecture that will drive the development and implementation of integrated IT investments across the department. Without strong leadership and a clearly defined infrastructure, VA jeopardizes its vision of providing seamless and more efficient service to its customers, and positions itself to continue developing systems in a manner that is neither efficient nor effective.

*11. Would you describe VBA's VETSNET project and estimate how much money and how many employee labor years the agency has allocated to VETSNET-type efforts over the past ten or more years?*

VETSNET consists of a series of projects, begun in 1986, aimed at replacing VBA's aged Benefits Delivery Network. VBA had anticipated that VETSNET, when completed, would allow real-time access to claims information and provide veterans service organizations and other entities greater access to compensation and pension benefit data.

Two of the major projects initiated under VETSNET were the education 1606 replacement project and the compensation and pension replacement project. VBA discontinued the education 1606 replacement project in November 1997 after spending approximately \$3 million on the initiative and without delivering a product. As our prior reports and testimonies have discussed, VA is continuing its effort to develop the compensation and pension replacement project. However, over the years, we and others have reported on problems that VA has encountered in completing the project. For example, we noted that the project was begun before VBA had fully developed its business requirements, and subsequent project delays resulted from confusion over the specific requirements to be addressed. The project has missed several key milestones, including its original May 1998 completion date and a revised date of December 1998. In 1999, VBA modified its strategy for developing the project, with the intent of incorporating software developed outside the

original project, including the rating board automation software tool (which was later modified to become Rating Board Automation 2000) and the Claims Automated Processing System (which was redeveloped into Modern Award Processing-Development, or MAP-D).

We have faced difficulty estimating the funds and staff years expended on VETSNET over the last 15 years because VBA does not directly track in-house staffing costs on a project basis. Rather, VBA estimates costs based on the number of staff reportedly assigned to the project multiplied by a site average cost. VBA also does not track costs incurred at its 58 regional offices for work related to systems development. Nonetheless, in reviewing past and current budget data, we determined that, over the last 15 years, VBA has spent at least \$400 million<sup>8</sup> on systems modernization projects that are now included under the VETSNET initiative. These costs cover the development of the VETSNET hardware environment and certain applications, such as the Veterans On-line Application (VONAPP).

*12. What improvements in veterans' service delivery have been derived from VETSNET?*

Many of the VETSNET components, including the compensation and pension replacement effort, have not yet been completed. As a result, few service delivery improvements have been realized to date. However, one new capability that has helped improve service delivery to veterans is VONAPP. Specifically, VONAPP offers veterans the ability to complete applications for compensation and pension, vocational rehabilitation, and education benefits at their homes, thus eliminating the need to visit a regional office. In addition, the application is transmitted to VBA electronically rather than by mail, thus also helping to reduce processing time.

Further, in November 2000, VBA implemented the Rating Board Automation 2000 software for the compensation and pension replacement project, which was expected to assist veterans service representatives in rating benefit claims. However, according to a VBA official, some regional offices have indicated that, rather than improve service delivery, use of the software tool has resulted in longer processing times. The Undersecretary for Benefits recently suspended the requirement for regional offices to use the software tool until the department has reduced its claims backlog. At this time, we have not collected specific information from VBA demonstrating how this tool has actually performed.

*13. Should VA call a halt to further development of the VETSNET project?*

VBA needs to carefully assess the current VETSNET/compensation and pension project to determine whether it is capable of producing an acceptable return on investment. As we have previously noted, this project has suffered from numerous problems and schedule delays, which threaten the overall success of the initiative. Responsibility for project success is not limited to VBA, however, and the department needs to do more to monitor the progress of this initiative. Specifically, VA needs to strengthen its management oversight to ensure that the project is meeting milestones, is not exceeding costs, and is consistent with the "One VA" information technology environment that the department envisions. VA's IT capital

<sup>8</sup>This amount was spent between fiscal year 1986, when VBA first began modernizing its systems, and fiscal year 2000. Fiscal year 2001 costs are not included in this figure.

investment process includes control mechanisms, such as in-process reviews, to help the department identify and respond to problems encountered in developing and implementing its projects. However, VA has not conducted an in-process review for the VETSNET/compensation and pension project since 1998.

Even if the results of such an assessment are positive, VBA will still need to perform certain tasks before it can successfully complete this project. As previously noted, VBA needs to develop detailed, integrated plans with milestones and costs as a means of determining what project activities need to be done and when, and for measuring the progress of this initiative. VBA also needs to ensure that the project obtains the needed support from the compensation and pension business line. Finally, VBA needs to review critical IT management processes, such as its software testing and evaluation activities, to ensure that its capabilities are at the appropriate level to achieve reliable results.

*14. What is your assessment of top management's commitment and support of information technology, and upon what do you base that assessment?*

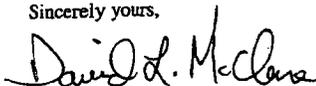
Indications are that top management is committed to and strongly in support of information technology as a critical tool for providing seamless services to veterans and their families. The VA Secretary has testified that resolving the department's long-standing technology problems is a priority, and has declared a moratorium on new IT spending until the department has defined an enterprise architecture. Further, the recent hiring of a senior executive to oversee the department's information security management program and the ongoing search for a CIO suggest that the Secretary is strongly committed to and in support of improving the department's information technology program. However, the success of these efforts depends on the extent to which the Secretary and his executive management remain focused on and involved in addressing the critical IT challenges that VA faces in the months ahead.

-- -- -- --

We provided a draft of this letter to VA officials. Their comments have been incorporated where appropriate.

We are sending copies of this letter to the Secretary of Veterans Affairs and other interested parties. Should you or your staff have any questions on matters discussed in this letter, please contact me at (202) 512-6257. I can also be reached by e-mail at [mcclured@gao.gov](mailto:mcclured@gao.gov).

Sincerely yours,

A handwritten signature in black ink that reads "David L. McClure". The signature is written in a cursive style with a large initial "D".

David L. McClure  
Director, Information Technology  
Management Issues

(310416)