HEARING II ON INFORMATION TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

SEPTEMBER 21, 2000

Printed for the use of the Committee on Veterans' Affairs

Serial No. 106–47

U.S. GOVERNMENT PRINTING OFFICE

71–000 DTP WASHINGTON : 2001

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

COMMITTEE ON VETERANS' AFFAIRS

BOB STUMP, Arizona, *Chairman*

CHRISTOPHER H. SMITH, New Jersey
MICHAEL BILIRAKIS, Florida
FLOYD SPENCE, South Carolina
TERRY EVERETT, Alabama
STEVE BUYER, Indiana
JACK QUINN, New York
CLIFF STEARNS, Florida
JERRY MORAN, Kansas
J.D. HAYWORTH, Arizona
HELEN CHENOWETH-HAGE, Idaho
RAY LaHOOD, Illinois
JAMES V. HANSEN, Utah
HOWARD P. (BUCK) McKEON, California
JIM GIBBONS, Nevada
MICHAEL K. SIMPSON, Idaho
RICHARD H. BAKER, Louisiana

LANE EVANS, Illinois
BOB FILNER, California
LUIS V. GUTIERREZ, Illinois
CORRINE BROWN, Florida
MICHAEL F. DOYLE, Pennsylvania
COLLIN C. PETERSON, Minnesota
JULIA CARSON, Indiana
SILVESTRE REYES, Texas
VIC SNYDER, Arkansas
CIRO D. RODRIGUEZ, Texas
RONNIE SHOWS, Mississippi
SHELLEY BERKLEY, Nevada
BARON P. HILL, Indiana
TOM UDALL, New Mexico

CARL D. COMMENATOR, *Chief Counsel and Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

TERRY EVERETT, Alabama, *Chairman*

BOB STUMP, Arizona
FLOYD SPENCE, South Carolina
STEVE BUYER, Indiana

CORRINE BROWN, Florida
BARON P. HILL, Indiana
TOM UDALL, New Mexico

CONTENTS

SEPTEMBER 21, 2000

OPENING STATEMENTS

WITNESSES

MATERIAL SUBMITTED FOR THE RECORD

HEARING II ON INFORMATION TECHNOLOGY

THURSDAY, SEPTEMBER 21, 2000

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

The subcommittee met, pursuant to notice, at 9:32 a.m., in room 334, Cannon House Office Building, Hon. Terry Everett (chairman of the subcommittee), presiding.

Present: Representatives Everett, Stump, and Brown.

Also present: Representative Evans.

OPENING STATEMENT OF CHAIRMAN EVERETT

Mr. EVERETT. The hearing will come to order. Good morning. This is the subcommittee's second hearing to follow up on the Department of Veterans Affairs—VA—information technology programs.

VA's IT budget is $1.4 billion and has been close to a billion dollars per year for the last 10 years. Our hearing will focus on VA computer security, VA's efforts to develop a Department-wide data architecture, and VA's computer systems, known as DSS and Vista.

We will hear testimony from representatives of the General Accounting Office, the VA Inspector General's Office, and the VA, as well as from Dr. Howard Green, the father of VA's decision support system. We will, again, address extremely serious Department-wide information security weaknesses revealed in GAO and VA IG reviews.

A September 1998 GAO report stated, "these weaknesses placed critical VA operations such as financial management, health care delivery, benefits payments, life insurance services, and home mortgage loan guarantees, and the assets associated with these operations at risk of misuse and disruption.

"In addition, sensitive information contained in the VA system, including financial transaction data and personal information on veterans' medical records and benefits payments is vulnerable to or deliberate misuse, fraudulent use, improper disclosure, or destruction possibly occurring without detection." Unfortunately, I think the IG's representative's testimony may show how true those words were.

The Department's past history in selecting and managing huge IT programs has been extremely poor and has had little to show in terms of better service to veterans and return the investment for taxpayers. We hear the VA's current motto of "One VA" a lot lately. I want to know why the VA can't reengineer its business process

as a Department and why it keeps these efforts separated in three administrations.

The VA has yet to define its integrated IT systems architecture, after requests by this subcommittee to provide a unified plan and real milestones. Ladies and gentlemen, this is not a One VA. This is a VA marching in three different directions.

We will also hear how effectively the Veterans Administration has used its $261 million decision support system (DSS). Maybe today we will find out as well how much longer VBA's decade-old modernization program, VETSNET, is going to take and what it's finally going to do to improve services for the veterans.

We have a full agenda. So I now recognize our ranking Democrat, Ms. Corrine Brown.

OPENING STATEMENT OF HON. CORRINE BROWN

Ms. BROWN. Thank you, Mr. Chairman. Information technology is a rapidly changing field. IT requires large investments every year; the costs are huge. They will not end. Congress must understand they are ongoing costs like food and electricity. The hardware and software are important. But the right management is critical.

Mr. Chairman, the security problems VA faces are serious. They represent an open door to the U.S. Treasury. But I am more concerned about management. The One VA concept, so vital to VA's survival, will either succeed or fail on its information technology. Yet VA's separate administrations for health, benefits, and cemeteries have separate chief information officers. They do not report to VA's top chief information officers but to the separate Under Secretaries for Health, Benefits, and Cemeteries.

VA must commit to outcomes, VA must have an empowering CIO. There is still time for decision. VA faces tough choices on data center consolidation and VETSNET. Today's series of hearings will extend beyond the 106th Congress, no matter which party is in control. Mr. Chairman, the future of VA services delivery depends on how well VA responds to the issues.

Thank you, Mr. Chairman.

[The prepared statement of Congresswoman Brown follows:]

PREPARED STATEMENT OF HON. CORRINE BROWN

Mr. Chairman, information technology is a complex, rapidly changing field. It seems to require larger investments every year. The costs are huge. They will be ongoing costs, like food and electricity. These costs will never go away, never be finally resolved. We in Congress need to get used to them.

Information technology evolves faster than agency cultures and management mindsets. The IT universe keeps evolving even as its users try to fit their systems both to their needs and to swiftly changing possibilities. It is like trying to repair a flat tire on a moving truck. The hardware and software are important, but the right managers are *critical*.

This morning, we will follow up on this subcommittee's May 11 hearing on Information Technology in the Department of Veterans Affairs (VA). At the earlier hearing, the General Accounting Office (GAO) and Office of the Inspector General (OIG) described a decade of unfulfilled promises, missed deadlines, and wrong turns that have cost taxpayers millions of dollars. They also reported that VA is making progress, and we can hope for better results if various recommendations are followed.

VA wants to find new ways of utilizing information technology as a tool to improve service to veterans. That is what Congress wants VA to do.

Mr. Chairman, I remain concerned about the basic IT issues, particularly information security and integrated architecture. The security problems VA faces are serious, of course, and must be addressed. They represent an open door to the U.S. Treasury.

But if I differ with my colleagues on this subcommittee, it is because I am less worried about security than concerned about *management*. The "One VA" concept—so vital to VA's survival—will either succeed or fail on its information technology. Yet VA's separate administrations for Health, Benefits and Cemeteries have separate Chief Information Officers (CIOs) who report not to VA's overall CIO—its Assistant Secretary for Information Technology—but to the separate Under Secretaries for Health, Benefits and Cemeteries.

I am encouraged by the positive direction of VA's capital planning and investment process. However, VA *must* commit to outcomes. VA must have an empowered CIO. VA *must* not allow decentralization to result in a crazy quilt IT network.

I am pleased to see Hershel Gober and Ned Powell—two of the most capable people I have known as appointive officials—directing VA in the final months of the current Administration, while there is still time for decisions. For example, VA faces tough decisions on projects such as the data center consolidation and VETSNET.

Today's hearing is the second in a series of hearings extending beyond the 106th Congress—no matter which party is in control. The future of veteran services delivery depends on how well VA responds to the issues we will raise in this series of oversight inquiries.

Mr. EVERETT. And I thank you. I will ask the witnesses to limit their oral testimony to 5 minutes. The complete written testimony and statement will be made part of the official hearing record. I ask that we hold our questions until the entire panel has testified.

At this point, I'd like to recognize Panel I, Joel Willemssen, Director of Civil Agencies Information Services of GAO and Joel, if you will, I ask you to introduce your staff, please.

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY HELEN LEW, ASSISTANT DIRECTOR; AND NABAJYOTI BARKAKATI, TECHNICAL ASSISTANT DIRECTOR, OFFICE OF COMPUTER AND INFORMATION TECHNOLOGY

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Ranking Member Brown. Thank you for inviting GAO to testify today. Accompanying me are Helen Lew and Naba Bakakati. And as requested, I'll briefly summarize our statement on seven key information technology or IT areas at VA.

First, VA's IT investment decision-making process has improved and it started to implement recommendations we made earlier this year. This should help ensure that the Department can maximize the value of IT investments and assess and manage associated risks.

Second, VA intends to have a chief information officer to direct the Department's IT activities; with the White House announcing last week that it plans to submit a nominee for confirmation.

In the third area, which is development of an overall Department strategy for re-engineering business processes to achieve the One VA vision, VA has not made as much progress. Instead, by delegating primary responsibility for re-engineering to individual VA administrations, each is able to pursue its own initiatives separate and apart from each other rather than focusing on achieving the One VA vision.

Fourth, we're concerned that the Department's strategy for developing a systems architecture will not likely result in the kind of integrated Department-wide architecture that's needed to guide systems development and to ensure the appropriate integration of information systems through common standards. Instead, by allowing each administration to develop its own, at least, three separate architectures could result.

Fifth, VA lacks a uniform mechanism that readily tracks IT expenditures. Instead, VA's different offices use various means for tracking such expenditures. Until VA develops a uniform mechanism, the Department will be less likely to make informed decisions on whether to modify, cancel, accelerate, or continue projects.

Sixth, VA's decision support system and VBA's compensation and pension replacement project continue to face challenges. The decision support system is an executive information system intended to provide VHA managers and clinicians on with data on patient care and health outcomes. However, it's not being fully utilized as demonstrated by the results of a recent survey of VHA's facilities. VHA has initiatives underway to encourage greater use, although agency officials do have some remaining concerns.

Regarding the compensation and pension replacement project, we've reported on problems with this effort for several years. Key issue remains that require top management, including developing an approved project management plan and schedule; addressing data conversion; developing data exchanges in addressing contract or volatility; and staffing uncertainties.

And finally, regarding computer security, VA has begun to address serious weaknesses identified by us and the Inspector General. However, because of these weaknesses, financial transaction data and personal information on veterans' medical records, face increased risks of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Until the Department develops and implements a comprehensive, coordinated security management program, VA will have limited assurance that financial information and sensitive medical records are adequately protected.

Mr. Chairman, that concludes a summary of our statement, and I would be pleased to address any questions that you or the ranking member may have.

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

Mr. EVERETT. Thank you very much. I'm going to allow myself and Ms. Brown both 10 minutes, rather than the customary 5 minutes, because I think this is a very serious issue that we both will have a lot of questions about.

Let me ask you how many times GAO has looked at computer security issues in the VA in the last 5 years?

Mr. WILLEMSSEN. We began looking at computer security at VA in-depth a little over 3 years ago. So that's since 1998. We have issued seven reports and also as part of that, issued two reports that were strictly limited official use only.

Mr. EVERETT. Of all these GAO studies, what recommendations has the VA taken corrective action on?

Mr. WILLEMSSEN. They have been responsive in a couple of areas. One is, they have developed an overall plan to get on top of

computer security issues. Secondly, they recently completed a Department-wide risk assessment of where risks are highest to their systems and associated data. Third, they've recently formed a group within the Chief Information Officer's office to bring more focused attention to the area. And fourth, where we've done specific work at individual facilities, we've seen responsiveness, in most cases, in addressing some of the issues that we've raised from a vulnerability assessment perspective and some of the other related systems issues.

Mr. EVERETT. GAO's September 19, 1998 report titled, VA Computer Control Witnesses Increased Risk of Fraud, Misuse, and Improper Disclosure says on page 23, "in April of 1998, DASIRM officials told us that the VA is in the process of developing a comprehensive security plan and management program that will incorporate a risk management cycle and include requirements for monitoring access activity, reporting security incidents, and reviewing compliance and policies with policies and procedures."

The director of VHA/MISS also told us in April 1998, that "the VHA information security programs office is addressing all of the security issues identified. As part of this effort, MISS plans to change its own site security review procedures and VHA plans to expand current security policy and guidance."

To the best of your knowledge, did any of these actions take place?

Mr. WILLEMSSEN. Mixed, Mr. Chairman. And I would answer it in this way. From a perspective of plans, policies, and procedures, progress has been made. There has now been recently set up a 3-year review cycle for facilities. A new set of policies came out earlier this year where not as much progress has been made as actual implementation. It's one thing and it's an important thing to have policies and procedures so that they can guide the activities of the facilities. It's yet another thing to get those implemented at the individual facilities. And right now, generally speaking, that's where VA needs to focus its activities, making sure that these policies and procedures are implemented, and included within their overall program they need to have a periodic review and evaluation of how well their facilities are doing. That's where they need to focus their attention now.

Mr. EVERETT. Is my observation, after 8 years on the VA Committee and chairing the subcommittee for 6 years, VA is long on policies but short on implementation, in getting things done. This spans 2 years and it doesn't seem to me there's been an awful lot of what you suggested actually put into action. Is that a fair assessment?

Mr. WILLEMSSEN. On the implementation side, there is a ways to go for VA.

Mr. EVERETT. The VA finally adopted the concept of a Department-wide integrated architecture in 1997. We asked for the plan and real milestone dates for completion in our May 11 hearing. We received a 2-page white paper in August stating the VA was going to hire a consultant to help develop this plan. After 3 years, the VA does not even have a draft plan and intends to allow VBA, VHA, and NCA to develop their own architecture. How will "One VA" ever evolve in this kind of strategy?

Mr. Willemssen. We think that VA will encounter difficulties achieving the One VA vision with that kind of strategy. We believe VA needs to reassess that strategy and look at it from a more unified Department-wide perspective, keeping paramount what the needs of the veteran are, what the needs of the primary customer are from a unified perspective.

Mr. EVERETT. It seems to me that we may have a prime example here of people protecting their own turf. I think it's about time for the Congress to do what I did when we faced this Y2K problem 3 years ago, and I called those responsible to my office and I said to them in private and, later, in public, I want to know whose head's going to roll if we don't get this done, because I'm going to make somebody's head roll.

We've had a lot of oversight hearings on this and in my estimation, very little has been done. And at some point, I want to find out why. You state the VA does not consistently track IT expenditures. My subcommittee staff and the minority staff has also requested and reviewed many of VA's IT contracts and concluded that there were a serious lack of consistency in how each administration procured, tracked, and verified and validated with respect to IT procurements.

How can the VA ever determine if all these independent contracts contribute to a One VA goal?

Mr. WILLEMSSEN. Under the current situation, it will be very difficult to do so. The lack of a uniform mechanism for tracking expenditures Department-wide, in combination with the decentralized business process re-engineering and architecture strategies. Those three elements in combination will make it very difficult to achieve the One VA vision as currently laid out.

Mr. EVERETT. How long has VHA decision support system been in existence?

Mr. WILLEMSSEN. Since about 1991.

Mr. EVERETT. How much does it cost?

Mr. WILLEMSSEN. I believe the latest figures through approximately June 30th, were about $249 million.

Mr. EVERETT. How long has DSS been fully implemented?

Mr. WILLEMSSEN. Since approximately October 1998.

Mr. EVERETT. And what can it do? What does DSS do?

Mr. WILLEMSSEN. The focus is on providing managers and clinicians with data on health outcomes and patterns of patient care.

Mr. EVERETT. How many VISNs use DSS?

Mr. WILLEMSSEN. The results of a survey that we found of the 22 VISNs, I believe 18 provided examples of how they used DSS. Now the range of examples varies quite a bit, but we did have 18 of them saying they used it to some degree.

Mr. EVERETT. Which VISNs and specific medical centers utilize DSS most effectively?

Mr. WILLEMSSEN. I believe it was VISNs 13 and 10 that provided us with the most examples of the different categories of use. So that doesn't get directly at your question of efficiency or effectiveness. But it is the best data indicator we had readily at hand where they could show different examples of how they used it. And I think it's a useful indicator. While not exact on effectiveness, it does give you some indication of use.

Mr. EVERETT. Which VISNs and facilities do not use DSS?

Mr. WILLEMSSEN. I believe among the VISNs that did not provide any examples, that was VISNs six, eight, 20 and 21.

Mr. EVERETT. And what is the major reason?

Mr. WILLEMSSEN. There were several reasons that were provided, but the one that came up most frequently had to do with the fiscal year conversion process. And VA is aware of this and is trying to address it in the upcoming cycle. The other issue is also they're aware, for the most part, the concerns and trying to address them.

Mr. EVERETT. Thank you. At this time, I'd ask Ms. Brown for her questions.

Ms. BROWN. Thank you, Mr. Chairman. And first of all, Mr. Chairman, once again, you've mentioned Y2K. That was an area that I was extremely proud of the VA because its leadership led the whole administration. I can't see a reason why we can't take that same concept and bring it over to this particular area.

In fact, it is almost crucial because it's the impetus of whether or not VA is to survive.

Mr. EVERETT. I certainly agree with my colleague, and I thought VA did an outstanding job among government agencies.

Ms. BROWN. It did.

Mr. EVERETT. And I just have to say, in this particular area, that I see an extreme lack of leadership being put forth.

Ms. BROWN. I'm not going to disagree with you, Mr. Chairman. And we've just got to figure out a way to get the leadership and the management in place so we can alleviate this problem just as we did with Y2K. The VA proposed to spend $1.4 billion in fiscal year 2001 in various IT initiatives to better serve our Nation's veterans.

What is your assessment of top management commitment and support of information technology and upon what do you base this assessment?

Mr. WILLEMSSEN. I would—to an overall assessment, I would say that it may be in a bit of a state of flux right now. I think——

Ms. BROWN. I didn't hear you. I'm sorry.

Mr. WILLEMSSEN. I think it might be in a state of flux right now in terms of top commitment. I think the Acting Secretary, I understand, is making this a commitment. I also know that with the White House recently announcing an appointment of a chief information officer, that represents a commitment.

But I also believe that as you and the Chairman stated, Y2K can represent a model to be followed by VA on how to address a tough management challenge. And I think VA can take some of the lessons learned out of the Y2K experience and apply it to some of the issues that we've talked about today.

It shows that the Department, when faced with a tough management challenge, can succeed. And I think if they put the kind of attention and resources on the issues we're talking about today, they can also succeed on this issues.

Ms. BROWN. I have a question on whether or not VA, in this area, should be centralized or decentralized. Somebody has got to be held accountable.

Mr. WILLEMSSEN. Yes. What I would suggest in the business process re-engineering, the systems architecture, and the cost

tracking area, there is a need for a more Department-wide approach to ensure some consistency and to really get at the One VA vision. As we've previously reported, if the Department is serious about One VA, then you have to carry out your initiatives to support that vision and doing it in a stove pipe fashion is not going to get you there. And you need to look at it from a more integrated Department-wide perspective.

Ms. BROWN. Would you describe the VBA's VETSNET project and estimate how much money and how many employees, labor years, and agencies have allocated the VETSNET-type effort over the past 10 or more years?

Mr. WILLEMSSEN. Ranking Member Brown, let me defer to my assistant director, Helen Lew, to provide—to answer that question.

Ms. BROWN. Okay. And what improvements to veterans service delivery have been derived from the VETSNET?

Ms. LEW. Okay. As far as VBA's system modernization, going back to the early 1990s, our cost estimate is something like $391 million. Now you specifically asked Ranking Member Brown about VETSNET. The VETSNET C&P replacement project cost, we have that estimate as about $17.9 million. Regarding your question about how has VETSNET improved services to veterans, we really are not sure, at this point, as to how specifically how that would improve things like timeliness and accuracy of services to veterans. One thing that the VETSNET project hopes to do is be able to implement new technology so that we can continue to pay veterans on time.

Ms. BROWN. Just a follow-up—from the amount of workload that I have in my one district office, part of the problem is the length of time that it takes to process claims. Is this a part of what you do? I mean VETSNET.

Ms. LEW. Well, VETSNET, they're hoping—VBA hopes that VETSNET will help them more efficiently process claims by being able to get various information from external organizations, such as the DOD, electronically. And they're also trying to allow the veterans to file their applications electronically. So there are some IT efforts underway to improve that overall process.

Ms. BROWN. Well, should we continue with it? Should we—I mean, what is your recommendation?

Mr. WILLEMSSEN. There are some——

Ms. BROWN. Is it working?

Mr. WILLEMSSEN. I think VA does need to address some issues in order for this effort to succeed such as converting data, making sure that data exchanges between this system and other systems are dealt with. And so there are issues still to be addressed in that particular effort.

Anything you want to add?

Ms. BROWN. I mean, should we have a time out and re-evaluate this?

Mr. WILLEMSSEN. Well, one thing that I'll point out in VA's favor is by taking an incremental pilot-based approach, that helps reduce the risk in the event they do encounter problems. They aren't looking at this as putting all their eggs in one basket. It is an incremental approach with a pilot test to the extent that that pilot test

is successful and it can move on and take on consideration of more full implementation.

Ms. LEW. I'd just like to add that it is our understanding that VA plans to process 10 claims early next year to test out the C&P replacement project. But I think, as we mentioned in Mr. Willemssen's testimony, before they can take the pilot and go forward with a full-fledged system, there are some things. They need to come up with a plan and a schedule for the various deliverables; they need to address things like data conversion issues and being able to do data exchanges between the VBA, C&P system, and the other VA systems.

Ms. BROWN. I think I asked how much money has been spent in this area.

Ms. LEW. Our data shows that since fiscal year 1990, VBA has spent a total of about $391 million on system modernization. That includes not only C&P but also the IT efforts on education, vocational rehabilitation, and loan.

Ms. BROWN. And how would you evaluate the program based on the amount of dollars that they've spent? Is it an A? I mean, give me some kind of rating.

Mr. WILLEMSSEN. I would say, overall, the evaluation would be not bright. What you'd want to focus on there is ask VA for that kind of investment, what can you show us on the benefit side? We haven't seen anything approaching the amount of dollars that have been invested.

And, therefore, I don't think you can view this as a success until VA can show, at least, more than a one-to-one return on investment. If they expended almost $400 million on this effort over 10 years, then we'd want to see, you know, on the benefit side, there should be at least that amount in return. We haven't seen that; therefore, I don't know how you could view it as a success.

Ms. BROWN. Thank you very much, Mr. Chairman. I yield back.

Mr. EVERETT. Thank you, Ms. Brown. I thank the panel for its usual good work and we appreciate your testimony here today and we may have additional questions for you.

Mr. WILLEMSSEN. Thank you, Mr. Chairman.

Mr. EVERETT. At this point, I'd like to recognize Michael Slachta, the Assistant Inspector General for Office of the VA Inspector General. And Mr. Slachta, if you will, introduce your staff, please, sir.

STATEMENT OF MICHAEL SLACHTA, JR., ASSISTANT INSPECTOR GENERAL FOR AUDITING, OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY STEPHEN L. GASKELL, DIRECTOR, CENTRAL OFFICE OPERATIONS DIVISION, AND THOMAS PHELPS, AUDIT MANAGER, CENTRAL OFFICE OPERATIONS DIVISION

Mr. SLACHTA. Good morning, Mr. Chairman.

Mr. EVERETT. Good morning.

Mr. SLACHTA. Ranking Member Brown.

Mr. EVERETT. Will you introduce your staff and proceed with your testimony.

Mr. SLACHTA. Mr. Stephen Gaskell, Director of my Central Office Operations Division, and Mr. Tom Phelps, Audit Manager, Central Office Operations Division, accompany me.

Mr. Chairman and Ranking Member Brown, I'm here today to report on our findings concerning the Department of Veterans automated information systems security program. During the past several years, the Office of Inspector General has identified Department-wide weaknesses in automated information security that makes VA's programs and financial data vulnerable to destruction, manipulation, and fraud.

Recognizing the seriousness of these issues, in fiscal year 1998, the Department reported information security as a material weakness under the Federal Managers Financial Integrity Act. Given the significant information security weaknesses that were identified in VA, the OIG has continued to focus audit coverage in this area. To the extent that our resources permit, our audit coverage will address the Department's information review and reporting requirements.

The OIG has been involved with the review and oversight of the Department's information security program for several years. Our work has included information security assessments of the Department's national data centers; the Veterans' integrated service networks; medical centers; and regional offices.

In addition to these efforts, we also identified an automated information security re: weaknesses as part of our vulnerability assessment we completed involving VBA's compensation and pension program. This assessment was done in response to a request for assistance from the Under Secretary of Benefits to help identify internal control weaknesses that might facilitate or contribute to fraud in the compensation and pension program.

The following describes, in a general sense, a few of our information security audits and reviews that have identified significant control weaknesses that makes VA's systems and data vulnerable to unauthorized access and misuse.

Audit tests, associated with our 1999 consolidated financial statement audit, demonstrated widespread system security control weaknesses. During this audit, control weaknesses were identified in the following areas:

In VHA, evaluations of the automated information security management program had one VISN and four health care systems by the OIG and the General Accounting Office, found widespread information security control weaknesses. While our evaluations also found that a number of significant corrective actions were initiated to address information security weaknesses, VHA's program and financial data continue to be vulnerable to error or fraud because of serious weaknesses in automated data processing general controls throughout VHA.

While VHA's management has taken action to improve information security, we found that these efforts will not result in adequate security unless there is better integration of their security management program. We do not believe that VHA will achieve adequate security unless VHA managers commit and dedicate adequate resources to their local security programs.

In VBA, we contracted to conduct penetration testing of VBA systems to help assess the effectiveness of information systems general control. The review concluded that a number of significant control weaknesses existed that make VBA systems vulnerable to un-

authorized access and misuse. These control weaknesses were so serious as to affect the security of information contained in VBA records to the individual veteran level.

In response to the penetration testing results, the Under Secretary of Benefits reported that corrective actions had been taken in a number of problem areas, with planned corrective action to be completed for all problem areas during fiscal year 2000. In addition to these efforts, the former Principal Deputy Assistant Secretary for Information and Technology stated that his office would provide whatever manner of assistance that was needed to VBA to facilitate correction of these significant security control weaknesses.

As part of the Inspector General's ongoing evaluation effort, our CAP reviews provide an independent and objective assessment of key operations and programs at medical centers in regional offices on a cyclable basis. CAP reviews—that's a Combined Assessment Program review—completed at 10 facilities during fiscal years 1999 and 2000 to date, have identified the following security control weaknesses.

In medical centers, we found that passwords were not changed at designated intervals. That all users with access to information systems needed to use stronger passwords. That user access levels needed to be properly updated to reflect current access requirements. Physical security of computer rooms needed to be improved. Annual information security awareness training for employees was not provided. And information systems contingency plans did not include a prioritization of mission-critical systems, designation of an alternative processing facility, or include post-disaster as to recovery issues.

In the regional offices, we found the duties of the benefit delivery network security officers and their alternates needed to be assigned to individuals not directly involved with the claims processing. All users with access to information security systems needed to use stronger passwords. And employees with access to information systems needed to receive security awareness training and annual refresher training.

In response to each of the information security weaknesses identified, medical center and regional office management agreed to take necessary corrective actions that we had recommended.

An audit was conducted to test the existence of the control weaknesses identified in our 1990 vulnerability in St. Petersburg. In addition, we tested various methodologies for detecting the existence of fraud. The audit confirmed that most of the information-related weaknesses identified in the vulnerability assessment existed at the regional offices.

Some stations were using employee's multiple passwords under multiple identification numbers to enhance employee production, but what actually occurred was the defeat of controls intended to promote separation of duties and prevent fraud or program abuse.

A timesaving feature that allows employees to complete various claims actions provided the opportunity for improper access.

Passwords, again, needed to be more secure.

Target security records were poorly structured and lacked personal identifying information.

In response to the report, the Under Secretary of Benefits agreed to take necessary corrective actions to address the identified control weaknesses.

This concludes my testimony, and I'd be pleased to answer any questions that you or the ranking member may have.

[The prepared statement of Mr. Slachta appears on p. 53.]

Mr. EVERETT. Thank you, sir. I must tell you that when I read your report that you've just summarized for us, I found it frightening. And that may be an understatement.

Could you please give me an indication how recently the testing was done?

Mr. SLACHTA. We tested during early 1999 and we are continuing to test today.

Mr. EVERETT. Obviously, I'm not going to ask you who the contractor was but his methods, would you call them sophisticated and cracking or would they—or have we got another case of a 17-year-old computer-knowledgeable young person being able to violate this system?

Mr. SLACHTA. In today's society, I wouldn't underestimate a 17-year-old. But no, I would not consider them sophisticated.

Mr. EVERETT. How far were your hired hackers able to get in?

Mr. SLACHTA. We were able to get in pretty far.

Mr. EVERETT. Were you able to get into the backbone of the system?

Mr. SLACHTA. Yes, sir, we were able to get into the backbone of the system.

Mr. EVERETT. In other words, you owned the system?

Mr. SLACHTA. Yes, sir, that was correct.

Mr. EVERETT. If you're on the system, what can you do? Could your team of hackers access data about veterans?

Mr. SLACHTA. As I indicated in the testimony, we were able to get to the individual veteran record.

Mr. EVERETT. What kind of computer data could they access—confidential information such as veterans' personal history, financial, medical information?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Would there be computer information such as a veteran's family member receiving benefits from VA?

Mr. SLACHTA. The master record identifies that a veteran has dependents. It does not necessarily identify the individual dependent.

Mr. EVERETT. Would there also be access to the VA's internal business data and interfaces with which computer systems, say externally, that the VA's linked to?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Did the VBA know its computer system had been hacked into?

Mr. SLACHTA. At the time that we did the reviews, they did not know.

Mr. EVERETT. That's good enough. So it's possible that others with less benign motives may have visited VBA's computers without VBA knowing it?

Mr. SLACHTA. The possibility is there. Yes.

Mr. EVERETT. Put it another way. Was there any way that VBA could have detected it? Did they detect your hackers?

Mr. SLACHTA. No, they did not detect our hacking. There were ways they could have but they did not.

Mr. EVERETT. How about the Veteran's Health Administration computer system? Was there penetration testing of them?

Mr. SLACHTA. We did not do penetration testing of the Veteran's Health Administration's system.

Mr. EVERETT. Have you assessed VHA's vulnerabilities?

Mr. SLACHTA. We think their vulnerability is high, sir.

Mr. EVERETT. In other words, you could get into the VBA's computers through the back door?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Would that include any computer-based medical records and informations that VA hospitals have?

Mr. SLACHTA. There's high a possibility of that. We did not do that, but there is a high possibility.

Mr. EVERETT. If you went in the back door, then, you could, obviously, get wherever you wanted to in the system?

Mr. SLACHTA. We believe so.

Mr. EVERETT. Given the state of security, could VA hospital computers have been hacked into without VHA's knowledge?

Mr. SLACHTA. I don't know, sir. We did not test theirs. So I don't know if they were aware, at that point, or not that we had gotten into the back door.

Mr. Everett. Well, if I make the statement that if I got into the backbone of the system, that I would assume that I could go into the VHA system.

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. How long has VA been aware that it had serious computer security problems, including vulnerability both to hackers and unauthorized inside access to systems?

Mr. SLACHTA. We've been reporting this—reporting the high vulnerability in the computer systems with our financial statement audits going back to 1997.

Mr. EVERETT. Would you agree that when the penetration tests occurred, VBA's security was ineffective and that VHA security would have been equally ineffective if penetration testing had occurred?

Mr. SLACHTA. I would say that VBA's security was ineffective. I don't know about VHA because we did not push theirs.

Mr. EVERETT. I would assume that the IG's office intends to follow up on these security issues.

Mr. SLACHTA. Yes.

Mr. EVERETT. Would the follow-up include more penetration testing?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. I think it should and I would hope that you would do that and I think it should also include VBA and VHA. Poor computer security does expose VA to fraud, does it not?

Mr. SLACHTA. Yes, sir, it does.

Mr. EVERETT. If you will, please, tell the subcommittee briefly what you can say publicly about the work of the IG's office on recent fraud cases and fraud investigations going on right now that relate to computer security and internal controls?

Mr. SLACHTA. At this point in time, we have three convictions for employee fraud due to the lack of internal control and possible computer security violations. We have many investigations underway at this time. We suspect that we'll be addressing further internal control problems.

Mr. EVERETT. If I surmise from your statement, that we might find more fraud cases involving VA employees. Would that be an accurate statement?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Would the three cases that have been sentenced, would two of those both be in excess of $600,000?

Mr. SLACHTA. Oh, yes, sir.

Mr. EVERETT. And the third?

Mr. SLACHTA. Is around $50,000.

Mr. EVERETT. And I believe all three of those are now serving prison sentences?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Would you characterize the number of investigations in the dozens?

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. Finally, let me, before I hand off to my colleague, let me ask very pointed questions. If I got into the backbone of the system and I went down into the finance office, could I write myself a check to a vendor that did not exist?

Mr. SLACHTA. I'm not a computer expert in that sense. But it is my belief, from what my staff told me, that you probably could.

Mr. EVERETT. And if I were a VA employee and I wanted to create a record or a payment to me, either in my name or get another Social Security number that was valid, could I do that?

Mr. SLACHTA. That was what was done in New York, sir.

Mr. EVERETT. Do we have any idea that this was not done elsewhere?

Mr. SLACHTA. No.

Mr. EVERETT. We may not know that it was done elsewhere but we do have a history of fraud within the VA. I don't know how we can categorically say it was not done.

Mr. SLACHTA. Correct.

Mr. EVERETT. Is there any way of ever determining that?

Mr. SLACHTA. We have some tests that we believe that we can use to identify some situations. We're in the process of——

Mr. EVERETT. You're running claims against Social Security numbers?

Mr. SLACHTA. Oh, that's done every year, sir. The problem comes in when you use a legitimate Social Security number. What we're trying to do is, we're trying to validate that everybody in the system is, in fact, a veteran.

Mr. EVERETT. You do that by checking into the regional offices. If you'd rather not answer your method.

Mr. SLACHTA. I would prefer not to answer in a public forum.

Mr. EVERETT. Certainly. I will probably have additional questions, but at this time, let me recognize Ms. Brown.

Ms. BROWN. Thank you, Mr. Chairman. I understand that this is a problem for VA but this is very scary for me, for all the federal agencies. Because if VA gets a "D" with this, I understand that the

rest of the federal agencies are worse than VA and that we have problems in this area with Defense, Aviation, the corporate community. This is very scary for me because I don't even trust debit cards, you need to understand.

How early in 1999 did you do this? What's the time frame?

Mr. SLACHTA. We started our testing, actually, in December of 1998, the penetration testing. We completed it in January of 1999.

Ms. BROWN. And so, to your knowledge, has VA implemented any upgrades or any programs to alleviate some of these problems since that time frame?

Mr. SLACHTA. The Under Secretary for Benefits has reported correction of 12 of the most serious issues that we reported on and he has provided us a schedule that says he's going to address the remainder by the third quarter of fiscal year 2000. We've not tested that. That's what we have.

Ms. BROWN. I've got to ask this question because I think it's so important to know who's in charge and who's responsible and the way the VA system is set up. In this area should it be centralized or decentralized? I mean, I need who's in charge, who's going to be responsible. You have all these various systems out there to have a better delivery system. But I don't know in this particular area whether we're talking about financial accountability.

Do you think it should be centralized or decentralized?

Mr. SLACHTA. We believe it should be centralized.

Ms. BROWN. Okay. And I have some other questions. Does VA need additional staffing to implement the changes needed to assure adequate internal control and quality? Or do the people who are there need better accountability?

Mr. SLACHTA. I'm not in a position to address VBA's staffing or VA staffing in total. What I can say is that the resources that are currently committed to information security, are insufficient. It is a collateral duty. We do not believe it should be a collateral duty.

Ms. BROWN. Explain.

Mr. SLACHTA. We think security is important enough that it requires—that it is a full-time job.

Ms. BROWN. It is.

Mr. SLACHTA. And it is not now.

Ms. BROWN. I see. Can we make the system crook-proof?

Mr. SLACHTA. No system is going to be crook-proof. A conspiracy is going to defeat any system. We certainly can make it tougher than it is right now.

Ms. BROWN. So we shouldn't look at this as just the cost of doing business.

Mr. SLACHTA. No, ma'am, it is not just the cost of doing business.

Ms. BROWN. What are some of your recommendations that you would recommend that VA implement to safeguard the system as best we can?

Mr. SLACHTA. We have made specific recommendations for computer security type of issues. I would rather not, in a public forum, speak to the exact recommendation.

Ms. BROWN. That's fine. Can you tell us whether or not your recommendations have been implemented?

Mr. SLACHTA. Again, the Under Secretary has indicated to us that he's taken the top 12 and he has corrected those.

Ms. BROWN. But you cannot verify that to us today?

Mr. SLACHTA. No. We will not do that. We will do verification as part of our normal next audit—the consolidated financial statement audit will look at the ADP controls, we will do the verification work at that point.

Ms. BROWN. Well, as serious as this problem is, you don't think that we should have some kind of a test run or something before then? I mean, I don't know what's the time frame.

Mr. SLACHTA. Well, that audit is in process now.

Ms. BROWN. Okay. Well, in rating, what I really understand is A, B, C. How would you rate the system as we speak today?

Mr. SLACHTA. I have difficulty with rating systems. I mean, I would say that our system is highly vulnerable. I can't rate it. I don't know what an "A" is or an "F" is. It's a highly vulnerable system. And the Department recognizes that by calling it a material weakness. I think that's important to recognize.

Ms. BROWN. I've got to ask you again. You're saying it but I guess you're not saying it so I can understand it. Has the Department taken the steps to correct the problems as we speak today? You can't verify that, yes or no?

Mr. SLACHTA. No, ma'am, I cannot verify that. They have indicated to us they've taken certain steps. There are further steps that need to be taken and will be taken during the course of the year. Beyond that, I cannot go.

Ms. BROWN. Thank you.

Mr. EVERETT. If I read what you're saying that as far as penetration of the system is concerned, there were very unsophisticated methods that were used to penetrate the system. And I guess what you're saying is that we should have a system that's more like a rock rather than a mushroom.

Mr. SLACHTA. I would hope so. Yes, sir.

Mr. EVERETT. Are you familiar with my letter of July 20, 2000 and VBA's August 15 response to it?

Mr. SLACHTA. Yes, sir, I was given a copy.

Mr. EVERETT. In your opinion, did VBA address the concerns I raised in my letter?

Mr. SLACHTA. The specific concerns about using the private companies and looking at what they are doing, no, it's not addressed, sir.

Mr. EVERETT. Have you seen any work product from the Data Task Force mentioned in VBA's response letter?

Mr. SLACHTA. We've not. No, sir.

Mr. EVERETT. Do you know what the Program Integrity Teams have accomplished since being established?

Mr. SLACHTA. No, sir, we do not. We know that they've had meetings, that they are in the process of developing control structures and procedures, but we've not seen any work product yet.

Mr. EVERETT. That's another thing. In the last 8 years, I've noticed that what VA is good about is having meetings. Do you know what VBA has done regarding intrusion protection?

Mr. SLACHTA. To some extent, I do. Yes, sir.

Mr. EVERETT. You would not like to describe that one.

Mr. SLACHTA. Not at all, sir.

Mr. EVERETT. Do you know whether VBA has addressed the vulnerabilities listed in the IG's assessment?

Mr. SLACHTA. I know they have addressed some of the vulnerabilities. They have indicated agreement and indicated that they were willing to take action on all of them. It has not been completed and there's some good reasons for some of them not being completed.

Mr. EVERETT. Sir, there are a lot of questions that I may ask you in private that I will not ask you in public.

Mr. SLACHTA. I'll be glad to meet with you, sir.

Mr. EVERETT. I think it's scary, frightening, the condition that the VA has allowed the computer security to get in. As I understand it, if you're on the system, you can go anywhere you want to go in the system. Now I recognize that the VA has possibly plugged some of these avenues. But in my, somewhat, limited knowledge of computers, I also recognize that it's not sufficient. That there are still methods.

And we also have to recognize that we were dealing with unsophisticated hacking methods. A hacker with a purpose, using a more sophisticated method, could probably do a great deal of damage to the VA. And may, indeed have, done a great deal of damage, one way or the other to the VA. We cannot disprove that they have not done that.

So I thank you for your work on this. The panel will probably have additional questions for you.

Mr. SLACHTA. Yes, sir.

Mr. EVERETT. I'd like to recognize Dr. Howard Green, who retired from the VA in October of last year. Dr. Green has been deeply involved with the DSS program since 1983, to include serving as Deputy Director for Technical DSS Implementation. He's also served as the chief of staff for the White River Junction VA Medical Center and as the associate dean of VA Hospital Affairs at Dartmouth Medical School.

Welcome, Dr. Green.

Dr. GREEN. Mr. Chairman and Ranking Member Brown, I'm appreciative of your invitation.

Mr. EVERETT. Could you hold up just a second?

Dr. GREEN. Certainly.

Mr. EVERETT. Our clock is not working here, and we've been informed that we do have a vote underway. So Ms. Brown and I will have to delay the hearing until we can go to the House floor and vote. So we'll just delay the hearing until that time. Thank you.

[Recess.]

Mr. EVERETT. The hearing will come to order and resume. Dr. Green, if you will, limit your testimony to 5 minutes, and your complete testimony will be made a part of the record. You may proceed, sir.

Dr. GREEN. Mr. Chairman——

Mr. EVERETT. Before I do that, without objection here, let me make my letter of July 20, 2000 to Honorable Joseph Thompson and the VA's response a part of the record.

(See pp. 31 and 34.)

Mr. EVERETT. Let me, again, recognize Dr. Howard Green.

Thank you, sir, and you may proceed.

STATEMENT OF HOWARD H. GREEN, RETIRED VA EMPLOYEE

Dr. Green. Thank you, Mr. Chairman. I appreciate your invitation to come to this hearing. I will make my statements brief and to the point. I feel like a skunk at a lawn party in this case because of what I might have to say.

The VA contract for the implementation of DSS finished in October of this last year and it was a successful contract. I'm glad to report that for the implementation phase, it came in under budget, on time, with more functionality available than was contracted for. I don't think you'll hear that very often.

The question is, what about the use of DSS and are we getting a return on investment for our large expenditure? And if we are not, why are we not? The answer is direct, sir. We are not getting our return on investment, and we should be.

But this is not an unusual phenomenon. The issue of Fortune Magazine on June 21 gives a rogue's gallery of 12 prominent CEOs that failed in industry and were relieved of their jobs, and their principal problem was failure of execution. These are good people; they will go on to other jobs and probably do well. But failure of executing systems and programs are what we're really talking about.

The DSS system, as it exists in the VA, is used by over 1,400 medical centers and health care systems worldwide. And 10 of the top 15 U.S. hospitals, as mentioned in U.S. News and World Report, have this system. It would be disingenuous of me to say that all are using it and getting a full return on the investment. But the sheer mass of the programs out there says that many people think it's worthwhile. I would mention Cleveland Clinic and Mayo Clinic as two of these.

Now the question, then, becomes who's responsible? Why isn't it getting the return on investment that we know it can get? I think President Truman's—Harry Truman's—sign on his desk—The Buck Stops Here—says it all: it is a summary of management and organizational theory starting from the time it all began. And what he meant by that is the buck stops with top management.

What do I mean by top management? I mean, top line management from the Secretary through the under secretaries, right down to the hospital directors. I do not mean the CIOs and CFOs. I will not discuss the reason for that now, but I will make the statement and you can question me on that later, sir, if you wish.

Now why is it that we have a dichotomy in our system between medical care where there is extraordinary accountability, and the legal system makes sure of that, and management? There are lots of reason for that but I think it's a cultural issue. I think we are in a system where accountability isn't the rule in management. And why is that?

Well, one of the factors is that the system, as it currently exists for getting resources, works. You lay the dead body on the table and you seem to be able to get money for it. The Washington Monument is portrayed as going to fall if we don't get the money. I'm concerned about what top management does as reinforced by management literature and what we've seen clearly shows that when top management speak, people listen.

In two meetings recently of large audiences in the VA, it is reported to me that the acting deputy secretary indicated that he really didn't have much use for DSS. He said, data was bad and there was no standardization. Some people, believing that, said, basically, I've got my marching orders. I don't have to do this. That's of grave concern because top management rules the roost. People in authority have an obligation to understand what they're saying before they say it. Those statements were not true.

There's no ownership of the VHA, DSS system. And what I mean by that is, there's no business plan signed by an executive in line authority that, basically, says this is our plan for DSS; this is what we're going to do; and we're going to use it.

The excuses to attack the system—I see that I have a warning light on so I won't give you the litany. I have some suggestions: get a business plan for DSS; use the opportunities in reducing and getting your return on investment from the functionality of the system to reduce cost, both in direct patient care and the production of the products that feed it.

Make sure you have an operational process improvement system which DSS supports—which, by the way, has to be done locally, led centrally but done locally. Get rid of this excuse "my VISN is not ready yet." There's no justification for that statement at this point. You have to involve the caregivers in this process—the physicians, the nurses—you have got to demonstrate real achievement; you have got to stop feeding failure with money; and you have to insist on outputs and not inputs.

The number of meetings held, the number of white papers written, the number of directives signed, the number of committees formed, the reorganizations and movement of the chairs on the deck of the Titanic, don't cut it.

Thank you, Mr. Chairman.

[The prepared statement of Dr. Green appears on p. 58.]

Mr. EVERETT. Thank you, Dr. Green. I can't say that anything you've said comes as a surprise to this subcommittee. In the 6 years I have chaired either this or the Benefits Subcommittee, those are some of the same obstacles that we've run into for the past 6 years. There certainly is a cultural problem within VA. There is also a tendency in the VA to not hold anybody responsible.

Further, when you try to get to the root of a problem, you can never find the donkey that you need to pin the tail on because he's never there. You will notice that there is no top management at this meeting today. That's not because they were not requested. Had I known earlier, I would have subpoenaed them.

When we first informed them that this meeting was going to take place, their schedules were open. By the time they got the letter to attend, their schedules were closed. As I said, if I had known this earlier, if we were not so late in the year, I would subpoena those gentlemen to appear before this subcommittee.

But there's a remarkable lack of responsibility in top management and within the VA, and that's unfortunate. Because it's our veterans who suffer and it's also the taxpayers who pay good money for veterans' care who suffer. The situation about the security is unbelievable; it is absolutely unbelievable.

And as far as Chairman Horn giving the VA a D, I'm going to ask him to reassess that and give them an F–, if that's the lowest thing that he can give them, because they certainly deserve to be there.

Let me ask you using DSS to maximize potential in the VA and getting a better return on the $261 million investment would be among those things that you named just a few minutes ago?

Dr. GREEN. Yes, sir, it would. I talk about top management because top management has to be committed to getting the return. It has to be able to say to people "you will do this" and mean it. And that just isn't there. You can get it, it's proven you can get it out of the system. There is so many opportunities.

I had a study done—it was informal so I didn't report it—by a consulting company. I was actually working on the thing and they saw a billion easy dollars based on their benchmarks in the private sector. And the system gives you the information to get it. But you just don't plug in the numbers and say, okay, it's done.

And I'm also not naive enough to think that you're going to get a billion dollars back in front of you, Mr. Everett. That money will be saved and turned to other purposes. But as a former chief of staff, I can tell you that if we could free up a billion dollars and just distribute it to the other veterans, that would be satisfactory.

Mr. EVERETT. You're a physician who practiced for many years in a VA hospital and you are well-versed in information technology as well. Would you comment on the GAO and IG testimony you've read and heard here regarding the computer security for medical records and information for VHA?

Dr. GREEN. Sir, I cannot say that I'm an expert in the field, and I'm certainly not a hacker, and I'm certainly not as good as a 17-year-old. However, it is my opinion, based on what we've gone through in our project, is that one could hack into the VHA systems and one could get into the source code and one could change the system.

Mr. EVERETT. There's nothing that you have told the subcommittee that we haven't publicly said in subcommittee hearings, including the solutions. The problem is, we talk about solutions within the VA but we never get around to solving the problem. There's always another paper to write, there's always a reorganization. As you put it, it's rearranging the deck chairs on the Titanic and that's pretty much what we've seen so far.

How do we ever convince the VA to solve these problems when they are an entity by themselves without any competition?

Dr. GREEN. You've thrown a very important factor into the particular equation, and that's called competition. You can take the managerial approach that a corporate executive would use, like Jack Welch, who entered a quality program called the Six Sigma program and made billions of dollars to the bottom line very quickly. It took a lot of investment.

But he had competition. He had to stay in the game. Can you create competition? Sure, you can. Is it politically acceptable? I can't answer that question.

Mr. EVERETT. We're losing World War II veterans at a rate of over 1,000 a day. And these are elderly veterans who, in many cases, are far away from health care—veterans' health care. We

have recently passed a bill in the House and I hope it will pass in the Senate that would allow these veterans to get care closer to home.

And we're also putting in the clinics. But I think that one of the answers is something that we have to politically face up to, if there's a will in this Congress to do so. That is to see if we need to expand beyond the current legislation being offered in the House.

And with that, let me thank you for your participation and I'll ask Ms. Brown for her questions.

Ms. BROWN. Thank you, Mr. Chairman. I just want to thank Mr. Green and I want to hold my time for the next panel.

Mr. EVERETT. Certainly. And Dr. Green, we will have additional questions for the record.

Dr. GREEN. I'd like to give you two observations in the terms of the cartoons that may speak to the point, Mr. Chairman.

Mr. EVERETT. Certainly. Without objection, they'll be entered into the record.

Mr. Bob Bubniak, the Acting Principal Deputy Assistant Secretary for Information and Technology at the VA. Sir, I would ask you to introduce your panel. At that point, please proceed and hold your testimony to 5 minutes, if you would. Your complete testimony, will be made a part of the official record.

Also let me say, at the beginning of our proceedings, this Chair has never made personal attacks on any VA employee, nor will he ever do so. As a matter of fact, some may recall, I halted the testimony of a Member of Congress from doing so when they appeared before the committee. So I want you to know that while we'll have some tough questions here, they are certainly not directed at either of you personally.

And I am very disappointed that you were sent down here without than having top management, who can make these decisions, who chose to stay back in their offices and would not appear before this subcommittee. And I will say, again, had I known that in time, I would have subpoenaed those gentlemen to ensure their appearance before this subcommittee.

If you will, please proceed, and we will hear your statement.

STATEMENT OF ROBERT P. BUBNIAK, ACTING PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY ADAIR MARTINEZ, CHIEF INFORMATION OFFICER, VETERANS' BENEFITS ADMINISTRATION; AND GARY CHRISTOPHERSON, CHIEF INFORMATION OFFICER, VETERANS HEALTH ADMINISTRATION

Mr. BUBNIAK. First of all, I'd like to introduce Gary Christopherson, who's the CIO for the Veterans Health Administration. Adair Martinez will be joining us shortly. She's the CIO for Veterans' Benefits Administration.

Good morning, Mr. Chairman and Ranking Member of the Subcommittee. I am pleased to testify before you today to discuss the Department of Veterans Affairs information technology programs. On June 1, 2000, the principal deputy assistant secretary retired and on June 2, 2000, Secretary Togo D. West, Jr., appointed me

Acting Principal Deputy Assistant Secretary for Information Technology and Acting Chief Information Officer.

Until the appointment process for a new assistant secretary is completed, the acting principal deputy assistant secretary is the acting CIO. Ms. Adair Martinez, who will be joining us shortly, joined VA on December 13, 1999, as the CIO of the Veterans' Benefits Administration. And Mr. Gary Christopherson joined VA on July 31, 2000, as the CIO of the Veterans Health Administration.

Because we're all relatively new to our positions and to the Department, we have been working closely to address a wide array of problems known to this subcommittee and to look into the future to ensure we can develop a shared One VA vision. In support of One VA, we remain committed to the full implementation of a Department-wide information technology architecture and we are now coordinating business process re-engineering and a Department-wide architecture with VHA and VBA partnership.

We are, together, developing an information technology architecture (ITA) and a technical reference model and standards profile was completed in May 1999. We are now developing the enterprise architecture to complete the ITA. To that end, in August 2000, VA provided a white paper which described the plan and steps to be taken as well as a statement of work for contractor support and a milestone chart with estimated completion dates.

I will continue to work with the CIOs of VBA and VHA to ensure that we have a shared outcome responsive to all and we are addressing our efforts from a corporate perspective.

In regard to security, I am aggressively investigating the establishment of a senior executive service security officer to take the lead in implementing an ubiquitous security program for the entire Department. The capital investment proposal was approved and will be funded for $85 million, with the first tranche of $17.575 million available in FY 2001.

We are sponsoring, for the first time, a Department-wide security conference to address crosscutting issues.

We recognize that severe security problems exist, and I've already taken steps to address known-vulnerabilities, but we want to ensure that we have an overarching approach to security and work proactively to effect safeguards.

We recognize Congressman Horn's grade of D and are committed to improvement. To that end, all our security efforts adhere to the risk management framework and best practices espoused by the General Accounting Office.

First, earlier this year, we had a contractor perform an objective and independent Department-wide risk assessment—the first ever in VA. The resulting risk management plan puts all our GAO, OIG and penetration test findings into an organized framework that we base our program budget plan on, both in direction and investment value.

The second step of the GAO framework is to implement all necessary policies and controls. We have issued a directive that prescribes employees' personal use of government equipment technology; issued a policy that raised the bar on password management and prohibited un-secure dial-in connections; issued a direc-

tive that sets minimum security requirements for our connections to the Internet.

We will, by the end of the month, award a half million dollar contract for the development of a formal program to certify and credit our computer systems. We are already running a contract that will provide security design guidance applicable to Internet self-service systems used by veterans and their families.

Early this next fiscal year, we will launch preliminary contracts related to intrusion detection, improved fire walls, simplified sign-on technologies, a better anti-virus regime, and public key infrastructure. The third step of GAO's framework, requires aggressive awareness in training programs to make sure the workforce understands its security obligation and that our security officers are equipped with necessary skills.

Already, we have beamed by live satellite broadcasts, into every VA facility, a 2-hour panel session aimed at .managementteams; established a full-feature Web site to post information and tools related to our program; published a Web-based workforce awareness curriculum; and by the end of this month, will award a quarter million dollar contract for Web-based security officer training media.

The fourth and final step of GAO's framework requires that we monitor and evaluate our program. In just the last year, we established an excellent contracted critical incident response operation which is VA's nerve center for rapid and coordinated action against virus outbreaks, network attacks, e-mail storms, or other kinds of security incidents. We're also addressing the issue of ensuring veterans' confidence in the security and privacy of their personal data on the Internet.

As you know, VA held 5 one-day regional conferences during 1999 and early 2000. The conferences brought together senior leadership, middle managers, first line employees, union representatives, and veterans' service organization members to support institutionalization of a true One VA culture. The idea was advocated by then Deputy Secretary Gober, to ensure seamless service to our customers.

We continue to work with the administrations and staff offices on these initiatives. I recognize that we have miles to go before we meet our One VA objective. But I have, with the support of my colleagues, Mr. Christopherson and Ms. Martinez, brought new focus on this noble goal.

This completes my opening statement. And are there any questions?

[The prepared statement of Mr. Bubniak appears on p. 68.]

Mr. EVERETT. First of all, for the record, I believe Chairman Horn's grade that he gave VA should be an F or anything lower. It ought to be something lower. I believe VA, on a self-evaluation, first gave themselves an 85 on that. Is that not true?

Mr. BUBNIAK. This is what I understand, sir, yes.

Mr. EVERETT. And that was knocked down by GAO another 20 points, and then Chairman Horn came out with a D. Let me ask you, VBA failed penetration testing and didn't know the intrusion had occurred. And according to the GAO and the IG testimony,

similar computer security vulnerabilities have existed in the VA health care system.

How can you reassure veterans and their families that hackers or unauthorized VA have not intruded into their personal, financial, and medical information maintained by the VA?

Mr. BUBNIAK. Sir, what I can tell you is we are taking active action to——

Mr. EVERETT. That's not what I asked you. Please answer the question directly. How can you assure VA veterans——

Mr. BUBNIAK. I cannot, sir.

Mr. EVERETT. Thank you.

Mr. BUBNIAK. I cannot do so.

Mr. EVERETT. I didn't really think you could. And I'm sorry to say that Chairman Horn was too generous, as I've pointed out earlier. I'm really outraged by the VA's inexcusable failure to safeguard the privacy of the confidential, personal information it maintains in its computers, including medical information. I think when they hear about this, many veterans and their families will be outraged.

I have to tell you, very frankly, I appreciate where you are and where you're coming from and the fact that you just arrived on the scene with this, so to speak. But I also can't tell you how many times I've been through this same thing, you know, where somebody is in charge of a problem and they move out of the way and somebody else comes in and they say, we're getting this thing corrected.

And in 6 years in dealing with computer modernization at the VA, I have seen almost no movement. We started trying to do something about the outrageous delay in the processing of initial claims at the VA back in 1995. Back in 1995, I was Chairman of the Compensation and Pensions Subcommittee. They were up around 200 days to do a claim. Well, my goal was to get them down around 65, the same as Social Security. I think VA wanted to get it to about 130, somewhere in there, which I found unacceptable.

We were led to believe in 1997 that steady progress was being made on that. And then, in a hearing that we held just a couple of months ago, we found out that this committee and this Congress had been mislead by the VA and that those actual numbers were not down in the 100s—130 or somewhere in there—that the VA had claimed, but were, indeed, up around 200.

And there were a quarter of a million veterans awaiting action on their claims. So forgive me for appearing to be skeptical of what you're saying. But I just have to tell you, we've heard this over and over again. And this is not personally directed at you.

As I said earlier, I am angry that the Department heads and the leadership ought to be sitting where you're sitting, that they're not here. They didn't have the courage to come here, frankly. And that's exactly the way I see it. All that we have heard concerning how veterans have been mistreated at West LA Hospital, subject to unauthorized invasion of their bodies, many cases that we've found of sexual harassment—I don't know where the outrage is in this country. Veterans ought to be up on their hind legs hollering at the VA to straighten themself out, they really should.

The VA had the specific information, the time, and the resources it need to fix the problems, and didn't do it. The VA had more than enough time, since it was informed about the security problems, to address the most serious vulnerabilities. They have had more time, and as we understand it, there's been some plugging done. But there's still, you know, the possibility of penetration that exists.

Has the VA ever informed the Veterans' Committee that it did not have the resources or funding it needed for computer security?

Mr. BUBNIAK. To my knowledge, no, sir.

Mr. EVERETT. The answer is no. Well, the level of VA funding that has been appropriated by Congress in the last 10 years, you probably are aware of this for IT, has been way over $5 billion. And as Mr. Dirksen said at one time, you know, a few billion here and a few billion there, and pretty soon you're talking about some real money. We're talking about some real money, and frankly, maybe we could find someone else that could do this for the VA because they, obviously, are not doing it for themselves.

Now the contracts that you're going to let will be outside contracts by people that you're absolutely sure will be able to solve these penetration problems. The VA is not going to try to do this themselves, are they?

Mr. BUBNIAK. No, sir. We will try and get expert assistance in making this happen.

Mr. EVERETT. Okay, thank you very much. Ms. Brown.

Ms. BROWN. Thank you, Mr. Chairman. Let me just say that this is a very serious and grave situation. The Chairman mentioned $5 billion. You know, if we can't clear up the problems with the veterans, which is the second largest budget that we fund, to my understanding, in the entire Congress.

Mr. EVERETT. Second largest organization.

Ms. BROWN. Organization?

Mr. EVERETT. Yes, ma'am.

Ms. BROWN. What about the percentage of the budget?

Mr. EVERETT. The Defense Department is first.

Ms. BROWN. First, and VA is second?

Mr. EVERETT. VA, as far as personnel is concerned.

Ms. BROWN. What about money?

Mr. EVERETT. No, it's not. About fourth or fifth.

Ms. BROWN. About fourth or fifth. But I'm the last person that would say that if we don't see major improvements, the VA could be outsourced, it could be dismantled. It is so important that we get a handle on this situation. And I want to give you an opportunity to—I have some specific questions but to tell me how we can get the VA like we did Y2K? I mean, it's just got to happen.

And I asked the question several times on whether or not we should have a centralized system or decentralized system. But somebody got to be responsible. I mean, it can't be that I just got here today. You know, we got to have a system in place that delivers services for our veterans. And I would just like a response, and then, I'll have specific questions. I want to give you the opportunity to tell me what we can do to make this system work for our veterans.

Mr. BUBNIAK. I can tell you, since my arrival on June the 2nd in the position, I've worked assiduously with my counterparts here

to address cross-cutting issues. I can't comment, Ms. Brown, on what happened previously. All I can do is address those issues that are facing me today and exercise good judgment in bringing solutions to the table.

I'm trying to learn from past mistakes and past errors and trying to do the right thing. I think the only way we're going to achieve this is, as you point out so correctly, with the leadership from the top. And I note the Acting Secretary is expressing a great deal of interest these days in these issues that we are addressed today.

And I certainly can tell you that my colleagues here to my right and to my left and I share your concern and are doing the best we can to address those issues.

Mr. CHRISTOPHERSON. If I may follow through in support of what Bob has said. As the newest one on the block, which is about a month and a half into the office here, I came here for one reason, and I think that's what Bob and I and Adair are really trying to do is to find a better way to take care of veterans.

We understand well there's a history. We may not have been part of that but we can't escape it. We have to live with that and go beyond there. To get back to the chairman's comment about key issues. How do we justify both expenditures in the past and expenditures in the future? To do a better job, the answer is absolutely we have to change that.

I think what you've seen happening, especially in the last several weeks here within VA, is a very different perspective on how we work together. The three CIOs, in particular, I think, are setting a very different tone about how we work; if you look, for example, at your concern, for example, on a number of key issues. For example, for the up front part of Web, we are working together now as a team to make sure that's a One VA approach to Web.

That also is true of the benefits and health parts and the cemetery parts of the equation. Architecture is the same thing. Common architecture, wherever we need common architecture, strengthens the systems in addition as well to make sure we have an integrated system that works from front to back.

Security, the same perspective, which is, we need a one VA security. Each facility will have its own but the end game is, you have to have a system around the outside edges that protects it, protects the veterans wherever their record may lie, whatever they may be doing in terms of care. We're looking at other issues around One VA registration, eligibility, enrollment-type system. Again, a One VA type of approach.

This is something we all believe will help us all do our jobs a lot better and it will make this a much better system for the veteran. And, again, the activities in the last 2 or 3 weeks, already have indicated we've made significant progress in trying to move those agendas forward aggressively.

But as I was indicating—talking to staff during the break, the proof is going to be in the performance. We've got to show we can deliver. The words are good, but they need to move us in the right direction and go further than in the past.

Mr. EVERETT. Thank you, sir.

Ms. BROWN. I have some questions to ask about the VETSNET. What is the current status of it? I'm particularly concerned about

the St. Pete regional office. Approximately 10 handpicked, the "vanilla cases." I don't know what that means. What's "vanilla?" Explain. What is that? I don't understand it. Explain the pilot to me.

Mr. BUBNIAK. Go ahead.

Ms. MARTINEZ. Oh, I know. You're talking about the 10 veterans we plan to pay in January.

Ms. BROWN. "Handpicked vanilla."

Ms. MARTINEZ. Let me start with the VETSNET progress. I came in just before Year 2000 in December. We issued the checks to veterans before January 1, 2000, to guarantee payment. So, by January we were running in the year 2000 environment. Then, in February, we had to worry about leap year. And, in March, we thought we were pretty much through everything.

During this time, I was learning about VA and, of course, learning about VETSNET. I went down to St. Petersburg and started doing work on VETSNET. I've gone over a lot of this with GAO and that's how you heard about the pilot, which we're really calling a "test" because we want to show you that we can pay veterans with the new VETSNET system.

The conversion is very complicated. There are 3.2 million veterans; records that we have to convert and we want to be careful about how we do it. I can talk about this for hours. VETSNET is many different systems and processes put together. You have the claims establishment and you have what we are calling "Map D", which is how you develop a case. I think case management's very important.

The next step is the rating, and we have just issued the rating system which went into production in August. That's the first real application out of the VETSNET C&P system. Then, you have the award and then you have the payment system. We want to show how all of these parts are going to work together.

The 10 vanilla VETSNET files are ones with original claims—which we consider simple cases to process. Since payments can be very complicated, we wanted to start, with simple cases and show that the payment works end-to-end. You know, more programming is needed for every single complicated claim.

Have I answered your question?

Ms. BROWN. Yes.

Ms. MARTINEZ. Okay. The other thing I wanted to add is that we were supposed to come up and brief the staff in August and we're putting our plan and our budgeting figures together right now for what I call VETSNET implementation, which includes having the application done. Then, you have the conversion. And, what you've all been calling information exchange, I call synchronization. You have to be sure that the systems are going to be synchronized.

We have batch, we have interfaces. There are a lot of projects to make VETSNET really happen that are outside of what we call the application. We would like to come up and have a chance to brief the staff in more detail about this.

Ms. BROWN. And that would be great, and I'll submit these questions pertaining to the system. But I guess we need to go back to the initial problem and the grading system of D or F.

Ms. MARTINEZ. Okay.

Ms. BROWN. What is it that the VA is going to do to improve this system?

Mr. BUBNIAK. One of the things that I've taken action to do is to establish—to get the groundwork going. And I've identified the senior executive service position already and we're now aggressively working on the job description to put a senior executive service level security officer in place. This individual will have wide authority to look at VBA, to look at the HA, and to develop a staff that he has already or she may have, depending on who is selected, to make the effort happen.

There are a few other agencies that do have a chief security officer, and we're looking at the way they do it. We have a very unusual set of circumstances, as you well know, at VA because we're not as concerned about top secret and secret and special compartmentalized information as, perhaps, DOD agencies are.

But we're very, very much concerned about veterans' records and their privacy issues. And we take this so seriously that I genuinely feel that having a chief security officer is the only way we're going to fix this. We have to fix this; we have to fully identify the problems; we have to take to heart the penetration tests that we've heard about; we have to fix what we've been told is bad. And as long as I'm in the position, I fully intend to do that.

Ms. BROWN. Can I have an additional minute, Mr. Chairman?

Mr. EVERETT. You certainly may.

Ms. BROWN. Okay. The other part is the taxpayers' dollars. Can anyone go into this today and write checks or invade the system? I mean, have we taken corrective action? They're monitoring the system as we speak. I mean, I've seen how 17-year-old hackers can—what steps have we put in place to ensure that we're not being attacked as we speak?

Ms. MARTINEZ. VBA is the one that had the penetration testing performed.

Ms. BROWN. The one that we know of.

Ms. MARTINEZ. Right. We had the penetration testing. I did a review of the actions. There were 48 recommendations and we have agreed with and taken action on 38 of them. The other thing is that, last year with the support of the Department, we got money to do a security pilot program that brought intrusion software; lots of security software.

So we are finding that we are defeating intrusions. We are seeing intrusions come in and we are defeating them. That doesn't mean that we're not missing some of them but that we at least, have a way to start tracking this.

Ms. BROWN. So I don't know as much about these computer systems as others might. But I guess my question is, if you're being attacked, would you know it?

Ms. MARTINEZ. Yes.

Ms. BROWN. You know today—you would know it today?

Ms. MARTINEZ. We know that the software has rules in it to take certain kinds of attacks. And if that's the way that we're being attacked, we can stop those attacks. That doesn't mean we catch all of these, as the IG said earlier. You know, no system is totally bullet-proof but we're putting patches on all the time. At least, we're starting to see intrusions and stopping them.

Ms. BROWN. All right. Thank you.

Mr. EVERETT. Are you characterizing what's been done as saying that no hacker can get into the VA right now or that you would know if any hacker tried in the entire system? You can't make that statement.

Ms. MARTINEZ. No, I cannot make that statement. I'm saying that, at least, now we have—we only started this pilot after the 2000 rollover. So this was after the penetration testing and it took us about 6 months to install the software. So it has really only been, probably, the spring/summer that we've even been able to see the results of this.

Mr. EVERETT. You were told in September 1990—the Department told GAO in September 1998 they were going to do that, and they've only recently done it.

Ms. MARTINEZ. We got money from the one VA fund to do a pilot and we started it with 1999 funds, and so we started it in 2000. I started it.

Mr. EVERETT. You couldn't know prior to your time. I understand.

Ms. MARTINEZ. Yes.

Mr. EVERETT. Well, let me also point out that I must reject your characterization. I know how difficult a job this was. This has been going on for 10 years now and only in January of 2001 will there be a pre-selected, sanitized test of the VETSNET system. So, you know, to say that it's a difficult job to integrate all that after it's been going on for 10 years, I can't accept that. I can't think of any corporation in this country that would have taken 10 years to solve this problem.

Having said that, let me finally just say to you, can you guarantee this subcommittee and the veterans of this country and the taxpayers of this country that the VA computer systems have not been violated to a point where medical records or private records of veterans have been taken and/or money been misappropriated through either internal hackers or external hackers? Can you give me that assurance?

Mr. BUBNIAK. Are you directing the question to me, sir?

Mr. EVERETT. Yes, sir.

Mr. BUBNIAK. No, sir, I cannot give you that assurance.

Mr. EVERETT. Okay. Thank you, sir. We'll have, as Ms. Brown indicated, additional questions that we would ask you to respond to in writing. I'd like to make a brief observation before I close the final IT oversight of the 106th Congress.

And for this hearing, the VA did not send a single top leader or manager or anyone else with the authority to actually make decisions about information technology. I hope everybody paid attention to Dr. Green's comments.

I'm fully aware of the Acting Secretary's interest in this. It was the Acting Secretary who took the lead and showed the leadership in solving Y2K problem. And to that, I give him great credit and I have admiration for what he's been able to do. But he's not been there very long.

And there has simply been an incredible lack of leadership within the VA. The VA's IT programs have been chaotic for a long time because of weak leadership and management. There's been some

small improvement, but the Department has a long, long way to go. I think the VA has had its chance and in the next Congress, the committees of jurisdiction should actively intervene in these programs to straighten them out.

It's time to move beyond oversight. This is an expression of "no confidence," and I do not know how to make that message any clearer. Further, let me point out that my ranking member, Ms. Brown, and I probably don't vote an awful lot alike. But if you will see what we have done on this Subcommittee from day one, we have acted in what we feel like is the best interest of the veterans of this country and the taxpayers of this country and I echo what she says.

It doesn't matter which one of us is sitting in this chair next year, we're going to do everything we can do to see that we get beyond people not taking responsibility and that these problems are solved. I think the future of the VA, as Ms. Brown has indicated also, the very future of the VA hinges on doing something about the culture problem which we have talked about, time and time again; Dr. Green has mentioned it also.

I don't know how to get that message across any stronger. But the VA is destroying itself, if it does not take some sort of action to improve.

The hearing is adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

APPENDIX

THE UNDER SECRETARY OF VETERANS AFFAIRS FOR BENEFITS
WASHINGTON, D.C. 20420

AUG 15 2000

The Honorable Terry Everett
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Everett:

I am responding to your letter of July 20, 2000, which addressed several program integrity issues involved in the processing of disability claims.

I will be pleased to meet with you on October 4, 2000, as you requested, to discuss the actions that we have taken to strengthen our internal controls over the past several years. However, because of the seriousness of the issues and the questions you raise, I did not want to delay responding until our meeting.

Your letter indicates that you were recently advised that the Veterans Benefits Administration's (VBA) claims processing reports were, at best, misrepresented. While it is true that VBA had a data integrity problem when I assumed the position of Under Secretary for Benefits, one of my first actions was to appoint one of our Senior Executives as chairman of a task force that was given the responsibility to fix the data integrity problem. The task force was also charged with the task of improving the overall quality and availability of our data. The task force's plan was documented in the Roadmap to Excellence and resulted in the establishment of the Data Management Office.

One of the first actions taken by the data task force, in cooperation with the Compensation and Pension (C&P) Service, was to use our data warehouse facility to conduct a series of computer runs to identify questionable transactions associated with the processing of original and reopened claims in the Benefits Delivery Network (BDN). These transactions were sorted and sent to each of the regional offices with a request for an explanation as to why the actions were taken. In several instances, the Office of Field Operations (OFO) met with regional office directors and service center staff to discuss the cases in question. As a result of these ongoing computer runs and their subsequent reviews by the C&P Service and OFO, we believe that our current timeliness data reflects actual processing time in the field. In my testimony before the Subcommittee on Benefits of the House Committee on Veterans' Affairs on March 26, 1998, I stated that the average time to process an original compensation claim increased

2.

The Honorable Terry Everett

from 133 days in October 1997 to 155 days at the time of the hearing. I feel that increase was due, in part, to the elimination of data manipulation.

Your letter states the OIG uncovered two instances of employee fraud during the past year. We assume those to be the cases that the OIG investigated at VBA's request during the past year. The most serious of those two cases, which occurred at the St. Petersburg Regional Office, was actually discovered by regional office management. That case was turned over to the IG for criminal investigation and prosecution by the U.S. Attorney. The employee was arrested in January 1999. The second case involved a claim that was processed by an employee over ten years ago. It was discovered as a result of an external criminal investigation.

Within the last year, VBA launched several initiatives designed to strengthen program integrity in each of the business lines in the field. We have established a Program Integrity Office that reports directly to the Deputy Under Secretary for Management. This new office is responsible for coordinating the program integrity activities of each business line as well as the support services. A program team has been formed by each business line and support service to review the current business processes to identify existing internal controls and any vulnerable areas that may require new controls. A team was also designated by OFO to review the effectiveness of internal controls that regional offices are expected to execute. The Program Integrity teams have also been tasked with identifying any systemic changes necessary to strengthen VBA's internal controls, especially as we look to the future when we will rely more heavily on external organizations to process significant portions of the front-end of the business – particularly in the Loan Guaranty and Education programs.

In order to assist the members of these Program Integrity teams in the identification of issues and recommended solutions, they received training on internal fraud detection during a two-week session conducted by the U.S. Department of Agriculture Graduate School and by VA's OIG staff.

The chairman of the C&P Program Integrity team, along with the staff director of the Program Integrity Office, also met with several corporations that developed data mining software and techniques for identifying anomalies in large transaction-based systems like the BDN. These companies, which include the IIT Research Institute, Federal Data Corporation, Computer Sciences Corporation and SRA, have worked with companies and organizations, including the Departments of Defense, Justice and Health and Human Services, in developing fraud detection programs. We are in the process of issuing a

statement of work that will allow these data mining companies to demonstrate their products when applied to actual BDN data.

Staff also met with the management team at the Veterans Health Administration's (VHA) Denver facility responsible for processing CHAMPVA health benefit claims to review the fraud protections they presently utilize. More recently, staff attended the Association of Certified Fraud Examiners' 11th Annual Fraud Conference in New York. This conference focused on all aspects of fraud investigation, included participants from both the public and private sectors, and provided small group training covering over 40 topical areas of interest.

In addition to establishing the Program Integrity Office, we have also formed the Security Infrastructure Protection Office under VBA's Chief Information Officer. This office is responsible for system security issues that include the policy and procedures associated with granting and controlling access to our data systems. These controls include password and access restrictions that ensure the separation of duties – a basic internal control principle. They are also responsible for "intrusion protection" from unauthorized external users, which has become increasingly important with the rapid expansion of the Internet and systems-architecture associated with the decentralized server-based systems that are so prevalent today.

Experience in the private and public sectors demonstrates that it is virtually impossible to preclude every instance of employee and beneficiary fraud in systems that support the type of claims and recurring payment processing business in which VBA is engaged. We believe the experts in the Inspector General community would readily concur with that statement. However, we recognize, like the IG community, that the risk of fraudulent and inappropriate payments can be greatly reduced when a comprehensive system of internal controls is consistently applied to a claims process like ours. The objectives of data integrity and program integrity actions we have taken over the past two and one-half years have been to continuously enhance and improve the effectiveness of our data and internal control systems.

I look forward to discussing these issues with you on October 4, 2000.

Sincerely,

Joseph Thompson

U.S. House of Representatives

COMMITTEE ON VETERANS' AFFAIRS

BOB STUMP
CHAIRMAN

ONE HUNDRED SIXTH CONGRESS

335 CANNON HOUSE OFFICE BUILDING

WASHINGTON, DC 20515

http://veterans.house.gov

July 20, 2000

Honorable Joseph Thompson
Under Secretary for Benefits
Department of Veterans Affairs
Washington, DC 20420

Dear Mr. Thompson:

I write to you about my concern regarding the integrity of the VBA claims processing data and VBA's exposure to fraudulent disability claims.

Recently I became aware that the claims processing data that had been reported by VBA relating to timeliness, was at best misrepresented. Furthermore, during the past year, the Inspector General has uncovered several instances where VA employees established fraudulent disability compensation claims whereby over one million dollars was stolen from American taxpayers.

There are many private companies that also have similar concerns and have successfully developed internal controls and information technology to prevent fraud and to accurately track processing of claims. Please contact and schedule meetings with private sector companies engaged in similar lines of business, i.e. the processing and paying of claims, to learn what technology and procedures are being used to protect against fraud and track the processing of claims.

Please be prepared to discuss your findings with me on October 4, 2000 at 2:00 pm. If you have any questions regarding this matter, please contact Alicemary Leach at 225-3569.

Sincerely,

Terry Everett

TERRY EVERETT
Chairman
Subcommittee on Oversight and Investigations

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
Thursday,
September 21, 2000

VA INFORMATION TECHNOLOGY

Progress Continues Although Vulnerabilities Remain

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-321

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on the Department of Veterans Affairs' (VA) information technology (IT) program. As requested, my testimony today will focus on the status of VA's efforts to

- improve its process for selecting, controlling, and evaluating IT investments;
- fill the chief information officer (CIO) position;
- develop an overall strategy for reengineering its business processes;
- complete a departmentwide integrated systems architecture;
- track its IT expenditures;
- implement the Veterans Health Administration's (VHA) Decision Support System and the Veterans Benefits Administration's (VBA) compensation and pension replacement project; and
- improve the department's computer security.

Taken together, these seven areas represent critically important challenges that VA needs to fully address in its information technology journey.

Results in Brief

Overall, VA's IT investment decision-making process has improved, and it has started to implement recommendations we enumerated in May[1] and August[2] of this year. Further, VA is obtaining a full-time CIO now that the Administration has identified a candidate for the position. However, the department no longer plans to develop an overall strategy for reengineering its business processes to effectively function as "One VA," nor, has it defined the integrated IT architecture needed to efficiently acquire and utilize information systems across VA. In addition, VA lacks a uniform mechanism that readily tracks IT expenditures. Instead, VA's different offices use various mechanisms for tracking IT expenditures.

VHA's Decision Support System (DSS) and VBA's compensation and pension replacement project continue to face challenges. As demonstrated in a survey to all Veterans Integrated Service Networks (VISN)[3] and medical centers directors, DSS is not being fully utilized. In addition, while VBA plans to pilot test portions of its compensation and pension replacement system in January 2001, other key issues need to be addressed before the system can be fully implemented. For example, VBA does not have a plan or schedule for converting data from the old system to the new system and exchanging data between the new system and other systems.

Finally, regarding computer security, VA has begun to address weaknesses identified by us and its Office of Inspector General. But until it develops

[1] *Information Technology: Update on VA Actions to Implement Critical Reforms* (GAO/T-AIMD-00-74, May 11, 2000).

[2] *Information Technology: VA Actions Needed to Implement Critical Reforms* (GAO/AIMD-00-226, August 16, 2000).

[3] VHA is comprised of 22 VISNs, which are regional organizations encompassing medical centers, nursing homes, and domiciliaries.

and implements a comprehensive, coordinated security management program, VA will have limited assurance that financial information and sensitive medical records are adequately protected from misuse, unauthorized disclosure, and/or destruction.

Background

The department's vision of "One VA" was articulated to assist it in carrying out its mission of providing benefits and other services to veterans and dependents. It stems from the recognition that veterans think of VA as a single entity, but often encounter a confusing, bureaucratic maze of uncoordinated programs—such as those handling benefits, health care, and burials—that puts them through repetitive and frustrating administrative procedures and delays. According to the department, the "One VA" vision describes how it will use IT in versatile new ways to improve services and enable VA employees to help customers more quickly and effectively—in short, to really become "One VA."

To help carry out its activities, VA plans to spend about $1.4 billion of its total fiscal year 2001 budget of about $48 billion on various IT initiatives. Of this $1.4 billion, about $763 million, $80 million, and $400,000, respectively, are intended for VHA, VBA, and the National Cemetery Administration (NCA). The remaining $589 million is for VA-wide IT initiatives in the financial management, human resources, infrastructure, security, architecture, and planning areas.

The Clinger-Cohen Act and other related legislative reforms provide guidance on how agencies should plan, manage, and acquire IT as part of their overall information resources management responsibilities. These reforms require agencies to (1) appoint CIOs responsible for providing leadership in acquiring and managing IT resources, (2) perform business process reengineering prior to acquiring new IT, and (3) complete an integrated architecture to guide and constrain future investments.

VA's IT Investment Decision-making Has Improved

The Clinger-Cohen Act requires agency heads to implement an approach for maximizing the value and assessing and managing the risks of IT investments. It stipulates that this approach should be integrated with the agency's budget, financial, and program management processes. As detailed in our investment guide,[4] an IT investment process is an integrated approach that provides for disciplined, data-driven identification, selection, control, life-cycle management, and evaluation of IT investments.

In May 2000, we testified before this Subcommittee that VA had improved its processes for selecting, monitoring, and managing Capital Investment Board-level projects.[5] In addition, VA had improved its in-process and post implementation reviews. However, as we testified, the in-process reviews may still not have been timely and lessons learned from post implementation reviews were provided only to the sponsoring VA organizations, and not to decisionmakers, such as the investment panel members, who could also benefit from them. Finally, the capital investment process used for projects below the Capital Investment Board-level was not as structured, and guidance for managing those projects was not complete.

[4] *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making* (GAO/AIMD-10.1.13, February 1997).

[5] Capital Investment Board projects are those that exceed specific dollar thresholds or that are seen as high risk or high visibility. The dollar thresholds for VHA, VBA, NCA, and staff offices are acquisition costs of $10 million, $2 million, $1 million, and $1 million, respectively, and/or life-cycle costs of $30 million, $6 million, $3 million, and $3 million, respectively.

To address these issues, we testified that VA needed to (1) establish and monitor deadlines for completing in-process reviews, (2) provide decisionmakers with information on lessons learned from post implementation reviews, and (3) develop and implement guidance to better manage IT projects below the Capital Investment Board threshold.[6] Last month we recommended that the Acting Secretary of Veterans Affairs implement these actions to improve VA's IT investment decision-making process.[7] VA concurred with these recommendations, and stated that

- the in-process review plans will include completion dates,
- post implementation review findings, such as lessons learned, will be provided to investment panel members, and
- the *VA Information Technology Capital Investment Guide*, which was printed and distributed to VA's agencies earlier this month, provides guidance on processes for selecting, controlling, and evaluating IT investments and procurements below the Capital Investment Board threshold.

History and Current Status of Effort to Appoint a Chief Information Officer

The Clinger-Cohen Act directs the heads of major federal agencies to appoint CIOs to promote improvements in work processes used by the agencies to carry out their programs; implement integrated agencywide information technology architectures; and help establish sound investment review processes to select, control, and evaluate IT spending. To help ensure that these responsibilities are effectively executed, the act requires that the CIO's primary responsibility be related to information management.

In July 1998, we reported that the responsibilities of VA's CIO were not limited to information management.[8] Specifically, the CIO served the department in a variety of top management positions, including assistant secretary for management, chief financial officer, and deputy assistant secretary for budget. We noted that in an agency as decentralized as VA, the CIO was faced with many significant information management responsibilities[9] that constituted a full-time job for any CIO. Accordingly, we recommended that the Secretary of Veterans Affairs appoint a CIO with full-time responsibility for information resources management.

VA concurred with this recommendation. It decided to separate the CIO function from the chief financial officer and established the position of assistant secretary for information and technology to serve as VA's CIO. This executive branch position—assistant secretary for information and technology—has remained unfilled, however, since its creation in 1998. Instead, the principal deputy assistant secretary for information and technology served as VA's acting CIO from July 1998 until he retired on June 1, 2000. The Secretary subsequently designated an acting principal deputy assistant secretary to serve as VA's acting CIO.

[6]GAO/T-AIMD-00-74, May 11, 2000.

[7]GAO/AIMD-00-226, August 16, 2000.

[8]*VA Information Technology: Improvements Needed to Implement Legislative Reforms* (GAO/AIMD-98-154, July 7, 1998).

[9]At the time, these responsibilities included ensuring that (1) VA's systems development projects would not be handicapped by incomplete architectures and (2) a sound information management review process providing systematic, data-driven means of selecting, controlling and evaluating IT projects would be institutionalized.

VA still intends to have a departmentwide CIO. The White House just announced last week that it intends to submit a nominee to the Senate for confirmation as assistant secretary for information and technology and department CIO.

VA Does Not Plan to Develop a Departmentwide Business Process Reengineering Strategy

The Clinger-Cohen Act requires agency heads to analyze the missions of their agencies and, on the basis of the results, revise and improve the agency's mission-related administrative processes before making significant investments in supporting IT. According to our business process reengineering guide,[10] an agency should have an overall business process improvement strategy that provides a means to coordinate and integrate the various reengineering and improvement projects, set priorities, and make appropriate budgetary choices.

We reported in 1998[11] that VA had not analyzed its business processes in terms of implementing its "One VA" vision. We also pointed out that VA did not have a departmentwide business process improvement strategy specifying what reengineering and improvement projects were needed, how they were related, and how they were ranked. At that time, VA concurred with our recommendation to develop such a strategy.

This past May,[12] we testified before this Subcommittee that VA no longer planned to develop such a strategy. According to VA's assistant secretary for policy and planning, the department will, instead, rely on each of its administrations—VBA, VHA, and NCA—to reengineer its own business process. We subsequently recommended to the Acting Secretary of Veterans Affairs that VA reassess its decision to delegate business process reengineering to the individual administrations.[13]

VA did not concur with this recommendation. Specifically, the department stated that the administrations best understand the desired outcomes of their missions and the means to achieve them. It further stated that business process reengineering is a constantly evolving function that is not conducted in a vacuum.

We agree that the individual administrations best understand their own operations and that business process reengineering is an evolving function that does not take place in a vacuum. However, by delegating primary responsibility for reengineering to the individual administrations, each administration is able to pursue its own reengineering initiatives separate and apart from each other, rather than focusing on achieving the "One VA" vision. Accordingly, VA is less likely to achieve this vision until it develops a departmentwide business process reengineering strategy.

VA Has Yet to Develop an Integrated IT 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 and IT goals. Leading organizations both in the private sector and in government use systems architectures to guide

[10] *Business Process Reengineering Assessment Guide* (GAO/AIMD-10.1.15, April 1997).

[11] GAO/AIMD-98-164, July 7, 1998.

[12] GAO/T-AIMD-00-74, May 11, 2000.

[13] GAO/AIMD-00-226, August 16, 2000.

mission-critical systems development and to ensure the appropriate integration of information systems through common standards.[14]

In 1997, VA adopted the National Institute of Standards and Technology (NIST) five-layer model[15] for its departmentwide IT architecture. However, as discussed in our 1998 report,[16] VA and its components had yet to define a departmentwide, integrated IT architecture. Accordingly, we recommended that VA develop a detailed implementation plan with milestones for completing such an architecture. VA concurred with this recommendation.

In May 1999, VA published a departmentwide technical architecture,[17] which included a technical reference model and standards profile. This document described one layer—the technology layer—of the NIST model. VA had not documented the remaining four layers—the logical architecture—showing the business processes, information flows and relationships, applications processing, and data descriptions for the department.

Mr. Chairman, during the Subcommittee's May 11, 2000, hearing, you requested that VA provide the Subcommittee with a plan and milestones for completing the logical portion of its departmentwide IT architecture within 60 days of the hearing. The resulting two-page plan, submitted to the Subcommittee on August 25, provides a high-level discussion of VA's approach for developing a target departmentwide logical architecture and time estimates for various deliverables. According to this plan, the VA administrations are expected to develop logical architectures for their administrations.

To avoid duplicating the efforts of the administrations, VA expects the departmentwide logical architecture to focus on crosscutting issues and interdependencies. VA is obtaining contractor support to develop a detailed plan with milestones and to assist in developing this departmentwide logical architecture. VA expects this architecture to be completed within 6 months of the contract award date. In commenting on a draft of this testimony, VA stated that it expects to have the contract awarded by mid-October.

VA's strategy for developing its logical architecture will not likely result in an integrated departmentwide architecture. In fact, VA acknowledges in its plan that the architectures developed by the administrations will not provide a unified picture of the department's architecture. By allowing each administration to develop its own logical architecture, at least three separate architectures could result. To avoid this, VA needs to reassess its current strategy and work together with VBA and VHA to develop an integrated, departmentwide logical architecture, consistent with the Clinger-Cohen Act. This will help foster achievement of the "One-VA" vision.

[14] *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology—Learning From Leading Organizations* (GAO/AIMD-94-115, May 1994).

[15] 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.

[16] GAO/AIMD-98-154, July 7, 1998.

[17] *VA Technical Architecture: Technical Reference Model and Standards Profile*, May 1999.

VA Lacks a Uniform Mechanism for Tracking IT Expenditures

According to *VA Directive 6000*,[18] VA officials are required to maintain complete and accurate data on all personnel and non-personnel costs associated with IT activities. Further, the *VA Capital Investment Methodology Guide* requires that project managers track expenditures against budget authorizations for IT projects. In addition, according to our IT investment management guide,[19] an important step in the IT investment control process is a disciplined process for regularly tracking each project's expenditures over time. Further, according to our IT investment guide,[20] organizations should have a uniform mechanism such as a management information system for collecting, automating, and processing data on expected versus actual outcomes, including expenditures.

Although required to maintain complete and accurate IT cost data, VA does not consistently track IT expenditures across the department. Instead, the department has delegated the responsibility for tracking expenditures for IT projects to project managers within VA's administrations and offices, leading to different tracking approaches and difficulties in readily identifying the extent of IT costs.

At the administration level, the extent of expenditure tracking varies. For example, VBA tracks IT expenditures centrally for procurements, such as hardware, software, and contract services. However, VBA does not track all regional office personnel costs associated with a project. In contrast to VBA, VHA has a decentralized process for tracking IT expenditures. Specifically, it has given responsibility for tracking more than 80 percent[21] of its IT expenditures to its 22 VISNs. However, VHA does not have a uniform mechanism for tracking IT expenditures across the administration. VHA's new CIO acknowledged the need for a system to track all expenditures associated with IT projects.

Until VA develops a uniform mechanism for tracking IT expenditures, the department will be less likely to make informed decisions on whether to modify, cancel, accelerate, or continue projects. At the same time, VA and its administrations may be unable to provide timely cost and budget IT information to the Congress.

To improve tracking of IT project costs, VA recently initiated several actions. First, it is developing a uniform numbering system for its capital investment projects. This system is expected to generate reports from VA's financial management system showing actual expenditures associated with those projects. However, the department has yet to establish a date for when this system will be implemented. Second, VA has recently issued draft guidance[22] directing the administrations to track actual IT expenditures. The department has not yet established a deadline for finalizing the guidance. Accordingly, the department needs to (1) establish timeframes for finalizing this draft guidance and then monitor its implementation to ensure compliance and (2) establish timeframes for implementing a uniform numbering system for its capital investment projects.

[18] *VA Information Resources Management Framework*, VA Directive 6000, September 17, 1997.

[19] *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (GAO/AIMD-10.1.23, Exposure Draft, May 2000, Version 1).

[20] GAO/AIMD-10.1.13, February 1997.

[21] VHA officials reported that the VISNs are responsible for about $700 million (82.5 percent) of VHA's approximately $867 million IT budget for fiscal year 2000.

[22] *VA Information Technology Capital Investment Guide.*

Challenges Continue for Two IT Projects

I would now like to discuss the status of VA's efforts to develop and implement VHA's Decision Support System and VBA's compensation and pension replacement project. Each is at a different stage of development and implementation, and each continues to pose challenges to VA.

DSS Utilization Continues to Vary, But Action Underway to Encourage Greater Use

VHA's Decision Support System 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. VHA expects to use DSS to (1) prepare budgets for its medical centers, (2) allocate resources based on performance and workload, (3) generate productivity analyses and patient-specific costs, (4) support continual quality improvement initiatives, (5) measure outcomes-based performance and effectiveness of health care delivery processes, and (6) improve efficiency of care processes through the use of clinical practice guidelines.

By the end of October 1998, DSS had been implemented at all VA medical centers. The total VA estimated cost from fiscal year 1994 through fiscal year 1999 to develop and operate DSS was approximately $213 million. As of June 30, 2000, VA calculated that it had spent another $36 million on DSS this fiscal year.

As we testified this past May, DSS was not being fully utilized.[23] Although cost reductions and improved clinical processes had been experienced by some VISNs and medical centers using DSS, none of the ones we contacted used DSS for all of the purposes VHA intended. 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, (2) the need for 2 years of DSS data for budget formulation and resource allocation purposes, and (3) DSS staffing issues, including insufficient staff, staff with inadequate skills, and staff turnover.

The May 2000 responses to two questions asked by VHA's chief network officer also indicate that DSS is not being fully utilized. Specifically, in a March 15, 2000, memorandum sent by VHA's chief network officer to all VISN and medical center directors, he asked for

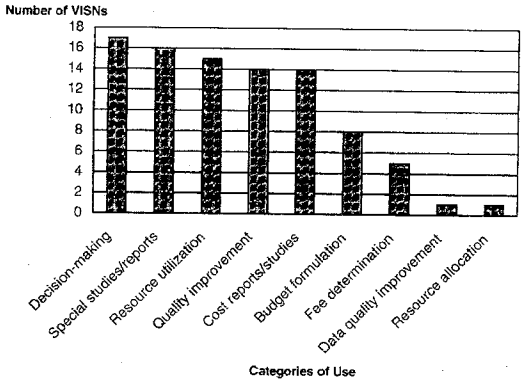
- specific examples describing how the use of DSS had benefited veterans at the VISN and medical centers, and
- explanations for why DSS was not being used, including identification of barriers to its use.

Regarding the first question on DSS usage, 4 of 22 VISNs—VISN 6 (Durham, North Carolina), VISN 8 (Bay Pines, Florida), VISN 20 (Portland, Oregon), and VISN 21 (San Francisco)—did not provide examples of DSS use. Further, VISN 6 and VISN 21 explicitly stated that they do not use DSS at the VISN level because they did not have reliable DSS data at the time from their medical centers.

As illustrated in figure 1, the remaining 18 VISNs provided examples of using special studies/reports and cost studies/reports to make decisions with regard to resource utilization and quality improvement. Of the 18 VISNs, two—VISN 13 (Minneapolis) and VISN 10 (Cincinnati)—cited seven or more categories of DSS use; three VISNs—VISN 14 (Omaha), VISN 18 (Phoenix), and VISN 22 (Long Beach) cited only two categories of use.

[23]GAO/T-AIMD-00-74, May 11, 2000.

Figure 1: Categories of DSS Use by VISNs



Note: Eighteen VISNs provided examples of DSS use. This figure depicts the types of uses, not the quantity.

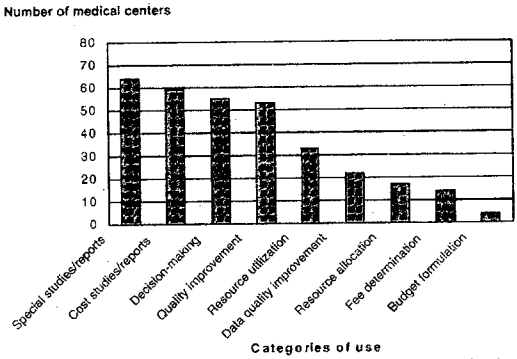
Source: GAO analysis of VISN responses.

Regarding medical centers, 59 of 140 did not provide specific examples of DSS use.[24] Three of the 59 medical centers—Beckley (West Virginia), Anchorage Health Care System, and Boise (Idaho)—explicitly stated that they did not use DSS. Both Anchorage and Boise medical centers cited staffing problems as a reason for not using DSS; Beckley indicated problems with DSS data integrity.

Figure 2 provides a snapshot of the 81 medical centers providing specific examples of DSS use. The Long Beach and Portland (Oregon) medical centers used DSS for the most categories—that is, eight or more. At the same time, three medical centers—Tomah (Wisconsin), St. Louis, and Wichita (Kansas)—cited only one category of use.

[24]These 59 medical centers did not provide specific examples of DSS use in their response to the March 2000 memorandum. This does not necessarily mean that they were not using DSS.

Figure 2: Categories of DSS Use by Medical Centers



Note: Eighty-one medical centers provided examples of DSS use. This figure depicts the types of uses, not the quantity.

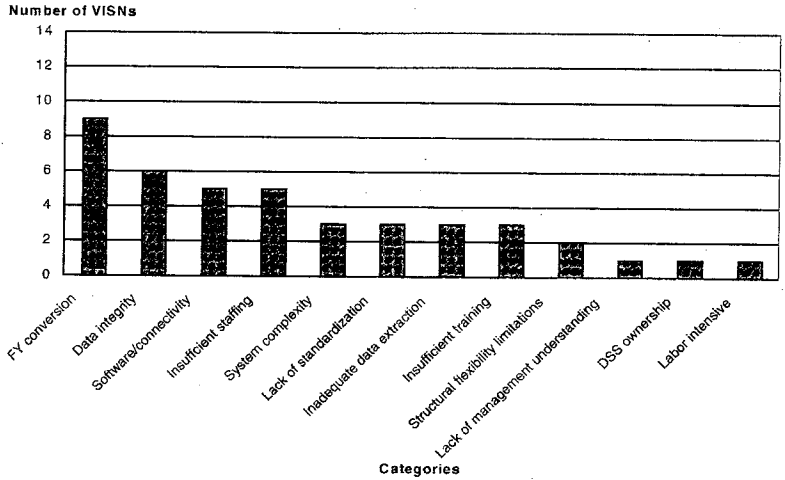
Source: GAO analysis of medical center responses.

Moving to the second question, on barriers, slightly over half of the VISNs—13—identified barriers to using DSS. As illustrated in figure 3, the barrier most often cited was the fiscal year conversion process,[25] followed by data integrity concerns, software/connectivity issues,[26] and staffing issues. Of the 24 medical centers identifying barriers, the fiscal year conversion process was also cited most frequently. For a snapshot of their responses, see figure 4.

[25]The conversion process entails closing out the financial and medical records for the fiscal year and establishing the structure for the new fiscal year. For fiscal year 2000, the process included a new national method to capture vendor-provided home/community health care workload, a new Veterans Health Information Systems and Technology Architecture extract that records mental health psychological testing workload, and the capability for summarizing monthly VA Denver Distribution Center costs by veteran social security number. Because of problems experienced during the fiscal year 2000 conversion process, clinical processing information did not begin until February 29, 2000.

[26]These included problems with computer crashes at the VA Austin Automation Center and problems with software enhancements.

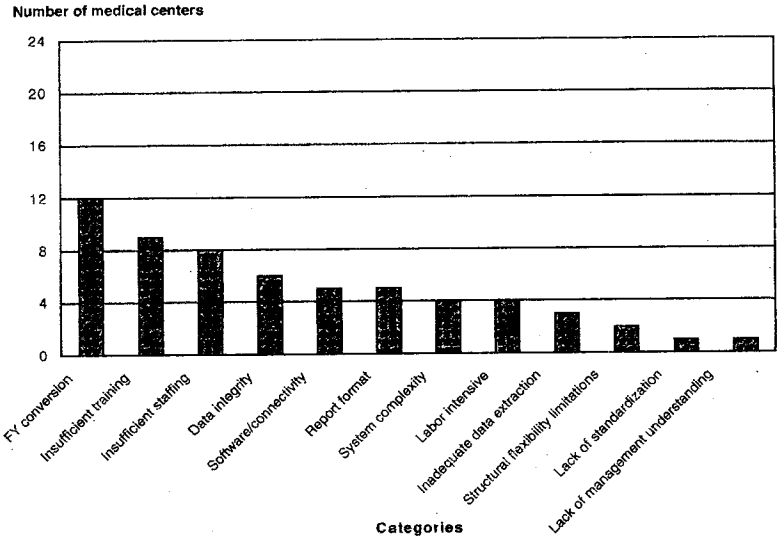
Figure 3: Barriers to using DSS identified by VISNs



Note: Thirteen VISNs identified barriers to using DSS.

Source: GAO analysis of VISN responses.

Figure 4: Barriers to Using DSS Identified by Medical Centers



Note: Twenty-four medical centers identified barriers to using DSS.

Source: GAO analysis of medical center responses.

To address barriers with the fiscal year conversion process, the 2001 fiscal year clinical and financial conversion guidelines were issued on July 27, 2000, and the goal is to begin fiscal year 2001 processing by December 18, 2000.

Initiatives Underway to Encourage Greater Use of DSS

To encourage greater use of DSS, VHA has initiatives underway. For example, in December 1999, the undersecretary for health mandated the use of DSS data rather than data in cost distribution reports for the fiscal year 2002 budget resource allocations. DSS data will also be used as a performance measure in 2001 to determine whether VHA providers are following clinical guidelines for diabetes, according to VHA's Chief Quality and Performance Officer. Finally, the VISN and medical center managers' use of DSS data is expected to be monitored in 2001.

Even with these initiatives, VHA officials within the Office of the Associate CIO for Implementation and Training and the VISNs and medical centers have told us that they are concerned that the recent decision to move the DSS program office from the Office of the CIO to the Office of the Chief Financial Officer may diminish DSS use for clinical purposes.[27] These officials are concerned that this move may shift top management support and commitment more to the financial rather than clinical benefits of using DSS. According to VHA officials, using DSS for clinical purposes is very important and allows VA to improve health care delivery to veterans. For example, as we testified in May,[28] the clinical practice of routinely ordering two units of pre-surgery autologous[29] blood for total knee replacement was changed, based on DSS data, at the Portland (Oregon) VA medical center, resulting in estimated savings of $600+ per case.

The transition plan for moving the DSS program office is currently being drafted and will address the oversight roles and responsibilities for DSS. The plan is expected to be completed by the end of this month.

Compensation and Pension Replacement Project Remains a Challenge

The second of the two projects you asked us to review is VBA's compensation and pension replacement project, one of the major initiatives under the agency's Veterans Service Network (VETSNET) strategy. This 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 others have reported on the problems VBA has encountered in completing this project.[30] We stated that one key reason for the project's delays was the lack of an integrated architecture defining the business processes, information flows and relationships, business requirements, and data descriptions. For example, the project was begun before VBA had fully developed its business requirements. Project delays subsequently resulted due to confusion over the specific requirements to be addressed.

[27]The move to the Office of the Chief Financial Officer is effective October 1, 2000.

[28]GAO/T-AIMD-00-74, May 11, 2000.

[29]Autologous (a patient's own) blood is provided by the patient in advance of surgery.

[30]*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.

Another reason for the project's problems was VBA's immature software development capability. In 1996 we reported that VBA's software development capability was ad hoc and chaotic—the lowest level of software development capability.[31] At this level, VBA could not reliably develop and maintain high-quality software on any major project within cost and schedule constraints. Reviews by VA and by us illustrated that this project had difficulties meeting deadlines and that not all critical systems development areas were addressed. To date, VBA has yet to reach the next, repeatable, level of software development.

The compensation and pension replacement project has missed several key milestones. For example, the project missed its original May 1998 completion date and a revised completion date of December 1998. In 1999, VBA changed its strategy for the compensation and pension replacement project to incorporate several software products previously developed and used at selected VBA regional offices. At that time, VBA did not have a completion date for this project.

Since then, VBA has developed short-term milestones for this project. Specifically, the first product scheduled for implementation under VBA's revised strategy is expected to be rating board automation 2000. This product is expected to be implemented this November and is to assist veterans service representatives in rating benefit claims. Other products under development as part of the compensation and pension replacement project include:

- Modern award processing-development (MAP-D)—which is expected to manage claims development processes, including the collection of data to support the claim, requests for exams to determine degree of injury or disability, and tracking of the claim. MAP-D is also expected to provide direct access to three other software products that address claims development processes.
- Search/participant profile—which is expected to establish the veteran record and collect basic information on the veteran and family.
- Award processing—which is expected to compute the award or payment amount based on the results of the rating process.
- Finance and accounting system—which is expected to develop the actual payment record and handle all accounting functions.

The project manager said that current plans are to complete development and testing of these five products by December 2000. A pilot test of all of the above products except MAP-D is expected to begin in January 2001. In the pilot, 10 new claims are to be processed and payments generated using the new products.

However, before the compensation and pension replacement pilot can be fully implemented, top management in VBA must address several important issues. First, large, complex projects, such as the compensation and pension replacement project should have an approved project management plan and schedule to determine what needs to be done and when, and to use as a means of measuring progress. VBA has yet to develop such a project plan and schedule for developing and implementing this system. Instead, detailed plans and schedules exist only for the next few months.

[31]Software Capability Evaluation: VA's Software Development Process Is Immature (GAO/AIMD-96-90, June 19, 1996) and GAO/T-AIMD-96-103.

Similarly, VBA has yet to address fully other critical systems development areas. The first of these is data conversion. Specifically, data in the existing VBA system will need to be converted to the new system. According to VBA officials, this is the most difficult remaining part of the compensation and pension replacement project. They told us that a data conversion strategy has been drafted and is under review.

In addition, VBA must develop data exchanges to allow the compensation and pension replacement system to share data with other systems. For example, it is critical that changes to veteran information, such as name and address, captured in the compensation and pension replacement system be changed in other VBA systems.

Lastly, VBA is vulnerable to disruptions due to contractor volatility and staffing uncertainties. For example, of the 25 contractors currently involved in the compensation and pension replacement project, over half (13) have been added to the project within the last year. According to VBA officials, they may also experience problems with obtaining in-house staff from its data centers to help develop the compensation and pension replacement system and other VBA projects, such as an effort to consolidate VBA's data center operations from Hines (Illinois) and Philadelphia to Austin, because they compete for some of the same people over the next 2 years. These concerns increase the likelihood that schedule delays and cost overruns may occur.

VBA officials acknowledge the above issues and have informed us that efforts are underway to address them. However, until VBA develops a fully integrated project plan and schedule that incorporates all critical system development areas, challenges and vulnerabilities will remain.

VA Continues to Address Computer Security Challenges

The last area you asked us to discuss is computer security—critical to any organization'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 is at risk of inadvertent or deliberate misuse, fraud, improper disclosure, or destruction—possibly occurring without detection.

Over the past several years we have reported on VA's computer security weaknesses. In September 1998 we reported that computer security weaknesses placed critical VA operations such as financial management, health care delivery, and benefits payments at risk of misuse and disruption.[32] We reported in October 1999 that VA's success in improving computer security largely depended on strong commitment and adequate resources being dedicated to the information security program plan.[33] In May 2000 we testified[34] that VA had still not adequately limited the access granted to authorized users, appropriately segregated incompatible duties among computer personnel, adequately managed user identification and passwords, or routinely monitored access activity.

Earlier this month, we reported that serious computer security problems persisted throughout the department and VHA because VA had not yet fully implemented an integrated security management program and VHA

[32] *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure* (GAO/AIMD-98-175, September 23, 1998).

[33] Information Systems: The Status of Computer Security at the Department of Veterans Affairs (GAO/AIMD-00-5, October 4, 1999).

[34] GAO/T-AIMD-00-74.

had not effectively managed computer security at its medical facilities.[35] 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. Specifically, as we reported, VA's New Mexico, North Texas, and Maryland health care systems had not adequately controlled access granted to authorized users, prevented employees from performing incompatible duties, secured access to networks, restricted physical access to computer resources, or ensured the continuation of computer processing operations in case of unexpected interruption.

To facilitate VA actions to develop and implement a comprehensive, coordinated security management program that would encompass VHA and other VA organizations, we reiterated our October 1999 recommendation that VA develop computer security guidance and oversight processes and recommended that VA monitor and resolve coordination issues that could affect the success of the departmentwide computer security program.

VA concurred with these recommendations and stated that it intends to develop an accelerated plan to improve information security at its facilities. Specifically, VA stated that it would track the resolution of the recommendations we made to correct specific information security weaknesses at the health care systems we visited. In addition, VA provided examples of security management activities performed by the VHA central security group to implement and oversee computer security throughout the administration. VA also stated that it would use its Information Security Working Group, which includes representatives of all administration and staff office security groups, to develop departmentwide policy, guidance, and processes.

In summary, the department still faces important challenges in several IT areas. While it has improved its IT investment decision-making process and plans to fill its department CIO position, VA may encounter problems achieving its "One VA" vision until it develops an overall business process reengineering strategy and a departmentwide, integrated IT architecture. Full implementation of our prior recommendations in these areas is essential to VA's achieving its "One VA" vision. In addition, VA's lack of departmentwide tracking of IT expenditures makes it difficult for the department to manage the risks of its IT investments. Further, top management support and commitment are essential to addressing the challenges VA faces in making greater use of DSS and in addressing issues involved in developing the compensation and pension replacement project. Improving VA's computer security will also take sustained leadership and commitment to developing and implementing a comprehensive security management program.

We performed this assignment in accordance with generally accepted government auditing standards, from June through September 2000. In carrying out this assignment, we assessed the actions taken to address our recommendations on improving VA's IT investment decision-making process. We reviewed documentation on VA's efforts to fill the CIO position and reviewed and analyzed VA, VBA, and VHA IT architecture documents, comparing these with NIST's five-layer standard, the guidance used by VA. To determine how IT expenditures are tracked, we reviewed and analyzed VA's policies and procedures and compared them with applicable guidance in this area. We discussed cost tracking procedures

[35] *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration* (GAO/AIMD-00-232, September 8, 2000).

with officials at VA, VBA, VHA, and five VISNs, and reviewed relevant documentation.

For the DSS project, we reviewed VISN and medical center examples for DSS use and barriers, and visited four VISNs—VISN 5 (Baltimore), VISN 8 (Bay Pines, Florida), VISN 18 (Phoenix), and VISN 21 (San Francisco)—to discuss their examples of DSS use and barriers to such use. Specifically, we analyzed the examples provided by the VISNs and medical centers and summarized them into nine categories of DSS use and 13 categories of barriers to such use. We also reviewed performance documentation and met with VHA officials to discuss actions planned for DSS use. For the compensation and pension replacement project, we reviewed plans and schedules for the project and visited the development site at Bay Pines. We also discussed issues with VBA managers in Washington, D.C. In the area of computer security, we evaluated security controls at three VHA medical facilities—VA Maryland Health Care System, VA New Mexico Health Care System, and the VA North Texas Health Care System—and reviewed our recent reports and VA updates on actions taken to address our recommendations.

We provided a draft of this testimony to VA for comments and incorporated changes where appropriate.

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.

Contact and Acknowledgments

For information about this testimony, please contact me at (202) 512-6253 or by e-mail at *willemssenj.aimd@gao.gov*. Individuals making key contributions to this testimony included Nabajyoti Barkakati, Michael P. Fruitman, Amanda Gill, Tonia L. Johnson, Helen Lew, Barbara S. Oliver, J. Michael Resser, and Kevin Secrest.

(511856)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)

VA'S INFORMATION SECURITY PROGRAM

TESTIMONY OF
MICHAEL SLACHTA, JR.
ASSISTANT INSPECTOR GENERAL FOR AUDITING
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS

HOUSE COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

September 21, 2000

Mr. Chairman and Members of the Subcommittee, I am here today at your request, to report on our findings 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 fraud. These information security weaknesses are so serious that since Fiscal Year 1998 the Department has designated information security as a material weakness under the Federal Manager's Financial Integrity Act.

Given the significant information security weaknesses that exist in VA, the OIG is continuing to focus audit coverage in the AIS program area. To the extent that our resources permit, our audit coverage will be expanded to address the Department's AIS review and reporting requirements. This effort will provide for an assessment of the Department's nationwide AIS posture, including tests of the effectiveness of information security control techniques. While the VA has established a *'Department Information Security Program Requirements and Budget Plan'* for addressing its security control weaknesses, this effort is expected to take several years to complete.

Our planned audit work will focus on 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. To help facilitate completion of necessary review work, the Inspector General has established an audit division whose primary mission will focus on information security. In addition, we will continue to review AIS security issues as part of the annual audit of VA's Consolidated Financial Statements (CFS) and as part of our continuing Combined Assessment Program (CAP) reviews of facilities. To further supplement this effort, we also plan to utilize contractor support to assist in completing penetration and vulnerability tests of selected VA automated systems.

The OIG has been involved with the review and oversight of the Department's information security program for several years. Our work has included AIS assessments at the Department's national data centers, Veterans Integrated Service Networks (VISN),

Veterans Benefits Administration (VBA) Regional Offices (RO), and Veterans Health Administration (VHA) Medical Centers (VAMC). In addition to these efforts, we also identified AIS related weaknesses as part of a vulnerability assessment we completed involving VBA's Compensation and Pension (C&P) program. This assessment was done in response to a request for assistance from the Under Secretary for Benefits to help identify internal control weaknesses that might facilitate or contribute to fraud in VBA's C&P program.

The following describes our information security audits that have identified significant security control weaknesses that make VA's systems and data vulnerable to unauthorized access and misuse.

Computer Security Implications from the 1999 Consolidated Financial Statements Audit

Audit tests associated with our annual CFS audit demonstrate wide spread system security control weaknesses. We found that often, the needed information security improvements were well known within the security community such as installing and implementing program patches, employing more secure system configurations, and making use of more secure management procedures, but little was done to correct these deficiencies. The following are selected examples of security control weaknesses that were identified:

- VBA Penetration Review

As part of the overall CFS audit, we contracted to conduct penetration tests of VBA systems to help assess the effectiveness of information system security general controls. The review concluded that a number of significant control weaknesses existed that made VBA systems vulnerable to unauthorized access and misuse.

In response to the penetration testing results, the Under Secretary for Benefits reported that corrective action had been taken in a number of problem areas with planned corrective action to be completed for all problem areas during Fiscal Year 2000. In addition to these efforts, the Principal Deputy Assistant Secretary for Information and Technology reemphasized the commitment of his information security program office to strengthening the overall security posture of VA, including the categories of control weaknesses found at the VBA facilities. He stated that his office would provide whatever manner of assistance that is needed to VBA to facilitate correction of these significant security control weaknesses.

- VHA ADP Security Review

While our review found that a number of significant corrective actions have been initiated to address information security weaknesses, VHA's program and financial data continue to be vulnerable to error or fraud because of serious weaknesses in Automated Data Processing (ADP) general controls throughout VHA. Our evaluation of the AIS

security management program at one VISN, and testing at four health care systems by the OIG and the General Accounting Office found wide-spread AIS security control weaknesses. These weaknesses included a lack of:

1. A comprehensive computer security management program.
2. A security plan that was risk based.
3. Contingency planning.
4. Access controls to network and main computer systems.
5. Management of network user identifications and passwords.
6. Monitoring network system activity.
7. Comprehensive physical security controls.

In response key actions being taken by VHA management to improve security include:

1. Contracting for additional penetration testing and risk assessments.
2. Follow-up testing to ensure local facilities have implemented prior recommendations.
3. Completing development of a technical security portion of the Regional Information Security Officer review program.
4. Providing security training to the Information Security Officers.
5. Completing security policy revisions.

VHA needs to improve the extent to which security is integrated within its organization and provide added authority to its security program. We believe that VHA's efforts will not result in adequate security unless there is better integration of the security management program. VHA has a decentralized organization responsible for managing data processing and sensitive information resources. We do not believe that VHA will achieve adequate security unless VHA managers commit and dedicate adequate resources to their local security programs.

Combined Assessment Program (CAP) Reviews of Facility Information Security

Our CAP reviews provide an independent and objective assessment of key operations and programs at VAMCs and ROs on a cyclical basis (about 30 reviews are planned annually at VAMCs and about 9 at ROs). These reviews, which include an assessment of facility

AIS controls, have identified a number of weaknesses that need to be addressed. For example, CAP reviews completed at facilities during 1999 and 2000 year to date have identified the following security control weaknesses:

- VAMC Security Issues

    1. Passwords were not changed at designated intervals.

    2. All users with access to information systems needed to use stronger passwords.

    3. User access levels need to be promptly updated to reflect current access requirements.

    4. Physical security of the main computer room needed to be improved.

    5. Annual AIS security awareness training and refresher training had not been provided.

    6. Information system contingency plans did not include a detailed prioritization of mission critical systems, designate an alternative processing facility, or include post-disaster recovery issues.

- RO Security Issues

    1. The duties of the Benefits Delivery Network Security Officers and their alternates needed to be assigned to individuals not directly involved with claims processing.

    2. All users with access to information systems needed to use stronger passwords.

    3. Each new employee with access to information systems needed to receive security awareness training and annual refresher training.

In response to each of the information security weaknesses identified, facility management agreed to take the necessary corrective actions that we had recommended.

Vulnerability Assessment, Management Implications of Employee Thefts from the Compensation and Pension System, and Observed Internal Control Vulnerabilities

In the past year, the Under Secretary for Benefits asked for our assistance to help identify internal control weaknesses that might facilitate or contribute to fraud in VBA's C&P program. The request followed the discovery that three VBA employees had embezzled nearly $1.3 million by exploiting internal control weaknesses in the C&P benefit

program. Our vulnerability assessment identified 18 categories of vulnerability involving numerous technical, procedural, and policy issues. The following key AIS related security weaknesses were identified:

1. Some stations were issuing employees multiple passwords under multiple identification numbers to enhance employee production, but what actually occurs is the defeat of controls intended to promote separation of duties and prevent fraud or program abuse.

2. A timesaving feature that allows employees to complete various claims actions provides the opportunity for improper access.

3. Passwords must be more secure. Some stations permitted the use of English words of as few as five characters for passwords, making it relatively easy for unauthorized persons to guess the password an employee is using.

4. Target security ADP records were poorly structured and lacked personal identifying information. This condition made it impossible to verify the propriety of user accesses or to conduct files maintenance.

In response to the vulnerability assessment, the Under Secretary for Benefits reported the initiation of actions to address the weaknesses identified.

Audit of the Compensation and Pension Program's Internal Controls at the VA Regional Office St. Petersburg, FL

This recently completed audit was conducted to test the existence of the control weaknesses identified in the 1999 Vulnerability Assessment of VBA's C&P program. In addition, we also tested various methodologies for detecting the existence of fraud. The St. Petersburg RO was selected for review because it was one of the largest ROs, accounting for 6 percent of C&P workload and it was the location where 2 of the 3 known frauds took place. The audit confirmed that most of the AIS related weaknesses identified in the vulnerability assessment existed at the RO. In response to the report recommendations, the Under Secretary for Benefits agreed to take necessary corrective actions to address AIS related control weaknesses.

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

Testimony Concerning the Veterans Health Administration Decision Support System (DSS) to the Subcommittee on Oversight and Investigations by Howard H. Green, M.D. – September 21, 2000

I am the originator of the VHA Decision Support System along with my colleague Dr. Elisabeth McSherry. The invitation to present testimony about the VHA Decision Support System (DSS) from the Chairman, Honorable Terry Everett, of this Subcommittee is appreciated. I have served the Department of Veterans Affairs as a resident physician, and attending physician. In 1973 I was appointed Chief of Staff of the VA Medical Center in White River Junction, Vermont and served in that capacity until 1994. From 1991 to 1999 I was the Contracting Officer's Technical representative for the DSS Contract and in 1994 assumed the role of Deputy Director for Technical Implementation of the DSS System. I retired from the VA on October 20, 1999.

Purpose of Testimony

The purpose of this testimony is to explain the capabilities of the DSS System as they relate to running the business aspects of VHA and how the DSS System supports the evaluation and monitoring of Health Care Quality. Finally it is my purpose to comment on the status of the DSS Implementation and the utilization of the system for the purposes for which it was intended. I will address the reasons why this implementation and subsequent use of the system have not yet reached the expectations established when the implementation began.

A detailed report of my evaluation of the DSS implementation was sent to Ms. Gail Cotten, Contracting Officer for the DSS Contract in October of 1999. Subsequently, a copy was provided to Ms. Helen Lew of the General Accounting Office, the staff of this subcommittee, and to Mr. Charles Yarbrough while he was the Acting VHA CIO.

It should be noted that the DSS system implemented by VHA is the same tool used by over 1,400 hospitals and Health Care systems worldwide. Many of these systems use this tool extensively for evaluating the cost and quality of their patient care system.

Summary of the Contract

The contract officially started on September 20, 1991. It went through eleven (11) modifications which were required because of changing conditions. Implementation of the system started in the medical centers in 1994. The contract was scheduled to end on September 20, 1999 but was extended to October 19, 1999 to accommodate the time required to complete negotiations on a follow on maintenance contract. Eclipsys Corporation (the vendor) agreed to this extension at current labor rates detailed in the contract. There are several important noteworthy points about the contract.

- The contract closed out approximately $761,000 under the original GSA disbursement authority of $24,368,533. This includes the extension period costs. The vendor was an important partner in meeting this goal.
- The functionality received exceeds that defined in the original contract document.
- The contract was completed on time.

Comment: I believe that this record has few parallels in VHA or possibly in DVA. My view is that a thorough review of contracts not meeting this standard should be carried out by both the Administration and by the Congress.

The Issue

This hearing is convened to determine in part whether the DSS System is being used by VHA for the purpose for which it was intended. Approximately 200,000,000 dollars (by the end of 2000) have been spent on installing this system (24 million for the vendor and 175 million or so contributed costs of VHA for personnel, supplies, travel, processing, etc.). It is time to determine whether the system is yielding the Return On Investment (R.O.I) expected.

The direct answer to this question is that the system is being creatively used in certain VHA medical centers, but is not currently being used across the system to generate the R.O.I. required. The real question then is why not? Since approximately 1400 Medical Centers and Healthcare Systems in the United States and Internationally – Australia, the

Netherlands, New Zealand and others – are using this exact system for meeting management and certain clinical needs.

What does DSS do?

There are six questions, which are of central importance.

The first: Does VHA need to know (to be in compliance with statute), what it costs, at the level of tests and procedures to deliver care and to sell its services to other Federal, State and Private entities?

The second: Does VHA need to know the cost for encounters of each patient for hospital, ambulatory, long-term care, etc?

The third: Does VHA need a system by which to determine the process of care in order to evaluate the efficiency of care, the adherence to clinical care guidelines, the frequency of selected adverse events and the impact of these adverse events on the cost of care?

The fourth: Does VHA need to be able to build budgets from workload defined by the descriptions commonly used in the private sector such as DRGs, long-term care Resource Utilization Group (RUG) classifications and ambulatory classifications as used by HCFA?

The fifth: Does VHA need to know what it costs for patient episodes in order to set rates for MCCF (medical care cost recovery) reimbursement from third party insurance; and to determine whether or not VHA is making or losing money on these transactions?

The sixth: Does VHA need to know patient specific costs in order to reasonably allocate appropriated funds to its principal operating units, the medical center?

This is precisely what DSS does. Furthermore, there is no other DVA or VHA system in operation which does this. DSS is the only system in place which is specifically designed to meet precisely the intent of the questions presented.

I have left out the seventh question and that is:

Does the VHA need a reliable system to answer the questions Congress asks about the costs of care such that the answer to the question can be proven if necessary by an audit of the process by which the answer was derived? Only the Congress can answer this question.

The DSS System is designed to accommodate this need.

Concrete Illustrations of what DSS does.

I can think of no better way to illustrate the DSS system capabilities than to cite the titles of presentations given between June 11-14, 2000 at the Eclipsys (the vendor) Decision Support 14th Annual User and Education Conference at the Washington Hilton and Towers in Washington DC. Presentations by VHA Medical Centers were well attended and the evaluations of the presentations were high.

Titles, Presentations by VHA Medical Centers:

- Alvin C. York VA Medical Center, Murfreesboro, TN

- Using DSS to Guide Clinical Interventions: A Case of Poly pharmacy and a Concomitant Illness of the Geriatric Population.
- Drug Utilization Review a Breeze with DSS: Utilization of HMG-COA Reductase Inhibitors (cholesterol lowering drugs).

Portland VA Medical Center

- Clinician's use of DSS Data to Identify Opportunities in Cost Reduction. (Note: the problem of a 10 million-dollar operating deficit appropriately includes physicians in its solution. DSS contributed significantly by providing necessary information.)

- Allocation of Faculty Salary Dollars and Determination of Cardiac Cath Lab Procedure Costs in an Academic VA Hospital.

VAMC North Chicago

- DSS Reports Database for Department Reviews. (Note: Department refers to operating units within the Medical Center such as Radiology, Laboratory Medicine, Surgery and their specialty units.)

South Texas Veterans Health Care System, San Antonio, TX

- Forecasting Effects of Integrating Mental Health in a Multi Hospital System.

VAMC Northern Indiana

- Automated DSS Monthly Processing and Audit steps. (Note: A tool developed to assist new DSS personnel responsible for maintaining the system, given the fact of employee turnover.

Selected presentations from Non-VA Medical Centers.

- **AMC Amsterdam – The Netherlands**. "Decision Support in the Operating Room Department.
- **St. Joseph Health System – Orange, CA** "Using Decision Support Information in Establishing Quality Improvement Benchmarks"
- **Jefferson Health System – Philadelphia, PA** "Promoting Clinical Integration in an Integrated Delivery System."
- **Mayo Clinic – Rochester, MN** "Thrills, Chills and Spills Revisited: Teaming Clinical and Financial Analysts to Support Performance Improvement.
- **Royal Children's Hospital, Women's and Children's Health Care Network** – Melbourne, Victoria, Australia "Integrated and Enhanced Quality of Patient Care using Sunrise Decision Support Manager"
- **The University of Iowa Hospitals and Clinics – Iowa City, IA** "Decision Support: Meeting a JCAHO standard on Resuscitation"
- **Wellington Hospital Capital Coast Health Ltd. – Wellington, New Zealand** "Benchmarking, A Tool to Improve Clinical Performance?"
- **Queensland Health, Brisbane – Queensland Australia** "Corporate Quality Improvement and Enhancement: The Queensland Health Way"
- **Texas Children's Hospital – Providence, TX** "Using Decision Support for Facility Expansion Projections"
- **Emory University Health Care – Atlanta, GA** "Consolidated Financial Statement and Department Management Reporting Using Transition II and Crystal Reports"
- **St. Michael's Hospital – Toronto, Ontario Canada** "Using Transition II to Support Effective Merger Decision-Making"
- **Children's Hospital, Stanford Medical Center – Palo Alto, CA** "Building a Basic Business Plan"
- **Holy Family Hospital – Methuen, MA and Caritas Christi Health Care System, - Boston, MA** "Negotiating Payment Rates that Mimic Patient Care Cost"
- **University of Chicago Hospital – Chicago, IL** "Using Eclipsys to Predict Base Staffing and Overtime/Temporary Labor Needs"
- **The Cleveland Clinic Foundation – Cleveland, OH** "Cost Savings and Cost Avoidance of Pharmacist's Intervention"

I believe that anyone reading this list carefully could come to several conclusions.

1. The DSS System has broad functionality.
2. There are University Medical Centers affiliated with the VA using DSS.

3. The nature of the Medical Centers using the system includes Fee for Service, Fixed Price Reimbursement, and Governmental Systems.

How does the DSS System Produce its Information?

Simply put the DSS System takes appropriate computerized extracts of workload data (tests, procedures, patient encounter, prosthetics, etc.) from the VHA VistA transaction and Austin Automation Center Systems and combines this with extracts from the VHA portion of the Financial Management Systems, applies management accounting and cost accounting principles to this data to yield its outputs. Audit procedures if used, assure that the data accurately represents that in the feeder system and in addition there are automated audits which can demonstrate deviations from the established standardization of internal structural rules promulgated as part of the implementation sequence of the system.

Proper function of the DSS System is optimized if it receives accurate and complete data from the feeder systems. The clear responsibility for this data rests with the top management of Medical Center, VISN's and Headquarters. Those who criticize DSS data quality are looking at the responsible party if they are facing a mirror.

Why is DSS information not being universally used to help to improve the management of VHA and to assist in improving the quality of its service?

It was clear by FY1997, that use of the information from DSS by management was not robust from those sites that had solid systems with information which was current enough for looking at production costs, processes and quality issues. Part of this had to do with the fact that most top managers and their staff did not know how to use the information to improve hospital performance, the second was that the leadership was not requiring them to manage at this level of process and cost details. The old formulas for extracting money through the political process and the "no brainer" actions of Medical Center integrations, shifting care from inpatient to ambulatory settings and creating better access to the system which should have happened long ago, appeared to be working.

President Harry S. Truman had a sign on his desk that said "The Buck Stops Here." This simple statement summarizes the management literature dealing with management accountability and organizational behavior.

It is well known that organizational behavior reflects the behavior at the top of an organization. Top management in the VA is and should be held responsible for failure to provide, execute and use appropriate information and strategy to optimize VHA performance, assure quality and to meet their fiduciary responsibility to the taxpayer. Those responsible in top management in the VHA include the Secretary, the principal Undersecretaries. The VHA VISN and Medical Center Leadership. The sign on the desk should not read "The Buck Stops with our Subordinates, the Systems, the Data, etc.

It is my opinion that the following factors although unpleasant, are supportable.

1. Accountability at the level of detail supported by DSS is feared. It is contrary to the traditional mechanisms used for managing in a governmental system. The action which will be suggested by careful analysis of DSS information could be powerful and will be seen as jeopardizing programs, power and careers.
2. There is no ownership by the Executives of VHA or DVA of the DSS System and the management principles it represents; hence, no leadership of significance.
3. The Department is essentially rudderless. A number of important positions, Secretary, Deputy Secretary, Assistant Secretary for Management, Undersecretary for Health, all are held by people designated as "Acting."

   Two positions (VHA CIO and CFO) which affect the DSS effort are held by new incumbents. Corporate Discipline (in the healthy sense), which in recent years has been tenuous at best, does not exist. The uncertainty generated by current circumstances has a profound effect on the behavior in the Bureaucracy. People shift their attention to personal survival and position.
4. The current method for acquiring resources by the Department of Veterans Affairs works. VA managers have become expert at manipulating the current system and don't want to change.

Statements made about DSS by top management are having a serious negative impact on DSS.

"It ain't so much the things we don't know that gets us in trouble. Its the things we know that ain't so." – Artemus Ward

I am particularly concerned about public statements about DSS made by the incumbent Assistant Secretary for Management who is now the Acting Deputy Secretary at the Leadership Forum in Phoenix and a meeting for VA VISN and Headquarters Executives in Seattle in August. He in essence stated that if it was up to him that he would kill DSS, the data quality was not good and the standardization was not good. (I did not directly hear these statements but they were reported to people in the DSS Program by several attendees). I do not believe that the Acting Deputy Secretary had had appropriate briefing by technically knowledgeable people about DSS nor is it likely that he had researched carefully the reports by GAO, the IG and the Program Office on these subjects.

The effect of such statements in hierarchical organizations by people who have authority to make decisions can have disastrous effects on programs. If made without proper investigation it represents a failure to exercise Due-diligence.

What are the excuses used by managers for not using DSS?

The most common excuses are as follows:

- **It's not ready yet.** – It is my understanding the Dr. Garthwaite has told the Congress that DSS is implemented in all of the medical centers. What might not have been said is that a number of medical centers have not structured the system entirely according to the guidelines provided. The IG report on standardization addresses these issues.
- **The data in DSS is no good for comparison because there is no standardization.** This is not a true statement.

  Dr. Kizer requested that the IG examine the issue of standardization within the DSS application, apparently because some Hospital Directors and Fiscal Officers said they couldn't rely on the data for comparing hospital performance because it wasn't standardized.

  The IG examined the issue and concluded that DSS had a structure and standardization guideline which if followed would give a system which was useful for managing locally and at the VISN systems level.

  Their exact conclusions are as follows:

  - "Local DSS staff and users need to understand that the basic DSS model, if adhered to, is fully capable of meeting the data needs of all management levels. DSS' ability to group production units into any set of larger reporting groups that users may choose ensures the maximum utility of DSS data at all management levels, and by maintaining relatively small production units with closely related products, DSS can calculate product costs with better precision.
  - To better guide local staff in their implementation of DSS systems, VISN and VHA Headquarters management need to continually update what their DSS data needs are. They need to determine what types of reports they want, what the data elements should be, and what the formats should be. We would expect these determinations to be part of an overall assessment of VHA's "business needs."
  - VHA top management must then ensure that DSS structures in use at medical centers adhere to the basic DSS model to satisfy the business and data needs of local, VISN, and VHA Headquarters managers.
  - Much of this effort will involve the "education" of staff at all levels. To this end, facilities and VISNs that have successfully implemented DSS in adherence to the model should be identified and held up to others as "best practices" sites, so that they can be emulated."

  The fact is that the feeder system data feeding DSS from VistA, Austin Automation Center encounter and Fiscal System data from FMS came from standardized fields.

Audit systems are available to demonstrate the integrity of this data and to demonstrate deviation from the DSS Structural Guidelines.

Dr. Kizer accepted the findings and recommendations of the IG.

The first and usual response of managers who duck responsibility and attendant accountability is to blame the system. Since the structure and standardization of DSS at any Medical Center is within the direct control of the Medical Center, the IG conclusions would appear to point to the famous statement by the cartoon character, Pogo – "We have met the enemy and it is us."

- **It's not easy to get information out of the system, it is not user-friendly.**

  Despite the fact that patient specific inpatient and outpatient costs from DSS are available on a secured VHA web site called the KLF report and extensive training on how to generate reports from the system, has been offered to VISNs and Hospital Management, the fact the site teams can generate extensive adhoc reports requested, and that the fixed reports from the system are designed for managers, the complaint continues. The simple fact is the complainers won't take the time to learn. The DSS Program Group is currently providing extensive training on the use of the system and the vendor is training users on an advanced SQL DSS reporting tool which uses standard state of the art third party point and click reporting tools (Crystal Reports) as a front-end to make it easier to get information. There will be no way to satisfy those who don't want the information and who are unwilling to change previous habits.

  In contrast to the top management, the people on the front lines of the site teams, although frequently understaffed, and on some occasions not having appropriate backgrounds for the task, have dug in and done a remarkable job of implementing this complex application. The number of successes are greater that the failures. A few sites have developed robust systems which have been used for aiding decisions at the medial centers and VISNs. These sites in the last three years have prepared and given presentations on how they are using the system to improve performance at the annual user group meeting of the Eclipsys (the vendor) Corporations Decision Support customers. These presentations have received praise from the private sector users. The VA gave the presentations listed above in this testimony and all were well done.

  It is my opinion that many of the site managers and site teams have far better insight on the processes which make the Medical Centers run than those who manage the Centers.

- **The data isn't timely.**

  There is no question that system-wide the medical centers are not in synchrony with the monthly processing of data. It is obvious that processing cannot begin until the transactional databases close.

Specific factors which impede bringing DSS to an optimal state.

End of year closure on transactional databases which feed DSS.

- The financial database (FMS) closes promptly within 5-7 days of the October 1st closure date. Therefore, this database does not impede movement forward into the new year.
- The workload database – dealing primarily with Medical Records Data are generally not actually closed until December. An inordinate number of corrections are entered at the end of the year. Sites cannot start the processing of October data and the end of year processing sequence which corrects and recosts the products and encounters until this closure. This sequence requires 2-3 weeks and is delayed until after the Christmas and New Year Holiday. The sites can however, build new structures in DSS required for the coming year as soon as they are known. In fact these structures could be built prior to October 1 of the current year.

Lack of communication between those responsible for the VistA transactional databases to those on the DSS technical support team.

This single factor was a major stumbling block in the implementation sequence and a principal cause of delay in the process of starting a new fiscal years information processing

sequence. DSS requires lead-time to adapt to changes planned in the VistA data set. Extracts have to be re-written and coded, deblocker of the extract e-mail messages changed at AAC – SAS routines redone. The new software must be carefully tested. This requires extensive work planning and writing of specifications. The VistA team assigned to support the DSS technical team was frequently not informed by other VistA developers of their changes, despite oral and written agreements to do so. This delays the ability of the DSS Technical Support people to get the appropriate change instruction to the field. The cooperation by VistA reached a nadir between 1996 and 1998 because of the assignment from the Birmingham, Alabama CIO field office to the Albany field office for VistA support. The Albany group had no experience or knowledge about DSS support. The number of people assigned to the project was reduced and there appeared to be growing hostility in VistA toward the DSS application. It is my belief that this hostility came directly from the top of the CIO organization. It was not until about 19 months ago when the program support was taken out of the Albany field office and reassigned to Bay Pines that this attitude changed. Lack of stability of programming staff assigned to dealing with the VistA needs of DSS is a constant problem.

Decreasing reliability of support by the Austin Automation Center

At this point, VHA spends about 12-13 million dollars per year on computer and system support of the DSS application. This represents 40-50% of the revenue received by AAC from VHA. It is important to acknowledge that this application represented a real challenge for the AAC in that it requires a very high degree of user interactivity to build the structure, set up processing sequence and generate reports prior to the advent of this application. The AAC was the home of a number of DVA, VISN and VHA databases requiring little end user interactivity, such as Payroll, the Financial Management System, the Patient Treatment File, etc. In short, it was a batch shop structured according to a set of routines and rigid timelines. DSS represented for AAC a huge change of role and operating philosophy. DSS was no more or less than a view toward the future role of mainframe computing systems which had begun much earlier in the corporate world. Control of the process and service to a single entity had to give way to service of multiple users and control by the customer. They had to shift over a short period of time to a vendor role offering services which met the needs defined by the user, not by them. This required a change on staff training, automation of processes which previously required manual intervention, design and execution of systems to analyze the flow of processes within the database and applications. The process towards this goal was going reasonably well, but began to deteriorate rapidly during the preparations for the FY2000 DSS rollover, this was unrelated to the Y2K issue which was done well. The number of errors made by the AAC in the testing and preparation for this rollover has been notably greater. I see little evidence that the AAC has given continuous training to staff who are assigned to the application. In fact the AAC staff was given the same training at the inception of the project as the medical centers were given and a vendor expert was physically assigned to AAC for a full year at the inception of the implementation, followed by approximately six months on site and then access as required. Although the AAC has begun the capability maturity model which is widely accepted in the computer world as a way to improve performance, they apparently have not used it as an analytic process improvement tool to track and analyze internal errors at the detailed processing task level. This decrement in performance delayed the initiation of FY2000 change over by two months.

Staffing of the site teams at the Medical Centers

Directors have not followed the guidelines for staffing numbers or the background experience of staff assigned.

Timeliness Need

There is little need for so called real time cost data. In a fixed cost environment product costs fluctuate on a monthly basis primarily because of volume. As the year progresses a year to date cost profile emerges (usually in the fourth month) which begins to make sense and at the end of the year the entire database is recosted to yield end of year costs for products and the patient encounters which use these products – cost trends with time are more valuable in many cases than short-term costs.

What is the critical factor required for integrity of DSS information?

Central to the whole process is the integrity of the data which is collected and used to monitor, measure, evaluate, control, and build the systems which reduce error, prevent mistakes and improve outcomes. DSS can be looked on as a tool which uses this data to aid in the improvement of patient outcomes.

The success of the DSS as such a tool is critically dependent on the integrity and completeness of data it receives from the transaction system. I will restrict my comments to this issue.

In 1995 the GAO report entitled VA Health Care Delivery, Top Management Leadership is critical to the success of Decision Support System. Concluded in the findings that:

1. VHA has not developed a business strategy for effectively utilizing DSS as a management tool.
2. Top Managers have not defined the business goals to be achieved and measured by using DSS.
3. Top Managers have not provided leadership necessary to DSS.
4. VA culture constrains progress.
5. Information infrastructure is inadequate. Clinical data is incomplete, inaccurate or inconsistent.

In my opinion all five of these conclusions are applicable today and because of this the DSS tool cannot be optimized. In terms of data completeness and quality we are a little better off than we were five years ago. Of these five factors the most critical has to do with VA culture. Dr. James P. Bogian, Head of the Veterans Health Administration, National Center for Patient Safety, refers to the need for a cultural change as it relates to the comfort with which error reporting can be done by health care professionals. Until people can tell the truth to their supervisors without fear of reprisal (shoot the messenger syndrome), we will continue to come up short of our goals. One of Dr. Deming's principles was to "Drive out fear." I can tell you that "shooting messengers" is a robust activity. For some reason the truth is unpleasant. Efforts by the head of DSS Data Systems (who is the co-originator of DSS) to clarify false statements to VA Officials and to point out data problems have been met with threats of disciplinary action by her immediate supervisor.

Culture change requires direct top down leadership and support to accomplish. Until the goal of patient care safety and quality becomes the unequivocal first priority, data integrity and quality will not change. Data issues are not the province of the CIO but must be the principal concern of top management. Absent this culture change, clear direction, and the promulgation of corporate discipline as it applies to financial and workload data systems, nothing will change. There has been a steady and perceptible degradation in fiscal information as VISNs, Program Offices, and Medical Centers ignore the published guidelines on the use of Cost Center and Budget Object Class categories. In fact there has not been a systematic audit of compliance in over ten years.

There has been no credible comprehensive audit of workload system data integrity and completeness. There is no major effort which places a priority on data collection technology to accomplish the need for a complete data set. The notable exception is the medication administration technology now being implemented. This effort began over ten years ago, and the implementation was flawed because the Intensive Care Unit (ICU) patients were not included in the original design.

Conclusion:

The DSS application in the great majority of medial centers can be used for decision making. If it is made clear by top management that their decisions will be in large measure influenced by DSS information then the integrity and completeness of transactional data which feeds DSS will begin to improve quickly. Where clinical matters are involved working physicians must be involved in the solution to both financial and clinical problems. The presentation at the DSS User Group in Washington, DC by the Portland VAMC, points to the effectiveness of this strategy. Failure of top management to become constructively involved in this process and in changing the VA culture guarantees an adverse outcome. The opinions expressed in this testimony are entirely those of the author.

Brief Curriculum Vitae: Howard H. Green, M.D.

Born: May 18, 1934 – Detroit, MI

Medical Specialties:

Internal Medicine – Board Certified
Nephrology

Academic Titles Dartmouth Medical School:

Assistant Professor of Clinical Medicine	July 1968 – July 1971
Assistant Professor of Medicine	July 1971 – July 1975
Associate Professor of Clinical Medicine	July 1975 – July 1992
Professor of Clinical Medicine	July 1985 – July 1992
Professor of Medicine	July 1992 – December 1994

Academic Administrative Titles:

Assistant Dean for VA Hospital Affairs	July 1973 – February 1975
Associate Dean for VA Hospital Affairs	July 1975 – December 1994

Department of Veteran Affairs; Veterans Health Administration

Attending Physician VAMC White River Jct., VT	1968 – 1973
Chief of Staff, White River Jct., VT	June 1973 - December 1994
Presented the DSS Concept to Chief Medical Directors Field Advisory Group	1983
Managed the DSS development and pilot testing program	1983 – 1994
Contracting Officers Technical Representative to the DSS Contracts	1991 – October 1999
Deputy Director for Technical Implementation DSS	1994 – October 20, 1999
Retired from Department of Veteran Affairs	October 20, 1999

Military Service:

U.S. Navy 1960 – 1963 – Submarine and Diving Medicine

Statement Regarding Status as a Witness

I, Howard H. Green, certify that as a non-governmental witness, I have received no Federal grants or contracts ever relevant to the subject matter of my testimony.

Howard H. Green 9/12/2000

Howard H. Green, M.D.

Statement by
Robert P. Bubniak.
Acting Principal Deputy Assistant Secretary for Information and Technology
Department of Veterans Affairs
Before the
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
U.S. House of Representatives
September 21, 2000

Good morning, Mr. Chairman and members of the Subcommittee. I am pleased to testify before you today to discuss the Department of Veterans Affairs' Information Technology programs.

On June 25, 1998, the decision was made by the Secretary to separate the Chief Information Officer (CIO) function from the Chief Financial Officer and create a new Assistant Secretary position to assume the duties of the CIO. The entire organization of the Deputy Assistant Secretary for Information Resources Management was realigned under the new Assistant Secretary. The new office was activated on July 1, 1998, with the assignment of a Principal Deputy Assistant Secretary. On June 1, 2000, the Principal Deputy Assistant Secretary retired and on June 2, 2000, Secretary Togo D. West, Jr. appointed me Acting Principal Deputy Assistant Secretary for Information and Technology and Acting Chief Information Officer for the Department. Until the appointment process for a new Assistant Secretary is completed, the Acting Principal Deputy Assistant Secretary is the Acting CIO. This separation of CFO and CIO duties permits the appropriate emphasis on the Department's information and technology issues, which are keys to improving service to veterans.

I'd like to bring you up to date on some of VA's major initiatives.

VA IT ARCHITECTURE

The Department of Veterans Affairs is committed to the development and full implementation of a Department-wide Information Technology Architecture. We do not expect this to be easy. VA has three (3) distinct Administrations, each with its own particular mission and large, legacy information systems. We have done many studies in the past aimed at coordinating or combining these stovepipe management information systems, all with little success. However, with the Acting Secretary's emphatic insistence on One VA, we are beginning to see more cooperation among the Administrations.

As a first step in developing an Information Technology Architecture (ITA), VA completed a Technical Reference Model and Standards Profiles in May 1999. VA is now developing the Enterprise Architecture to complete the ITA. An Enterprise Architecture is the explicit description of the current and desired relationships among business and management processes and information technology (IT). It will describe the "target" environment VA wishes to create and maintain by managing its IT portfolio. The Enterprise Architecture will be a tool used to enable VA to transition from the current to the targeted IT environment. We intend to create a status management capability to track our progress from the current environment to our target environment.

A cross-organizational workgroup, comprised of both business operations and information technology staff from each of the Administrations and staff offices, was approved by the VA's CIO Council to guide the development of the enterprise architecture and to ensure that the architecture fully integrates VA business processes and technology so that it truly reflects One VA. VA's

Administrations and staff offices have been solicited for workgroup representatives.

At the May House Veterans' Affairs Committee oversight hearings, VA's then Acting CIO agreed to provide Congress with a plan for developing the Enterprise Architecture. In August 2000, VA provided a white paper, which described the plan and steps to be taken, a statement of work for contractor support, and a milestone chart with estimated completion dates. At that time financial data on information technology expenditures for the last five (5) years was also provided.

VA INFORMATION SECURITY

During the past sixteen months, VA has pursued an aggressive security improvement program that focuses attention to security in our capital investment planning and project approval processes. But most importantly, we created a durable central security organization, whose program model is a continuous process based on risk management principles endorsed by the General Accounting Office (GAO).

We want to assure you that VA does not underestimate the challenges we face to achieve adequate security in all six of the general control areas against which GAO measures any agency's security. We accept Congressman Horn's grade of a D as a rebuke and a wake up call. We are committed to changing that grade to an A as soon as possible. We have much work to do in the areas of access controls, application software development and change control, personnel controls, system software controls, and service continuity controls. And, of course, we must cultivate the security program management groups at the Department and component office levels that are the catalysts for improving all these controls.

Like many agencies, VA let the fast pace of the Internet and other computer innovations outstrip our attention to, and investment in, security practices. So we now have much catching up to do. We have experienced some of the same embarrassments as other agencies – defaced public web sites, sluggish reaction to virus attacks, and so forth. We appreciate the value of the comprehensive audit results we have from GAO and our Inspector General. These audit results are tangible evidence of how much work we have to do. But they also give us an excellent perspective on just what and where the problems are.

So we are now acutely aware that an underlying cause of our present security posture is that we had not instituted a management approach that proactively attacks risk at its roots. Instead, there was a tendency to react to individual audit findings, with little ongoing attention to systemic causes of weaknesses. Since we strengthened central security management in 1999, improvements have been pursued within a risk management framework, and will continue to be pursued in that way.

A variety of initiatives are already completed or underway in formal risk assessment, policy development, controls implementation, and awareness and training programs. Efforts are pursued from a Department-wide perspective, and concentrate on areas where consistency, balance, and economies of scale across the Department are essential to good security.

In just the last year, we contracted for, and completed, an independent VA-wide risk assessment. We vetted and issued policies in the areas of password strength, dial-in connections, anti-virus controls, and employees' personal use of government office technology. These were some policy areas of greatest concern based on existing audit findings. In addition, we now operate a VA-wide critical incident response operation that is VA's nerve center for rapid and coordinated action against virus outbreaks, network attacks, E-mail storms, or other kinds of security incidents.

We are investing real dollars in the development of a formal system certification and accreditation program to prevent a future generation of security-starved systems. We are also investing real dollars in awareness tools and events, and in a detailed

curriculum of training for our security officers. For example, last June we broadcast live by satellite television into every VA facility a two-hour management panel titled "Information Security – The High Cost of Management Apathy".

In the area of technical controls, we are laying the groundwork now for significant capital investments next year in major security infrastructures -- including public key infrastructure, biometric controls, intrusion detection, and better virus protection. These capital investments are embodied in an FY 2001 capital investment initiative approved by the Secretary last year in the amount of $17.5 million. This level of commitment to funding an agency's central security management is probably unprecedented in the civilian agency sector.

Because these efforts are now undertaken by a central security management office, scarce security resources in the Administrations and Staff Offices can now concentrate on internal compliance measurement, which by its nature demands inside change agents to overcome cultural and political barriers. We are very excited about what we are doing on information security, and do not plan to lose this momentum in the coming months.

I have begun investigation into the creation of a Senior Executive Service level position to head the Department's IT Security Program. This senior position would serve as the CIO's management advisor and senior consultant regarding development, publication and implementation of Department-wide information security standards, policies and guidance, as well as coordination and integration of all aspects of VA's cyber, telecommunications and information security program.

SMART CARD

During the One VA conferences, discussion focused on providing veterans a Smart Card that would contain veteran-specific information. This information would be contained on a card the size of a credit card. The concept is that a veteran could use this card to obtain expedited services at any VA facility. For example, by using the Smart Card, veterans would not have to repeatedly fill out the same forms concerning eligibility and income information each time they visited a new medial facility or regional office. The card will have critical medical data such as blood type, known drug allergies, etc. The Acting Secretary is fully supportive of the Smart Card concept and has expressed his desire to have Smart Card functionality in place at VA.

The Veterans Health Administration (VHA), working closely with the Office of Information and Technology, was charged with taking the leadership role in combining the business needs of the VHA, the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA) in implementing a Department-wide common Smart Card. A VA Smart Card Steering Committee and the VA Smart Card Project Management Team have been established to finalize plans and ensure effective acquisition and implementation. We are working together as One VA to develop the plans, requirements, and resources for a One VA Smart Card for America's veterans.

On August 31, 2000 a Smart Card proof-of-concept demonstration was conducted for the Acting Secretary and Veterans Service Organizations representatives. The demonstration showed how the Smart Card could support express registration to save time for the veteran and the VA staff while improving data quality. The demonstration also showed how a veteran using a kiosk could digitally sign forms using keys securely carried on the card. Our goal is to launch an initial implementation of the VA Smart Card in Veterans Integrated Service

Network (VISN) 2 and VISN 12 during January 2001 and begin national implementation by January 2002.

GAO REPORT ON VA'S IT PROGRAMS

We have achieved much progress in addressing GAO's recommendations, particularly in our information technology review process. The Department will continue to strengthen its capital investment planning, make improvements to streamline the process while continuing to capture information needed to make informed investment decisions. We also recognize that VA faces real challenges, including those GAO identified.

When the Secretary decided in 1998 to establish an independent CIO function, the Department moved swiftly to realign its resources to support that decision. Since then the Principal Deputy Assistant Secretary for Information and Technology has served in the CIO capacity, spearheading the Department's efforts to streamline and integrate itself to a One VA posture that provides seamless service to our nation's veterans. While we have yet to achieve that vision, we continue to make strides towards this end. Our efforts in building an enterprise architecture and mature capital investment process are key strategies to achieving this vision.

DECISION SUPPORT SYSTEM (DSS)

DSS, which was implemented nation-wide in July 1998, is a medical center-based cost distribution program used to produce management information for VHA decision-makers. It directly supports the management of VHA facilities by providing workload, patterns of care and clinical outcomes information linked to resource consumption costs associated with health care processes. In an evolving competitive health care environment, DSS is aimed at improving procedures and practices while lowering costs of care at VHA facilities. As of August 31, 2000, 139 of 140 sites are processing FY 2000 data. The remaining site is on an accelerated plan to come up to the standards of the rest of the system.

Decision Support System (DSS) is a critical information system for effectively managing at the clinic, medical center, VISN and headquarters levels. While implementation has been slower than projected, the system is now in place. DSS differs from other existing VA databases in that it integrates selected elements from each episode of care, resource allocation and clinical procedure into a longitudinal format. This allows statistical outcomes comparison amongst VHA facilities on key data elements, including fiscal, care descriptors and resources per episode of care. Using this information, DSS allows VHA management to analyze and compare workload and cost data in great detail. It also allows medical centers to perform product line analyses, modeling, clinical performance measurement and clinical quality management.

DSS supports VA's quality improvement initiatives by providing information systems support for outcome-based performance measures that document the effectiveness of the health care delivery process. The combination of observations relating patient care outcomes (quality) with resource utilization information (cost) can facilitate understanding of the value of health care services provided by the VA medical centers.

DSS supports a) budgeting and planning for medical centers; b) VISN resource distribution to medical centers; c) productivity analysis; d) outcome measurement based performance and effectiveness of health care; e) benchmarking for VA comparative aggregate data at network or national levels; and others. Significantly, in August 2000, the Acting Under Secretary for Health made the decision to transfer DSS to the Office of the Chief Financial Officer to be used as a replacement for the workload distribution engine for the Veterans Equitable Resource Allocation (VERA) system.

Initially, DSS was envisioned to be an individual medical center based system. As VHA evolved toward a more VISN-centered management model, different VISN and national reporting requirements were identified. Additionally, the degree of standardization required for VISN and national reporting and decision support added complexity to the implementation.

During implementation, a number of issues arose which still require additional attention. DSS is being asked to do corporate roll-ups of information that are beyond what original software was originally intended to do. Our people are finding that loading data into DSS is proving to take a lot of work and very careful attention. Further, DSS is not yet sufficiently user-friendly to make it as valuable as it needs to be to managers at all levels.

But let me very clear. We are strongly committed to a decision support system that helps us effectively manage the veterans health system at all levels. Managers need these tools and they need to use these tools.

VHA leadership and the DSS Steering Committee are working hard at improving the standardization and ease of use of this critical management support tool. At the same time, we are looking carefully at what is the best long term approach to ensuring that a user-friendly and effective decision support system is available to and used by all of our managers. We know this is an issue of high interest to the Committee and we will work closely with the Committee to ensure a decision support system is in place and effectively used.

VETERANS HEALTH INFORMATION SYSTEMS AND TECHNOLOGY ARCHITECTURE (VistA)

VHA operates the largest centrally directed health care system in the United States made up of 172 medical centers, 341 Congressionally approved community based clinics, 134 nursing homes, and 41 domiciliaries. The operational support backbone is the Veterans Health Information Systems and Technology Architecture (VistA) system. VistA is a combination of more than 130 health care applications that have evolved over time. Let me provide more detail about the evolution of this environment.

- In 1982, VHA committed to building an electronic health care architecture called the Decentralized Hospital Computer Program (DHCP). The focus of this program was the implementation of software applications that were easily integrated into a complete hospital information system. VA began developing applications using VHA programmers who worked directly with user groups in software prototyping environments.

- In 1996, DHCP went through a major modernization. The existing processing architecture was overhauled to utilize state-of-the-art client server technology, and the applications were modified to utilize intelligent workstations using Graphical User Interface (GUI) conventions. This major renovation signaled the beginning of VistA, a rich automated environment that supports the day-to-day operations at VHA health care facilities. In addition, VistA includes necessary links that allow commercial off-the-shelf software and products to be used with existing and future technologies.

VistA incorporates all of the benefits of DHCP as well as an array of commercial and other information resources that are vital to the day-to-day operations at VHA medical facilities.

VHA's goal for VistA is to improve the quality and timeliness of health care service provided to veterans. To meet this goal, VHA has established standard criteria for the design, development, and implementation of software. The criteria are:

a) all software developed and implemented throughout the VHA medical care system must be standardized and able to be exported to all VA medical facilities;
b) all software must be technically integrated using a common database, programming standards and conventions, and data administration functions;
c) all software must use standard data elements;
d) all software must allow timely access to data;
e) all software must avoid dependence on a single vendor; and,
f) all software must have system integrity and protect data against loss and unauthorized change, access, or disclosure.

VistA, starting with DHCP, was developed some 20 years ago and represented a major breakthrough in providing a strong information system dedicated to providing quality health care and managing the medical centers. For all these years, DHCP and, more recently, VistA has carried a heavy load and done it well. We have the intellectual capital, amongst VA and our private sector partners, and the system underpinnings to deliver a much stronger information system for the future.

Today, it is a system that must become much more flexible for it to support a mobile veteran population or manage at the VISN and national levels. While some parts are up with current developments in information technology or are state of the art, other parts are not.

Today and for the future, the requirements placed on a veterans health information system are increasing and at a faster pace. For the future, VistA will need to evolve into an information system that makes an individual veteran's health information available any time, any place, to any authorized health care provider and in real time. It needs to be an information system that is flexible, can change quickly, incorporates the latest provider and management applications, and uses the power of the web to support veterans and health care providers. It also needs to be fully integrated with our efforts to establish One VA.

VHA's IT strategic vision focuses on expanding VistA to become a veteran's information resource, with the health record owned by the veteran and used in partnership with the veterans health system doctors, nurses, pharmacists and other providers. The VHA CIO is working with national leadership to translate the strategic vision into an operational plan.

Information is such a powerful tool to help us improve veterans health. It is incumbent upon us to use the best information system available to ensure the best health care for and maximize the health of our veterans.

VETSNET

VETSNET is an integrated information system designed to meet the critical needs of veterans and their families and/or beneficiaries who receive benefits and services from VBA. The initial phase of VETSNET created an infrastructure and then focused on replacement of the Compensation and Pension (C&P) payment systems.

During the last several months, VBA has conducted a series of planning summits to identify and plan for essential steps required for successful VETSNET C&P implementation. As a result of these summits, a wide number of VETSNET C&P sub-projects have been identified and project team leaders assigned responsibilities for each of these areas.

On June 12, 2000, VBA established a VETSNET Implementation Project Management Office (IPMO) to facilitate information exchange and coordination

between all the VETSNET project teams and to serve as the focal point for the VETSNET project. The Director of the VETSNET IPMO is the same individual (Sally Wallace) who led VBA's successful Year 2000 (Y2K) conversion effort, and VBA is following the same model that was used for the Y2K initiative.

The VETSNET IPMO is currently in the process of developing an integrated project management plan with proposed costs and milestones. Project management methodology is currently being emphasized throughout VBA, and the IPMO is applying this technique to ensure that the application development and implementation remain on track. Additionally, the VETSNET IPMO is in the process of updating the VETSNET Capital Investment Plan to incorporate implementation and deployment costs and activities.

Both VETSNET and VISTA users can now access shared veteran information through an intranet application that is capable of capturing data from the Beneficiary Identifier and Records Locator System (BIRLS) and the Benefits Delivery Network (BDN) and displaying the data in a web browser environment. This new tool is called Intranet BIRLS/BDN Access (IBBA). IBBA is a tool which was developed by VBA with support from VHA. IBBA accesses VBA's key benefits information systems. It works through a standard web browser on any personal computer (PC) connected to the internal VA communications system. Inquiries are sent through the system, through a security application and routed to the appropriate database. A snapshot of the requested information is taken and returned to the browser screen. Appropriate personnel in each of VA's Administrations and the Board of Veterans' Appeals were given access to IBBA in a phased approach during June, July and August, 2000. VA is starting to build One VA with IBBA.

CONCLUSION

Mr. Chairman, we know that we have problems. We know that we are not where we need to be, particularly in the areas of IT Security and our IT Architecture; but we are making progress toward One VA.

Mr. Chairman, that concludes my statement. My colleagues and I will be happy to respond to any questions you may have.