AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

INFORMATION TECHNOLOGY AT THE VA

HEARING

BEFORE THE

SUBCOMMITTEE OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 26, 2002

Printed for the use of the Committee on Veterans' Affairs

Serial No. 107–41

U.S. GOVERNMENT PRINTING OFFICE

91–753PDF WASHINGTON : 2004

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

COMMITTEE ON VETERANS' AFFAIRS

CHRISTOPHER H. SMITH, New Jersey, *Chairman*

BOB STUMP, Arizona
MICHAEL BILIRAKIS, Florida
TERRY EVERETT, Alabama
STEVE BUYER, Indiana
JACK QUINN, New York
CLIFF STEARNS, Florida
JERRY MORAN, Kansas
HOWARD P. (BUCK) McKEON, California
JIM GIBBONS, Nevada
MICHAEL K. SIMPSON, Idaho
RICHARD H. BAKER, Louisiana
ROB SIMMONS, Connecticut
ANDER CRENSHAW, Florida
HENRY E. BROWN, JR., South Carolina
JEFF MILLER, Florida
JOHN BOOZMAN, Arkansas

LANE EVANS, Illinois
BOB FILNER, California
LUIS V. GUTIERREZ, Illinois
CORRINE BROWN, Florida
JULIA CARSON, Indiana
SILVESTRE REYES, Texas
VIC SNYDER, Arkansas
CIRO D. RODRIGUEZ, Texas
STEPHEN F. LYNCH, Massachusetts
RONNIE SHOWS, Mississippi
SHELLEY BERKLEY, Nevada
BARON P. HILL, Indiana
TOM UDALL, New Mexico
SUSAN A. DAVIS, California

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

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

STEVE BUYER, Indiana, *Chairman*

BOB STUMP, Arizona
MICHAEL BILIRAKIS, Florida
TERRY EVERETT, Alabama

JULIA CARSON, Indiana
BARON P. HILL, Indiana
TOM UDALL, New Mexico

CONTENTS

September 26, 2002

	Page
Information Technology at the VA	1

OPENING STATEMENTS

Chairman Buyer	1
Hon. Julia Carson	2
Hon. John Boozman	4, 10

WITNESSES

Gauss, John A., Assistant Secretary for Information Technology, Department of Veterans Affairs, accompanied by Bruce A. Brody, Associate Deputy Assistant Secretary for Cyber Security, and Frank A. Perry, Chief Technology Officer	13
Prepared statement of Dr. Gauss	75
Griffin, Richard J., Inspector General, Department of Veterans Affairs, accompanied by Michael Slachta, Jr., Assistant Inspector General for Audit	5
Prepared statement of Mr. Griffin	30
Willemssen, Joel C., Managing Director, Information Technology Issues, General Accounting Office, accompanied by Valerie Melvin, Assistant Director for Accounting and Information Management Issues	6
Prepared statement of Mr. Willemssen	34

MATERIAL SUBMITTED FOR THE RECORD

Article in *Federal Computer Week* entitled, "VA restructuring IT management," April 12, 2002, submitted by Chairman Buyer	27
Written committee questions and their responses:	
Chairman Buyer to Department of Veterans Affairs	83
Chairman Buyer to U.S. General Accounting Office	90

INFORMATION TECHNOLOGY AT THE VA

THURSDAY, SEPTEMBER 26, 2002

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

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

Present: Representatives Buyer, Boozman, and Carson.

OPENING STATEMENT OF CHAIRMAN BUYER

Mr. BUYER. Subcommittee on Oversight and Investigations of the House Veterans' Affairs Committee will come to order on the 26th of September, 2002.

The record shall note that Ms. Carson will be here shortly, and that I will go ahead and proceed with opening statements.

I will permit her to make a statement when she arrives and yield her sufficient time. And if she does not arrive, we will proceed with the record. She has all of your statements. Your statements will be submitted for the record. I will proceed with my opening statement.

Today, this subcommittee will hold its fourth follow-up hearing on the Department of Veterans Affairs information technology programs.

The VA has made considerable progress addressing the IT concerns of the delivery of benefits to our nation's veterans and their dependents. Secretary Principi has led the VA towards a clearly defined strategic plan that integrates the planning, funding, project execution, and project management oversight of the VA information technology. The Secretary's action in this area is a welcome step that I believe is long overdue.

Over the past decade, we in Congress have authorized and appropriated hundreds of millions, literally billions of dollars, to be invested in the VA's IT systems. Unfortunately, little has come from this significant expenditure to develop a one system architecture.

As Chairman of the Oversight and Investigations Subcommittee, I am particularly pleased that Secretary Principi has little toleration for unacceptable business practices that have characterized the VA's IT program over the past decade.

During our last hearing on March 13, I asked Admiral Gauss, and I am paraphrasing:

"You sit before us as an Admiral, a retired Admiral, in a position that you have no distinct line of authority. So I look at you and

say if I were in your position, how would I define my authority. I sure do not want my service to be purely pastoral."

I believe that hearing and the testimony, actually, the statements from my colleagues, and the possibility of proposed legislation to give the Admiral direct line authority, prompted Secretary Principi's decision to boldly reorganize the VA's information technology structure.

The Admiral now has the type of authority such a position warrants, and I thank the Secretary for his leadership. The mission of the VA's Enterprise Architecture is to develop and implement a high performance, One-VA IT architecture that will support the VA's overall strategic goals.

This vision is clearly articulated in the VA's Enterprise Architecture Plan that was approved by Secretary Principi on September 5th of 2002. The VA's goal is to "Provide world class service to veterans and their families through the effective management of people, technology, processes, and financial resources."

The One-VA Enterprise Architecture outlined in a detailed report issued by the VA Enterprise Architecture Innovation Team in August 2001, is a marked departure from the historic failures of previous VA IT programs.

The primary difference is the VA now has a clearly defined plan. The Secretary knows that the failure to execute this plan in a timely and cost-effective manner is not an option. We are anxious to hear about the plans and how Dr. Gauss intends to execute the IT program to make it a reality.

There are several outstanding issues that need to be addressed immediately. In an article which appeared in the *Federal Computer Week* dated August 12th of 2002, Secretary Principi acknowledged there is resistance. There is a quote he has in this article:

"There is resistance to embracing the Agency's Enterprise Architecture and the implementation of cyber security initiatives is lagging." That is troublesome.

At our last hearing, we wanted to find out whether or not the VA is spending its IT money wisely. Obviously, we now know that it is not. Today's hearing will provide us with the VA's insight concerning recent changes made by the Secretary, and how this will enhance its ability to move forward with their IT projects.

We will also hear from the VA's Inspector General. He will share his findings concerning the VA's Information Technology Security Program. The GAO will round out the panels and provide us with a critical overview of the VA's progress in several key areas: Enterprise Architecture, information security, VETSNET, and the government computer-based patient record program.

Since the Secretary's goal of a One-VA is one that is shared by members of this subcommittee on a bipartisan basis, we will continue to monitor VA's progress in achieving this important objective.

I now yield to Ms. Carson for any opening comments she would like to make.

OPENING STATEMENT OF HON. JULIA CARSON

Ms. CARSON. Thank you, sir. Thank you very much, Mr. Chairman.

I would like to welcome our panelists and guests at this hearing. For many of you, it is a return visit from our March 13 hearing on this same subject. Much has happened in the past 6 months regarding the VA's approach to managing its IT. Much has happened from a change management perspective.

At our March meeting, the VA IT experts doggedly defended their existing system for flexibly managing the tremendous IT portfolio of "One-VA." Central to these management flexibility protocols was the fact that neither the Chief Information Officer nor the Chief of Sovereign Security Executive had direct line authority over any IT managers in the field.

There were dotted lines on the organization chart where there should have been solid lines. Many on this dais, and several expert witnesses, questioned the adequacy of what some saw as IT management by gentle persuasion. Our concerns initially sprang from disheartening data involving the lack of training accomplishments of information security officers in the Veterans Benefits Administration. Without centralized IT leadership, only 40 percent had completed the short online training program one year after being directed to do so. The program takes between 5 and 20 hours to complete. Why was there no sense of urgency to complete training?

Both the IG and the GAO had pointed out problems with VA information security. We did not have long to wait for the next indicator of a problem. This one in my hometown, Indianapolis, Indiana, came to light in May of this year. VA had released sensitive information about veterans, including Social Security numbers, credit card numbers, and specific and personal medical information.

It appeared that the folks in the field were not taking the folks at the Central Office seriously about IT security. A high percentage of IT security folks were still in training status, and guidance papers for dealing with IT were flooding the field from many directions. Everyone wanted a say.

On May 21, I wrote to the Secretary and very strongly indicated my displeasure with VA's lack of centralized IT control for cyber security. I am so pleased the Secretary heard my message. On August 6, he and Admiral Gauss took powerful and warranted steps to align vital IT functions and give the VA Central Office the authority to reasonably oversee IT in the field.

I am fully aware that this sea change in IT management was a painful decision. It is sometimes easier to criticize from outside the system than to act within the system. Your change actions altered the culture, and that took courage, and I applaud you.

Obviously, you need time to find your feet and catch your bearings under your new IT management system. From an organizational management perspective, I think it is inappropriate to question IT management system accuracy at this time. But I wish to better understand the past and where the cyber experts believe the department is heading with regards to IT.

Since it has only been 22 days since the Secretary approved the VA's Enterprise Architecture, Version 1.0, we will give you some time and wish you Godspeed to succeed.

I would like to open the door into one specific area of interest today, more to broach the topic and to get background information

than to open a full investigation today. VA has several failed IT projects that can be likened to skeletons in its collective closet. We have heard of the setbacks of VETSNET, and today wish for a progress report. Least known, but in some ways more troubling, is a system known as "HR Links." My colleague, Mr. Evans, has received a letter from IG. Upon their second review, it seems that no one was accountable for the failed HR Link System. Mr. Griffin, the VA IG, states in his 30 August 2002 letter, "Clearly, there was a lack of oversight and accountability of project management." For a failed system with a quarter of a billion dollar price tag, that is not acceptable.

Today, under new IT management, VA is embarking on new solutions regarding changes to the IT portfolio. While this is happening, the provisions of Clinger-Cohen must be met, milestones established and met. And someone must keep one eye on finances. Contracts for IT must assure our taxpayers a bang for their dollar. I am interested in how this will work under the new "One-VA."

And, Mr. Chairman, I would yield back the balance of my time. And thank you very much for your patience in listening to my concerns.

Mr. BUYER. Mr. Boozman.

Mr. BOOZMAN. I do not have any questions. I just want to thank you and the ranking member for convening the meeting today, and really look forward to the testimony.

Mr. BUYER. Thank you. I would like to recognize some visitors we have in the audience here today from Russia. With us today is a delegation from the Russian Duma, and you are here to learn about our veterans' programs, legislative process, and how the oversight committee in fact works.

With us is Mr. Igor Ligachev. Please stand. Thank you, sir. He is the Deputy Chairman of the Committee on Veterans' Affairs within the Russian Duma. We have Mr. Valeri Dorogin and Mr. Ivan Zakharov. Thank you, gentlemen, for being with us today.

I have had the distinct pleasure of visiting St. Petersburg and Moscow. I have worked with the Defense Committee within the Duma, and have visited the White House within Moscow. It was a very enlightening experience.

We began to lay down, in 1993, cooperative agreements to begin a mutual destruction of chemical munitions. And I am most hopeful that our continuing relationship on that issue with the Nunn-Lugar dollars will continue. And I appreciate your leadership on the issues of weapons of mass destruction and non-proliferation.

We were allies in World War II. There was great sacrifice by Russia, by your people, not just your men in arms and women, great sacrifice. It was unfortunate that we had parted ways for 40 years, and had a standoff and viewed ourselves as enemies; and that was unfortunate, at great cost not only unto the former Soviet Union, but also unto our own country.

As we now stand as leaders of a new century, I welcome you here to the United States. We welcome your openness, as you also welcome us to visits of your country. I believe that as each of us seek the greater understanding and wise tolerance, we, as two countries that can help lead the world to an everlasting peace, that will be the shining example of our efforts.

So I appreciate your being here today, and please pass on to your veterans our appreciation from World War II, and as we move in concert to bring peace into the world. Thank you.

To our panel today, I would like to recognize Mr. Joel Willemssen, Managing Director, Information Technology Issues of the U.S. General Accounting Office; Mr. Richard Griffin, the Inspector General of the Department of Affairs.

Mr. Slachta, nice to see you back. We are working you overtime, I think. And, Ms. Melvin, also, is with us, she is with the GAO.

Mr. Griffin, you may proceed. You are recognized for 5 minutes.

STATEMENT OF RICHARD J. GRIFFIN, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY MICHAEL SLACHTA, JR., ASSISTANT INSPECTOR GENERAL FOR AUDIT; AND JOEL C. WILLEMSSEN, MANAGING DIRECTOR, INFORMATION TECHNOLOGY ISSUES, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY VALERIE MELVIN, ASSISTANT DIRECTOR FOR ACCOUNTING AND INFORMATION MANAGEMENT ISSUES

STATEMENT OF RICHARD J. GRIFFIN

Mr. GRIFFIN. Thank you, Mr. Chairman.

Mr. Chairman and members of the subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs Information Technology Security Program.

Since our March 13, 2002, testimony to the subcommittee, we completed a second national audit of VA's IT security program. The audit found that the Department has a number of initiatives in process which, if fully implemented, will improve VA's information security posture.

A few examples of key department actions include: Establishment of a VA-wide security plan and the required policies, procedures, and guidelines mandated by the Government Information Security Reform Act; implementation of a VA-wide anti-virus protection; staffing of information security officer positions; and centralization of the Department's IT security program under the Office of the Chief Information Officer.

Although progress has been made, much work remains to implement key IT security initiatives, establish a comprehensive integrated VA-wide security program, and fully comply with the requirements of the Government Information Security Reform Act.

Penetration testing completed during the past 2 years verified that VA's information system could be exploited to gain access to sensitive veteran health care and benefit information. In response to last year's testing, the Department strengthened security controls at the facilities where we conducted our testing. During this year's follow up testing at these same sites, the security control measures established prevented our external penetration attempts.

However, continuing automated system control vulnerabilities allowed our internal penetration testing to gain access to sensitive veteran benefit and health care information. The vulnerabilities exploited this year were present during our previous testing a year ago.

The Department has not taken appropriate corrective action to eliminate these vulnerabilities in response to last year's findings. The nature and number of vulnerabilities found warrant immediate attention to reduce the significant exposure and high risk of an internal attack.

The Department's administration and staff offices have individually managed and controlled their Information Security Program activities. Our security assessment results show that this decentralized management approach has not worked.

Many security vulnerabilities identified in last year's audit remain unresolved, and additional security vulnerabilities were identified this year. The Department's decentralized management approach to information security impeded the Department's ability to successfully strengthen its overall security posture.

We met with the Department CIO on July 22, 2002, and advised that we would be recommending that the Secretary centralize authority for the implementation of security remediation efforts to the CIO's office. This centralization of authority would include management and decision authority on all Department security remediation efforts.

We had previously recommended centralized oversight in a prior year's audit. On August 6, 2002, the Secretary issued a memorandum centralizing the Department's IT Security Program including authority, personnel, and funding in the office of the Department's CIO effective October 1, 2002.

Based on the results of our second annual audit of VA's IT Security Program, we made several recommendations to the Department's CIO, to include the following actions: (1) install intrusion detection systems nationwide; (2) complete infrastructure protection actions; (3) complete data center contingency planning; (4) complete certification and accreditation of VA systems; (5) upgrade or terminate external connections; (6) eliminate vulnerabilities in the application program and operating system change controls; (7) control physical access to computer rooms; and (8) identify budget resources necessary to accomplish VA's priority security remediation efforts in the next 12 months.

In addition, the CIO must require the administrations to correct identified security vulnerabilities at their facilities and data centers, improve security awareness at the operating level, and highlight the need to assure compliance with existing VA information security policy, procedures, and controls.

In deference to our Russian visitors, there is an expression, doveryai, no proveryai, which means trust, but verify. The Department has an excellent plan in place. We will continue to verify that the implementation of that plan occurs and occurs timely.

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

Mr. BUYER. I now yield to Mr. Willemssen, the GAO. I don't want to interrupt the testimony.

STATEMENT OF JOEL C. WILLEMSSEN

Mr. WILLEMSSEN. Thank you, Mr. Chairman, ranking member Carson, Congressman. Thank you for inviting GAO to testify today.

As requested, I will briefly summarize our statement on VA's progress in addressing key information technology challenges since we last testified before you in March.

Over the past 6 months, VA has demonstrated clear progress and made important strides in improving critical IT areas. For example, the Secretary's recent announcement on realigning the Department's IT structure can set the stage for improved performance.

Although yet to be finalized, the Secretary's decision to centralize IT functions, programs, and funding under the Department-level CIO, Dr. Gauss, can improve accountability and enable the Department to truly implement and deliver on its One-VA vision.

Further, the additional oversight that is provided to the CIO could positively influence VA's ability to more effectively capture and manage its IT investments. VA also continues to make great progress in developing its Enterprise Architecture, which is its blueprint for evolving its information systems and developing new systems.

Secretary Principi recently approved the initial version of VA's Enterprise Architecture focused on defining the Department's as-is or current environment and its desired or to-be, target environment. At the same time, VA still needs to complete some critical actions to successfully complete this endeavor.

Among those actions, it needs to select a permanent chief architect, and needs to establish a program office to facilitate, manage, and advance the architecture. In another critical area, VA's information security continues to be of significant concern, but the Department is making progress in strengthening this program.

Included among the actions it has taken is an expansion of Department-wide incident response and analysis capabilities and monitoring and detection activities. Nevertheless, VA has not yet established a comprehensive computer security management program that would include, among other things, routinely monitoring and evaluating the effectiveness of security policies and controls. Further, VA lacks an independent component to ensure validation of the corrective actions taken.

Compared to the organizational accountability and control in Enterprise Architecture, the Department has not yet made as much progress in addressing the challenges associated with the replacement of compensation and pension payment system; VETSNET is the replacement effort.

Now to its credit, the VA is acting to improve accountability, validate requirements, and focus on testing of the replacement system. Nevertheless, after more than 6 years of effort, full implementation of this system is not envisioned before 2005.

This means that more than 3 million compensation and pension benefits payments that VA makes each month will continue to depend on an aging system that will need additional maintenance to ensure continued accurate processing of payments.

Finally, with regard to the government computer-based patient record initiative intended to share patient health data, VA and the Department of Defense have made progress on this, as part of a substantially revised, scaled down strategy.

As part of this new strategy, staff in VA medical facilities throughout the country now have access to defense health data on

separated service members. Two-way exchange of such information between DOD and VA under the revised initiative is now planned for 2005.

That summarizes my statement, and we would be pleased to address any questions you may have. Thank you.

[The prepared statement of Mr. Willemssen appears on p. 34.]

Mr. BUYER. This line of "Concurrent with this effort, Department-wide IDS, the intrusion detection systems capability will be incrementally deployed on a strategic basis to provide significantly increased security protections for these gateways."

I'm sorry. But my intellect is being challenged. Help me out.

Mr. GRIFFIN. I'm sure Dr. Gauss can give the one hundred percent response to that, but I think it is a combination of prioritizing the order in which you address weaknesses based on the greatest threat, but also considering available budget dollars.

Mr. BUYER. I am going to ask Dr. Gauss, but I'm just curious. I mean you have got to read the same stuff I do.

Mr. GRIFFIN. I read that and I——

Mr. BUYER. "On a strategic basis," what does that mean? Is this bureaucratic wordspeak, or what is it?

Mr. GRIFFIN. Well, I think you have to have a strategic plan and you have to decide, "Okay. Where is our greatest vulnerability? And we need to fix that first."

Mr. BUYER. All right.

Mr. GRIFFIN. But that is just my read of the language there. I am sure Dr. Gauss——

Mr. BUYER. All right.

Mr. GRIFFIN (continuing). Will speak eloquently about it.

Mr. BUYER. Were you a punter in football?

Mr. GRIFFIN. No, I just do not like to speculate with someone else's words.

Mr. BUYER. You know what? That is what we have to do. We have to interpret words. We have the author here, and I am going to ask him.

Mr. GRIFFIN. Right.

Mr. BUYER. But I was just curious what you thought.

Mr. GRIFFIN. Well——

Mr. BUYER. You have been deep into this stuff. I am not here to put you on the spot or——

Mr. GRIFFIN. No, I understand.

Mr. BUYER. All right. Mr. Griffin, in your opinion, what should VA be doing right now to shore up its vulnerabilities relating to outside penetration?

Mr. GRIFFIN. They need, as I just mentioned, to establish their priorities based on the greatest known vulnerabilities. As I mentioned in my testimony, there were sites that we had penetrated last year during our audit which we went back and retested this year.

So those particular sites that were demonstrated to have been vulnerable a year ago were made priorities, and the proper protections were put in place to preclude external penetration. That is something that needs to be implemented.

Mr. BUYER. What barriers are present for the implementation of these external system protections?

Mr. GRIFFIN. I think it is a combination of factors. Certainly, budget is a one consideration . How much money is going to be available to do these things immediately? Each year we identify and prioritize those things that we think need to be addressed in the next 12 months. That is the basis for the list that we have provided in our written testimony.

As you suggested, there needs to be compliance or a buy-in from all of the people in this huge decentralized department to the fact that the Secretary has decided we are going to have centralized control.

The Secretary has directed that we will have ISOs at every facility; and ISOs, Information Security Officers, not just in title, but people who have been properly trained to perform their mission, and who understand the Department's policy and will make sure it happens at their facility.

Mr. BUYER. The GAO, on page 19 of your testimony, you state that, "The VA must also still develop a program management plan to delineate how it will develop, use, and maintain, the Enterprise Architecture." You further state that, "Such a plan is integral to providing a definitive guidance for the effective management of the Enterprise Architecture Program."

And I guess I am confused because, according to Dr. Gauss, they have developed and will implement a version 1.0 of the One-VA established—which establishes ten enterprise business functions and seven key enabling functions.

Don't these business and enabling functions provide the management tools necessary to start the process for implementing the VA's Enterprise Architecture?

Mr. WILLEMSSEN. They do, in part, provide the tools. And I would commend VA on its excellent effort in putting together that initial architecture. But in order to be an effective architecture, it has got to be something other than a document in a binder. It must be implemented.

To do that, among other things, you need a chief architect. You also need a program management office that is going to implement the architecture and enforce it so that, among other things, when a particular entity, for example, wants to develop a new system, the office is there as a control and a check, "Does this map to the architecture, the direction we want to head?"

So, again, I commend VA on an excellent effort in putting the architecture together. But now, from this point forward, in addition to getting into more details about, VA is going to have to implement it and make it happen, and make it be more than just paper.

Mr. BUYER. Did you get any feedback from the VA relative to this testimony and recommendation?

Mr. WILLEMSSEN. In fact, our recommendations, our outstanding recommendations in today's testimony are consistent with the long list that we provided to VA back in March. And in talking about this with Dr. Gauss, in all of the areas we have not met any resistance.

I would say the biggest hurdle that Dr. Gauss has right now is time. I think they have made great progress over the last 6 months but they still have a lot of things to do. He and I have talked about not only having the road map that we have laid out in the Enter-

prise Architecture and information security areas, but now the next step is let's put some timelines and milestones on those tasks that he feels he can be held accountable to.

I think that would be an excellent step in the right direction.

Mr. BUYER. That is good counsel.

Mr. Boozman, you are recognized for 5 minutes.

Mr. BOOZMAN. In your testimony, you talked about penetrating, you know, the system. I know there is patient records. There is benefits and things like that.

I mean what—have we had problems like that in the past of—as far as benefits that were not supposed to be paid?

Or, I guess what I am asking is, if somebody penetrates the system, what—are we talking about stealing patient records? Are we talking about—what is the downside?

Mr. GRIFFIN. Well, there is risk on both the VBA and VHA side of the house. In VHA, the risk is access to privacy-protected medical records.

And in today's world, where identity theft is unfortunately a fairly prevalent activity, by being able to gain all of the identifiers for a person, it is fairly simple to establish yourself under their identity and perpetrate any number of different types of fraud.

On the benefit side a person could access the system and generate unauthorized payments to fictitious payees.

Mr. BOOZMAN. Has that been a problem? I mean is that something that we know about, or——

Mr. GRIFFIN. Well, that is something we demonstrated that that could be done. We have had some criminal cases the past couple of years that involve people manipulating the benefits delivery network to issue checks in the names of the people who had died many years ago, and so on.

So it is a problem. Although, we have not had a massive number of incidents, the capability exists.

Mr. BOOZMAN. Right. You said that we had done better as far as the external penetration, that the tests were good there. The internal, we are still lacking.

What kind of timeframe do you feel like would be adequate to get that squared away?

Mr. GRIFFIN. Based on our successful penetration and manipulation in the benefits arena, I think that needs to be a high priority. Whether that can be accomplished in the next 12-month time period, I am not certain.

Mr. BOOZMAN. Okay, very good. Thank you.

Mr. BUYER. I ask unanimous consent to permit the counsel for the minority to ask questions. Hearing no objection, so ordered.

Mr. SISTEK. Thank you very much, Mr. Chairman. I have two quick questions about management controls under One-VA. The first question I will ask to Mr. Griffin. You are familiar with the new plan for centralized cyber security. My question to you is: Does that plan have adequate reach to the field? Is there an adequate feedback loop established between the furtherest reaches of the field and the Central Office regarding cyber security oversight enforcement reporting?

Mr. GRIFFIN. As you know, this plan has just been promulgated in the last 30 days. I know that the administration CIOs have been

given the title of deputy under Dr. Gauss's purview. And there is a plan that will reach into the facilities down to the ISO level.

I know there has been a first ever meeting of the security officers, independent of their respective facility directors, who they had always taken their marching orders from in the past.

Again, a plan has been crafted, but the proof will be in the follow up to make sure that appropriate reporting requirements are in place, and that the people in the field realize that this is not a policy to put on the shelf never to be heard from again. It has got to be rigidly enforced.

Mr. SISTEK. Thank you. This question would be for either the IG or the GAO. And, again, it is about management accountability.

There was a system that has recently been discontinued called the HR Links System. And I understand that both the IG and GAO are somewhat familiar with this system. We believe that there may have been inadequate oversight of the HR Links System while it was in production.

What safeguards are now in place under the One-VA Enterprise Architecture to prevent any similar oversights, any similar lack of management control?

Mr. GRIFFIN. I think the centralization move is probably the key move in order for there to be accountability at the headquarters level. This ensures you won't have 160-some medical centers, and 58 ROs, and a number of cemeteries picking and choosing hardware, software, and systems that they might have a bias for locally.

From the accountability standpoint—and HR Links, which went on for several years, there were initially two different people serving as co-leaders of the initiative. The baton got passed several times.

I think there were promises made regarding the capabilities of some of the software, which turned out not to be legitimate claims as to the volume they could process. They eventually learned that the programs would not handle the VA's processing volume.

Mr. SISTEK. You are comfortable that such a set of problems would not—you could not construct a similar set of problems under the new Enterprise Architecture because of the centralized authority?

Mr. GRIFFIN. I think the centralized authority is key. But not to lose sight of the requirements and the fact that we are going to be doing annual audits, and that GAO is also going to be looking at this activity.

My people, who work in the IT security area, are working very closely with Dr. Gauss's people. Everybody knows what the mission is, they know that we are going to be monitoring progress and determining whether things are being accomplished timely.

I think there is a good working relationship from the standpoint of our oversight and their mission requirements.

Mr. SISTEK. Thank you. Mr. Willemssen, do you have any insights into this?

Mr. WILLEMSSEN. Yes, what I would add to that is that a key control that Dr. Gauss is planning to put in place is with his new responsibility for direct oversight of the one billion plus in IT funding. He is going to be asking for specific spend plans from each of

the administrations, so that he will now have something that prior CIOs have not had—he will know where the money is being spent.

That has not been the case in the past. I can recall testimony I gave before the subcommittee a couple of years ago, where a question was asked about how much money is being spent. The question could not be answered. With this organizational setup, and with his plans.

VA will have got a mechanism and procedures set up where he will have that insight to where the money is being spent and what is being successful, and what is not being successful. And when it is not being successful he will be in a position to cut the project.

Mr. SISTEK. Thank you very much. I yield back. Thank you, Mr. Chairman.

Mr. BUYER. I am going to be asking Dr. Gauss this question. But I am curious about whether it is the software or hardware manufacturers out there; or whether it is relicensing issues.

In a tough economic time, I can understand how some companies might want to fight to hold on to what they have, for whatever short-term, and not see the horizon, and what benefits can be there later on.

Have you noticed anything out there where companies have not been at all cooperative?

If you don't know, just say you don't know, and I will get into this with Dr. Gauss.

Mr. WILLEMSSEN. Nothing comes to mind at this point, Mr. Chairman.

Mr. BUYER. All right. I will have follow-up questions that I will submit for the record. And I appreciate your testimony and the work—not only yours, but that of your staff. Thank you for your testimony.

Mr. WILLEMSSEN. Thank you.

Mr. GRIFFIN. Thank you, Mr. Chairman.

Mr. BUYER. I now recognize Panel 2, Dr. John Gauss, Assistant Secretary, Veterans' Affairs for Information and Technology. I ask you, Admiral Gauss, do you like going by Admiral or Doctor, or Secretary, or what do we call you?

Mr. GAUSS. Mr. Chairman, the reason I have put my former military title aside is that when Omar Bradley was the head of the Veterans Administration, he had a policy that senior officers should put their titles aside, since there were so many veterans who were working at the VA. And I chose to honor that tradition. And since I had another title that had been suppressed for 32 years, I decided to resurrect it.

Mr. BUYER. Doctor, okay. How about Secretary?

Mr. GAUSS. Yes, sir, that would work, too.

Mr. BUYER. Dad is the best title, though, isn't it?

Mr. GAUSS. Sir?

Mr. BUYER. Dad is the best title. That is what I have found.

Dr. Gauss, Secretary, Admiral, you are now recognized for 5 minutes.

STATEMENT OF JOHN A. GAUSS, ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY BRUCE A. BRODY, ASSOCIATE DEPUTY ASSISTANT SECRETARY FOR CYBER SECURITY, AND FRANK A. PERRY, CHIEF TECHNOLOGY OFFICER

Mr. GAUSS. Thank you, Mr. Chairman, and members of the subcommittee. On behalf of the Secretary of Veterans Affairs, I am pleased to have this opportunity to come here today and update you on the progress the Department has made in strengthening our information technology program, and specifically address issues related to VA's Enterprise Architecture, our cyber security program, the recent realignment of the Department's IT structure, and issues raised at the March 13 hearing.

Since my testimony is quite lengthy, I would like to summarize it in my opening statement. On March 13, I appeared before this subcommittee and gave you my personal commitment to reform the way VA uses information technology.

I committed to publishing an approved Enterprise Architecture Implementation Plan by April 30. The plan was published on April 22nd. I committed to ensuring that our networks and systems we depend upon are made secure and available. These efforts are in execution.

I committed to personally overseeing VETSNET to ensure its progress meets the projected time of being ready to deploy by April of 2004, or recommending to the Secretary that the effort be terminated.

In my written testimony, there are details that support the actions that we have taken on VETSNET. The Undersecretary of Benefits and I have recommended to the Secretary that he continue in fiscal year 2003, since I believe they are on a glide path to be ready for deployment by April of 2004.

And, finally, I committed to conducting the deployment review for the Government Computer Patient Records Program to ensure a quality product could be effectively deployed. The review was held on April 26. The product was successfully deployed between May 27 and July 17 of this year.

With respect to GCPR and the other issues that had been identified in the GAO reports, I believe we have satisfactorily addressed all remaining issues as addressed in my written testimony.

With respect to Enterprise Architecture, the Secretary approved version 1.0 on September 5. It provides a clear pathway for the transition of both business processes and information technology across the Department.

Additionally, staffing has been approved for the Enterprise Architecture Office to include a Senior Executive Service Chief Architect. Recruitment for those positions is underway. Further detail relating to the Enterprise Architecture efforts are contained in my written testimony.

To correct our data network deficiencies discussed in the March 13 hearing, we are executing a four phase project to re-architect our data network. That effort is underway, in execution, and details are in my written testimony.

With respect to cyber security, the Department has made significant progress in correcting deficiencies identified by the Office of the Inspector General and the General Accounting Office.

This year, the Department fielded one of the largest anti-virus capabilities in the world, which protects over 140,000 desktop computers connected to VA's intranet from malicious attack. To date, over 2 million viruses have been successfully detected and eradicated.

In July, a multi-year contract to significantly upgrade the capabilities of our VA central incident response capability was awarded. This enhanced capability will provide such global services as firewall and intrusion detection management, vulnerability assessment done by our office, and penetration testing done by our office.

In addition to the anti-virus and incident response capability efforts, the Department is continuing to deploy other specifically focused initiatives that have been developed over the past 6 months to correct IT security weaknesses.

These programs include our Enterprise Cyber Security Infrastructure Protection Program, and our newly established Cyber Security Professionalization and Compliance Programs. Details of these three programs are contained in the written testimony.

In a memorandum signed by the Secretary on August 6, he directed that all IT personnel and resources be centralized under the Office of the Chief Information Officer. The first action I took was to assign the administration chief information officers to become Department Deputy CIOs for Health, Benefits, and Memorial Affairs.

Also, the senior IT manager in each VA Central Office staff office that operates or maintains IT networks and equipment now report to me. Initially, I focused on establishing a clear unambiguous reporting chain for the Department's cyber security efforts.

We have developed an organizational structure that combines the cyber security staff elements of the administrations with the Central Office's cyber security staff, thereby creating a single integrated cyber security program office for the Department.

Further, information security officers at the VHA VISN level, and at the VBA network service center level will become direct reports to the Office of Cyber Security early next fiscal year.

Within each hospital regional office and cemetery, the ISOs will report directly to their respective facility director rather than the inconsistent manner of reporting of the past.

In order to further consolidate, align, and properly staff our IT organizations, I have convened a group of senior leaders from the Department to develop a detailed reorganization package to submit to the Secretary by no later than November 1.

I hope I have provided some insight as to the progress that has been made since the March 13 hearing. I believe these efforts demonstrate our very strong commitment at all levels to build an effective information technology program to meet the Department's and our veterans needs for the long-term.

With your assistance, we will be able to continue on this path to assure our continued ability to service our veteran population and their dependents. Thank you for this opportunity to discuss these very important issues. I will be happy to answer any questions.

[The prepared statement of Dr. Gauss appears on p. 75.]

Mr. BUYER. Secretary, what specific quantifiable commitments is the VA willing to make to the subcommittee on a full scale implementation of the One-VA architecture, and how long will it take, and how much will it cost?

Mr. GAUSS. Mr. Chairman, with the publishing of version 1.0, we have identified the key business functions and key enabling functions for the Department and decomposed them into their subfunctions. Version 1 was not able to define the entire "to be" future of the Department; rather, it focused on seven key areas.

Within those seven key areas we can commit to having our networks modernized, which was one of the seven key areas, by September of 2004. We can commit to having our enterprise Cyber Security Infrastructure Protection Program completed by September of 2004, and fully implemented.

Mr. Chairman, when we dissect that program, it is possible folks would say, "Well, why are you waiting until 2004?" That is the absolute latest date, and we will try to accomplish it much, much sooner than 2004.

We have in our 2004 budget——

Mr. BUYER. Excuse me.

All right. Go ahead.

Mr. GAUSS. We have in our 2004 budget's submission request to the Office of Management and Budget the requested dollars for initiating new projects focused on consolidating the eight different ways that we register veterans and determine their eligibility, to consolidate the five different ways that veterans can seek help on the processing of their benefits claims and for medical care from five processes to one. If approved those projects will start with some seed money in 2003, and start for real in fiscal 2004.

The Department can also commit to completing the management plan that the General Accounting Office talked about over the next 6 months and continue the evolution of that architecture to expand it to include the "to be" structure for other business areas in an upgrade mid-year and final version 2.0 late in the spring.

Mr. BUYER. Thank you. Mr. Boozman, do you have any questions? You are recognized for 5 minutes.

Mr. BOOZMAN. I guess I just have a quick comment, and maybe you can comment on it. You know this problem just seems to be central. And I think homeland security has brought it out that we have a real problem because of the fact that, you know, our computer technology is changing, and this and that, that our agencies aren't able to talk to each other. And they are certainly not doing a good job of communicating with, you know, among themselves.

Mr. BUYER.But I guess my question is we are spending all of this money. You know, we have sent a man to the moon. You know, we have done all of these things. I just don't understand why we can't get this fixed, in the sense that it seems like we almost, at this point, almost need a national initiative, you know, where we step in and focus not just for your agency, but all of these agencies and try and get a system that the government can use systemwide because you all have got the same problem.

Mr. BUYER.See what I am saying?

Mr. GAUSS. Yes, sir.

Mr. BOOZMAN. Much like, you know, like the NASA Program, again, you will fix that effort for us. I really see that we need some intervention. We are spending an awful lot of money among all of these agencies. And, again, as the technologies change and staff, you know, that still does not guarantee that we are going to be able to talk to each other.

Mr. GAUSS. Yes, sir. We do spend a lot of money across government on infrastructure-related items. When I talk about data networks, that is the plumbing to make the information move, there is nothing exciting about the plumbing, but we spend far too much money on the plumbing.

If you are going to protect your data, and you are going to protect your applications, you really have to know what your plumbing is so you can put the protection for the movement of that information on it. But that is another infrastructure problem that is not glamorous.

And I agree with you, sir, that it is a far reaching problem beyond just the Department of Veterans Affairs. But being the largest civilian department in government with over 220,000 employees, we represent a large part of that problem. And that is why we are focusing on getting our network squared away, so we can in fact secure information and reduce the reported vulnerabilities from our Office of the Inspector General, and the General Accounting Office.

Mr. BUYER. Okay, thank you. Minority counsel is recognized.

Mr. SISTEK. Thank you again, Mr. Chairman.

Dr. Gauss, oversight of the ISO community under the new plan does not extend to all field level activities. In other words, an ISO at a medical center would not have direct line authority linked to either you or to your cyber security chief.

Do you think the current system is adequate and why?

Mr. GAUSS. I truly believe that by consolidating the headquarters cyber security programs into a single program for the Department, and having field representatives within the VISNs and within intermediate field structure for VBA, that we have the tools to provide the individual ISOs at the hospitals and regional offices with the direction, the oversight, and the inspection of their work.

As I stated in my testimony, we will be requiring weekly reports from those ISOs to the intermediate management areas that then go up to Mr. Brody's office for adjudication. There is an interesting trade space here, in terms of accountability.

Mr. SISTEK. Okay.

Mr. GAUSS. If we believe that the individual director should be held accountable for the mission, then the individual director should have the tools necessary to do it. The flip side says there is a potential conflict from an independence standpoint. But I think if we look at the alignment we had last March, to the alignment we will have come 1 October, we will make significant progress.

Mr. SISTEK. One quick question, different area, the finance process, how you finance and track IT projects in the VA is probably going to undergo a change as a result of your move to One-VA.

What would facilitate that? How else can that process be improved on? Would a separate budget, for example, be a useful item?

Mr. GAUSS. To answer the first part, we are requiring the submission of financial execution plans prior to the start of the fiscal year that outline in detail what is going to be done, who is going to do it, how much is going to be spent, and when it is going to be spent.

And I am pleased to report that I have already received the fiscal 2003 spend plans from all three administrations. And I am also pleased to report that the quality of the initial submission far exceeded my expectation.

Now we have some work to do. Some were better than others. Some had more data than needed. We will rebalance them between now and Christmas, but that is a financial control mechanism.

With respect to budget and budget authority, there is a lot that we do in IT that is common across the Department that might be appropriate for central funding, such as the core of the network backbone, the cyber security program to protect the infrastructure, investment capital to modernize our computing environment to transform from a facility-centric environment to a network-centric environment.

The eligibility and registration initiative to collapse eight processes to one; the national contact management process to reduce five to one; and, perhaps, core FLS. The rest of the money, in my view, should remain in the administration budgets to meet mission-specific applications and pay for the operation and maintenance of those applications unique to the administrations.

Mr. SISTEK. Thank you, Dr. Gauss. Mr. Chairman, I believe we will have some post-hearing questions along that vain. Otherwise, I am finished with questions.

Mr. BUYER. Secretary, I apologize. We have three votes. I anticipate the first is 15 minutes, and two 5 minute votes, so we probably have 6 minutes to go.

And because I have worked so hard to empower you, and I want to ensure that the Secretary's commitment to the One-VA Enterprise Architecture is successful, I have some questions for you.

Mr. GAUSS. Yes, sir.

Mr. BUYER. So I am going to recess the subcommittee and reconvene at 11:30.

Mr. GAUSS. Yes, sir.

[Recess.]

Mr. BUYER. The subcommittee will come back to order. Dr. Gauss, I want to ask a few questions on VETSNET, a program in which a lot of money has been invested. You know around here they like to say, "Well, it is a lot of money for pretend claims," and all kinds of sour jokes.

I mean I have no interest in beating you up. You know I could go through and say, "All right. How much money is spent? How is it benefitting the veterans?" Just can you give us a horizon here on VETSNET?

Mr. GAUSS. Yes, sir, I can. The development work that is left to complete deals with the financial module and the payment award module. And with those two modules complete, from a compensation and pension perspective, VETSNET will be ready to deploy and move the payment of compensation and pension checks off of the old Legacy BDN system.

At the last hearing, I committed to the committee to personally oversee and have the product delivered, a quality product delivered by April of 2004. We have built a comprehensive plan following the hearing. And over the past 6 months, every milestone in that plan has been executed.

We have a program manager assigned, who is now responsible and accountable for cost, schedule, and performance execution. Our plan included the validation and finalization of all requirements except for reports generation by September. That date was met.

The date that reports are due is by Christmas. On Tuesday of this week, the Undersecretary of Benefits and I jointly chaired a review of the health of this project. And we both believe and have recommended to the Secretary that we continue funding into fiscal year 2003.

We will hold another review in December, when the final piece of the requirements definition is due to complete and review the detailed progress of the program. The contractor is scheduled to deliver the developed product in the second—by the end of the second quarter of calendar 2003.

The reason that I want from the end of June to the beginning of April is to take the product, run it through a comprehensive functional test to be sure it meets all of its requirements, repeat the comprehensive stress test that was done last year, put it into an operational environment, and have the user community verify, validate that it is both effective and suitable, and at that point declare victory and ready to field.

And I have personally gone through this schedule. The Undersecretary has gone through this schedule. And we believe that realistically we can deliver a finished product ready to deploy with quality by April of 2004.

Mr. BUYER. Concerning the government computer-based patient records program, can you tell us what's been accomplished and who is presently in charge of implementation?

Mr. GAUSS. We have worked with DOD and defined VA as the executive agent for the project. We have assigned—last September, we assigned a dedicated project manager. Last September, we held a review of GCPR and baselined its schedule.

We set a second quarter of calendar year 2002 date to finish development and deliver the initial product. All of those dates were met. The first version is deployed in the field. We started deployment on May 27, and we finished deployment on the 17th of July.

As far as the future, we have a Memorandum of Agreement between the Deputy Secretary at VA, and the Undersecretary for Personnel and Readiness at DOD that maps out the future steps to be taken in that project. We believe that we have satisfied all of the recommendations that were in the June 2002 GAO report, as it relates to GCPR.

Mr. BUYER. How is this empowerment from the Secretary working?

Mr. GAUSS. It has been working well. The week after the memo was signed, we had a conference in Austin, TX, with predominantly the technical community, but there were folks from the administration headquarters present. And I can guarantee you that that memo got everyone's attention.

And the people in the field have been most cooperative in working with my office to do what is necessary to put the proper controls in place. It was the field that volunteered to draft the format for our financial execution plans.

So they formed a team; I worked with the team, and we came out with a template, published it, and 2 weeks ago I received VHA's spend plans that were very high in quality. I also have VBA and NCA's spend plans for fiscal year 2003. Since this is a new process, we will work our way through some of the bugs between now and Christmas.

But, overall, if you were to ask me do I know where the 2003 money will be spent, I can tell you today I have a very good idea and by Christmas I will be able to tell you I know exactly where it is being spent.

Mr. BUYER. Well, it appears by the editorial I read from the *Federal Computer Week*, that some of your counterparts CIO's are sort of jealous. They like your direct line of authority. They like your budgeting authority, and maybe this will become a model for other departments.

So I have a question. Is it Mr. Brody?

Mr. GAUSS. This is Mr. Bruce Brody. He is our Associate Deputy Assistant Secretary for Cyber Security. And on my left is Dr. Frank Perry, who is the Chief Technology Officer, and Acting Chief Architect. And it was Frank who led the 97 day effort to get version 1 of the architecture complete.

Mr. BUYER. Well, thank you for your work.

Mr. PERRY. Thank you, sir.

Mr. BUYER. I recall from one of the hearings we had with regard to security of your systems, you had more of a problem from internal than external. Is that still the case?

Mr. BRODY. Are you referring to the weaknesses of these systems or the accessibility of information?

Mr. BUYER. Yes, and penetration and privacy issues.

Mr. BRODY. Generally speaking, in most government agencies the predominant threat is from internal users. But after September 11, we determined that it was the top priority of the Department to protect the enterprise from external attack. And that is where we have been focusing our attention.

Mr. BUYER. Help me out here. Break it out. For whatever reason, I have this in my mind that the overwhelming concern with regard to security and breaches of privacy was from internal sources, and that was the degree of your problem.

So have you like shifted focus to the 20 percent, and not to the 80 percent of the problem, or is it a 60/40, 70/30?

Mr. BRODY. I am not sure of the exact percentages. What I can say is that in dealing with the internal threat, we have not been entirely negligent. We have put some controls in place. We have content monitoring, content filtering. We have intrusion detection systems. We have anti-virus and other malicious code detection measures in place.

We have a robust incident response and incident management capability. But where we have been dedicating a tremendous amount of focus since September 11 has been in protecting the boundary of the enterprise from external attack.

Mr. BUYER. September 10, 2001, major issue not only in this committee, but also the Health Subcommittee of Ways and Means, several different committees of the Energy and Commerce Committee was privacy. Privacy, that was the big issue prior to September 11, and I just want to reinforce that.

And, hopefully, you will place me in degree of confidence, Dr. Gauss, that while you work on the external, let's not forget about these issues. Okay?

Mr. GAUSS. May I add something here?

Mr. BUYER. Sure.

Mr. GAUSS. As we started to map out the blueprint of our networks, we found over 200 external connections to places outside of VA, and over 1,000 dial in accesses into VA. And we found that most of them were not protected. So, from a threat perspective, it was the entire universe including internal at the VA that could potentially violate and compromise our information technology systems.

So, from a risk management perspective, we viewed to put the protection on the external boundaries to reduce the threat from global to within VA. And, as the IG and the GAO had stated, we have come a long way in that external protection. And now we will focus on protecting against the internal threat.

Mr. BUYER. Well, this takes me to this sentence that confused me. When you talked about taking—that you were systematically going to collapse over these 200 existing structures on page 5, can you help explain what you meant by this, "Concurrent to this effect department-wide, IDS capability will be incrementally deployed on a strategic basis to provide significantly increased security protections for these gateways?"

Mr. GAUSS. Yes, sir. Mr. Chairman, I would like to apologize to members of the committee for the poor language that I chose in that sentence.

We will be setting up a pilot in January of 2003, that will demonstrate the hardened boundaries at our data centers and to the external world. Once we prove that it works, we are going to put it at two other locations in 2003. We do not have the sizing data to know if the three sites will hold—can handle the capacity needed to support VA.

If we find three is enough, we are done. If we find we need a fourth, or a fifth, or a sixth, so the intent of that sentence was meant to be, "We have a plan in place to put the initial capability. We are going to collect data, measure our ability to support the entire enterprise, and if we have to put a fourth, or a fifth, or a sixth, we will then do it at that time, migrate our networks into this architecture, disconnect the backsides, and put a very high security boundary from the outside, and inside where our key data is stored. We will then move to every facility within VA and provide protection everywhere."

Mr. BUYER. This goes to the question that I had asked the IG and the GAO relative to cooperations out there from vendors, companies. You have got many different forms of existing contracts, maintenance agreements, and the list goes on and on. So I want to know how cooperatively these companies are working with you or not working with you.

Mr. GAUSS. In my opinion, having worked with a large contracting base in my current and prior life, I really have not seen cooperation levels change that much as a result of the economy, which was part of what your question was to the IG and the GAO.

I am finding that I am not really seeing any change in how we deal with these folks. Now one of the benefits of having a chief technology officer is that we have somebody who can look deep into the technical offerings the companies are making to determine whether it is good stuff or not good stuff. A lot of VA's historical problem is that we have bought some things we probably should not have.

Mr. BUYER. Well, see, that is what we want to correct. We do not want all of these multiple different levels of purchases, different types of software. That is why we are coming to you.

Mr. BUYER. Yes, sir. Dr. Perry, can you—one of you—be able to tell us about this solicitation?

PCHS, is that what I hear it is called, this 1.2 billion solicitation?

Can you sort of break out what you are doing here with this and how it fits, one of you?

Mr. PERRY. It is an enterprise-wide contract for procuring commodity items and other IT specialty items. And through that it gives us an opportunity to gain additional controls over the acquisition process so that from an architectural perspective, and from a security perspective, we can assess the worthiness of products prior to putting them onto that acquisition vehicle.

And then, subsequently, whenever folks need to procure them, we do not have to reassess unless a new element comes along.

Mr. BUYER. Dr. Gauss, did you want to add something?

Mr. GAUSS. One of the important benefits of PCHS II is that it is a multiple award contract. And I am requiring every purchase made on that contract to be offered to all four primes to give them the fair opportunity to compete for the award. And that has given us very good price advantage.

So it is not just four companies who can go market their individual wares and charge what the market will bring. We put competition in place for every procurement. And, as Dr. Perry said, they were architecturally compatible. The products were architecturally compatible with where we head to the future.

Mr. BUYER. But there are not very many operating systems, right?

Mr. GAUSS. Yes, sir.

Mr. BUYER. I do not know how you are going to make these determinations of the least "responsive" bidder. You know if you say, well, we are going to go to four primes—and I am just saying I recognize some real challenges that you may have.

I have not always been a proponent of sole source contracting, but sometimes in some places there can be advantages to it. And, hopefully, you are exercising the good judgments.

If I were a medical director out there, and I want to upgrade my systems, maybe a server or (ers), maybe printers, my desktops, can I do it on my own or do I have to go through you?

Mr. GAUSS. First of all, you would have to identify it in your spend plan. Second, we have an IRM approval process where you would have to request approval to do it. And, third, you would be

required to purchase it off the PCHS contract. Now should you have a requirement that is not on the contract——

Mr. BUYER. And this is going to apply to everyone?

Mr. GAUSS. Everyone.

Mr. BUYER. So whether it is in the claims to—okay.

Mr. GAUSS. Now should you have a requirement that is not satisfied by the contract, then I would entertain a waiver to use a different contracting vehicle. But I expect waivers to be few and far between. I have granted one waiver so far since PCHS II has been awarded.

Mr. BUYER. So do you envision in the future that the VA would have—let's just take servers as an example.

Mr. GAUSS. Mm-hmm.

Mr. BUYER. That you would have servers come from one particular company, and that is who has that maintenance agreement?

We do not have multiple agreements out there with multiple vendors. We are going to have one.

Mr. GAUSS. We have four primes on the PCHS II contract, so they would come from one of those four vendors. We have had process control over those four.

Mr. BUYER. So you could still envision overlapping of different vendors, whereby, you have got some servers in use, and then a few years later, you might open up another solicitation and you are still going to end up with mixed systems?

Mr. GAUSS. Well, when you look at the basic technology of the server, you really have three operating systems to deal with. You have a Windows operating system from Microsoft; you have UNIX operating systems, which are kind of fading out of the market frankly; and you have LINUX, which is being introduced.

Windows operating systems run on chips produced by Intel Corporation. And so, whether you buy a Dell, or you buy a Compaq, or you buy another brand that runs Windows, you are running on a chip. And what is different is some of the interface drivers for the different peripherals.

I know this is getting down into the weeds, but the basic technology is the same, be it a Dell, be it a Compaq, or be it another vendor. So I do not see that diversely as being a big problem.

Mr. BUYER. As we seek to have more sharing agreements, and interoperability and connectivity between DOD and VA, if DOD is on a Microsoft system, and you are on a LINUX, would there be problems?

Mr. GAUSS. Let me ask Dr. Perry to address that question.

Mr. PERRY. At the network level, we could deal with those kinds of issues by dealing with messaging standards, and things like web services, to address those issues where I do have heterogenous platforms.

But, in several cases, Dr. Gauss talked earlier about the registration and eligibility. That is the second major effort that we are trying to do jointly with the Department of Defense, since when they register members, service members and their dependents in their benefit systems, that provides us with a golden opportunity to reuse that as an original source of information coming across.

And what we have agreed with the Department of Defense is to pursue the fiscal 2004 new start that Dr. Gauss talked about for

a One-VA registration and eligibility system jointly with the Department of Defense.

And, in fact, in that case, we have also agreed that we would use the same technology, and basically establish a single shared repository of personnel demographic information and bi-directional flow into and out of the repository from both DOD and the VA.

Mr. BUYER. All right. When you used the term "shared"——

Mr. PERRY. Shared repository.

Mr. BUYER. Huh?

Mr. PERRY. A shared repository for personnel—personal demographic information. Basically——

Mr. BUYER. No, that is not what my question is. When you go back to your comment of sharing technology with DOD, what is DOD's operating system?

Mr. PERRY. Across the Department, they use many. There is probably one each of quite a large subset of what is out on the market. In specific areas such as the area that I am addressing here, the registra——

Mr. BUYER. Let's take records. I mean that is where we want to be able to move these veterans records. If they get a medical board, they are medically boarded out of the military and we wanted to shift that over directly to the VA, if it is on a Microsoft system, would we want to keep it in a Microsoft system at the VA?

Mr. PERRY. What is more important than the operating system is standardizing the data that comes across.

Mr. BUYER. Okay.

Mr. PERRY. Both the syntax of the data, the structure that it takes, and the semantic meaning of all of the data elements. And many of the interoperability initiatives that we are pursuing with the Department of Defense are in fact on standardization of data, so that it is not so much of an issue what operating system, or frankly what data repository applications on top of that, if we all have the same Lexicon.

In some cases, we could go farther and actually have the same platform and the same applications reused. But the essential element is that we have shared meaning and understanding of the data that we exchange; and that standardization of data is sort of the, both necessary and sufficient condition to have interoperability.

Mr. GAUSS. From a technology standpoint, the key there is in the database engine. And we will be using the same database engine as DOD. And that will give us that interoperability to transfer the information once the data is standardized and formats are properly defined.

Mr. BUYER. And this standardization of data, is it going well?

Mr. PERRY. Yes, it is, in the health care area that is proceeding fairly well. And I think setting an example to be used potentially more broadly than just DOD and VA.

And, as we embark on doing the similar thing, with regard to personnel information, basic registration information, how to contact veterans, how to go through the process of determining their eligibility, we will do the same thing there, and in fact have a shared repository of that data with DOD.

Mr. GAUSS. Our biggest challenge is going to be able to gain access to all of the DOD data that is necessary to have in VA. For example, not all of the data that is in the DD–214 is available from DMDC. So part of our work effort with DOD is to get that data from DOD, so we can share with it. Definitionally, I think we are in good shape.

Mr. BUYER. Boy, that is one of the basics, isn't it? A DD–214 is like the entry to our system.

Mr. GAUSS. Yes, sir.

Mr. BUYER. Congratulations, how far you have come in 6 months.

Mr. GAUSS. Well, the DD–214, copy 3, unfortunately, copy 3 of the DD–214 is mailed to the Austin Automation Center. And the first time it gets digitized is when someone in VA hand jams it into a VA computer to create an electronic record. We have to fix this. When I retired, I got a letter three——

Mr. BUYER. Let me ask this question. There has got to be a quicker way to do that, isn't there?

I mean if I give you that DD–214, can't you just have that?

Mr. GAUSS. It is a carbon copy DD–214.

Mr. BUYER. Say again?

Mr. GAUSS. It is carbon copy.

Mr. BUYER. A carbon copy?

Mr. GAUSS. Yes, sir.

Mr. BUYER. Oh.

Mr. GAUSS. We have to fix——

Mr. BUYER. It is not on a machine with vacuum tubes? You know this is—you know unbelievable.

Mr. GAUSS. Yes, sir.

Mr. BUYER. Is there some worry about fraud or something as to why a DD–214 cannot be scanned into your system, and then sent?

Mr. GAUSS. Unfortunately, the way that the DD–214 gets filled out is not consistent. For example, in my DD–214, the fact that I served in the Vietnam Theater of Operations does not—is not reflected on my DD–214.

Mr. BUYER. And you are an Admiral.

Mr. GAUSS. Yeah, well, part of the problem is that they start with your most recent tour of duty, work back, and when they run out of space. It is a terrible process and it needs to be fixed. And that is in our gun sights to get fixed.

And this effort with DMDC has a very high priority to get the missing data, and get it electronically, and get it from DOD electronically, so we can start the process flow. I was appalled that it took 37 days for me to get a letter after I retired from the VA saying you are eligible for all of these benefits.

And I told my staff I have good news and bad news. The good news is VA knows I am alive. The bad news is why did it take 37 days? I should have had that letter on the 2nd of July. We have to fix this.

Mr. BUYER. As you move, you have been empowered because you are the agent of change. And when you are the agent of change, you upset people, you upset systems. So my question is about liability exposure.

Should we anticipate any liability exposure from any contracts with any vendors in which you may be altering, amending, or canceling?

Mr. GAUSS. I do not see any, frankly. Very sincerely, I do not see any. Most of the contracts that we have in place have base years plus options. Failure to exercise an option does not incur a liability.

Termination of a contract while in execution that has a term and a set of conditions could expose you to termination liabilities. But the way our contracts are right now, I do not see that.

Now, let's assume——

Mr. BUYER. The reason I asked the question is that we want to empower you so much that you make judgments for the horizon, not based on any particular fear of a liability. Okay?

Mr. GAUSS. Yes, sir.

Mr. BUYER. And I want you to keep the timeliness because of the billions of dollars that we are laying out here. When veterans are in line to get in the system, and we are willing to make a commitment in billions to you or 1.2 millions for your PCHS. That is why we are taking time here today.

Mr. GAUSS. Yes, sir.

Mr. BUYER. So if there is a contract out there and they say, "Well, I can't do this because," talk to us and let's try to work cooperatively here. Because I want you to keep your eye on the horizon. I want you to open those doors. I want you to change systems. And if you have got somebody that is in the way, and they are willing to give up their "goodwill"—okay?

Mr. GAUSS. Yes, sir.

Mr. BUYER. They are willing to give up their goodwill, have at it. Okay?

Mr. GAUSS. Yes, sir.

Mr. BUYER. Let me yield to minority counsel. I think he has one question.

Mr. SISTEK. Thank you, Mr. Chairman.

Earlier today, the chairman broached a question on the internal threat. And last April 2001, the subcommittee heard testimony on various types of authentication tools, public key-based digital signatures, et cetera.

What is the Department doing today in that regard concerning the internal threat? And where are we going 4, 5, 6 years from now?

Mr. BRODY. As I mentioned earlier, we have a number of programs in place to deal with the internal threat. They range for anything from our active monitoring of the environments, penetration testing, vulnerability scanning, the malicious code deployment, which is the largest in government.

Mr. SISTEK. I think we were looking more for authentication tools specifically.

Mr. BRODY. On the authentication side, we have a major program that has not been initiated yet, but we will be wheeling out over the coming year, referred to as the Authentication and Authorization Infrastructure, which involves the use of public key infrastructure, as well as potential smart cards and multi-factor authentication that we will deploy across the department and be used for authentication purposes.

Mr. SISTEK. When will you have that fielded and operational department-wide?

Mr. BRODY. We have asked for funding in the fiscal year 2004 budget. It has—of course, that carries with it an fiscal year 2003 authorization. So we will be kicking that off in the very near term.

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

Mr. BUYER. One question I have, I wrote a little note down when you used the term, "In 2004, I get to declare victory on VETSNET," and I thought about that. I don't know what that means.

Mr. GAUSS. Having a product, a quality product, that is ready to deploy into the field, so that as we roll it out and transition from the old system, that it is going to work, be useable, and start doing the job.

When the deployment is complete, we then shut down the benefits delivery network that runs on the Honeywell, and what had been originally envisioned to be achieved through VETSNET would be achieved, albeit, later than had been planned and at a larger cost.

Mr. BUYER. All right. Mr. Secretary, I want to thank you. I want to thank the Secretary Principi for empowering you. And I believe his move was the right move, in order for him to hold true to his vision of one Enterprise Architecture for the VA.

I compliment you on your work that you have done here over the last 6 months. I will accept your sincerity, Mr. Brody, that you are going to watch both. And, Dr. Perry, I am impressed by your eloquence. I am not a techie, but I can hang with you, which scares me, scares me a lot.

This concludes the hearing. And, Secretary Gauss, thank you very much.

Mr. GAUSS. Thank you, sir.

[Whereupon, at 12:22 p.m., the subcommittee was adjourned.]

APPENDIX

VA restructuring IT management

Move gives more power to department CIO

BY JUDI HASSON

Department of Veterans Affairs Secretary Anthony Principi has ordered the reorganization of information technology operations at VA headquarters by centralizing budget and management control in the chief information officer's office.

Principi said he ordered the changes because the VA had been hampered in carrying out plans to create "one VA," a pledge he made when he took office, and "time is running out."

"We have a lot of work to do," Principi told Federal Computer Week Aug. 9. "It's been very clear to me that this road is long and difficult."

In an Aug. 6 memo to key officers, Principi wrote: "Despite our best efforts, accountability for our IT resources remains elusive. To get from where we are to where we need to be across all VA's IT programs, we must reorganize how VA's IT is managed and financed."

There has been resistance to embracing the agency's enterprise architecture plan, Principi said. The implementation of cybersecurity initiatives is lagging, and CIO John Gauss has not been provided with IT budget details to "develop an integrated department IT portfolio."

Effective immediately, the VA's IT functions and personnel will be realigned under Gauss. Gauss also will be in charge of IT appropriations beginning Oct. 1.

The changes will affect the three CIOs within the VA — K. Adair Martinez, CIO at the Veterans Benefits Administration; Gary Christopherson, CIO at the Veterans Health Administration; and Joseph Nosari, CIO at the National Cemetery Administration. All three will become deputy CIOs reporting to Gauss.

"That is the kind of support and action that every CIO dreams of," said Roger Baker, a former CIO at the Commerce Department who tried to reorganize the CIO structure there in a similar fashion. "It's a real tangible demonstration that VA is very serious about getting much better at IT very quickly."

CHANGES IN STORE

Although the changes won't have an immediate impact on operations at more than 150 VA hospitals, Gauss is holding a meeting Aug. 12-15 in Austin, Texas, for almost 300 VA IT employees to discuss the new structure and future changes.

In a separate memo, Gauss told all IT personnel that there would be "no job loss due to reorganization."

"Change doesn't necessarily need to be slow and ponderous," said Alan Balutis, executive director of the Federation of Government Information Processing Councils. "I don't think there's anything wrong with going in sometimes and breaking a little china to achieve some results." ■

VA bolsters IT security

BY JUDI HASSON

The Department of Veterans Affairs has embarked on an innovative cybersecurity approach that could serve as a model for other federal agencies.

A consortium of five high-tech companies, known as the VA Security Team (VAST), began work Aug. 1 protecting the VA's entire network, from hospitals to cemeteries to medical and insurance records.

The VA awarded the consortium a contract potentially worth $103 million over 11 years for the VA's Computer Incident Response Capability.

"We're the second-largest federal government computing enterprise," said Bruce Brody, the VA's cybersecurity chief. "The magnitude of our enterprise alone makes it a target of malicious intent."

The VA has long been a target of hackers. Since January, VA computer systems have blocked more than 2 million virus attempts. And a private auditing firm hired by the VA's inspector general easily broke into computers at the agency and gained control of the data.

In March 2001, Brody was hired as the associate deputy assistant secretary for cybersecurity to fix the problems.

Brody said VAST would be handling incident analysis, management and response for the VA's nationwide system, which will include dealing with vulnerabilities and computer forensics.

In addition, the consortium will be handling managed security services nationwide that will be "mandatory for every hospital."

SecureInfo Corp., a San Antonio-based cybersecurity company that has done similar work for the Defense Department, is leading the consortium to detect and respond to threats and real-time incidents around-the-clock.

Other consortium members include Applied Engineering Management Corp.,

EDITORIAL

COMMENT

FEDERAL COMPUTER WEEK

EDITOR IN CHIEF
Allan Holmes
aholmes@fcw.com

EDITOR
John Stein Monroe
jsmonroe@fcw.com

ART DIRECTOR
Jeff Langkau
jlangkau@fcw.com

MANAGING EDITOR
Colleen O'Hara
ohara@fcw.com

TECHNOLOGY EDITOR
Rutrell Yasin
ryasin@fcw.com

SENIOR EDITORS
Christopher J. Dorobek
cdorobek@fcw.com
John Zyskowski
jzyskowski@fcw.com

EDITOR AT LARGE
Judi Hasson
jhasson@fcw.com

SENIOR WRITER
William Matthews
bmatthews@fcw.com

SENIOR REPORTERS
Dan Caterinicchia
dance@fcw.com
Diane Frank
dfrank@fcw.com
Dibya Sarkar
dsarkar@fcw.com

REPORTER
Megan Lisagor
mlisagor@fcw.com

PRODUCTION EDITOR
Terri J. Huck

ASSOCIATE ART DIRECTOR
Susan Morrison

COPY EDITORS
Amanda McClements
Patricia Tisak
Chris Wright

GRAPHIC DESIGNER
Allison Cusato

EDITORIAL ASSISTANT
Molly Ferrara

FCW.COM

MANAGING EDITOR, ONLINE
Diane Tomasik
dtomasik@fcw.com

ONLINE PRODUCER
Lisa L. McNair
lmcnair@fcw.com

FCW TEST CENTER

REVIEWS EDITOR
Patrick Marshall
pgmarshall@pgmarshall.net

SENIOR WRITER, REVIEWS
Michelle Speir
mspeir@fcw.com

FCW IS A PUBLICATION OF
101COMMUNICATIONS LLC
3141 FAIRVIEW PARK DRIVE, SUITE 777
FALLS CHURCH, VA 22042-4507
(703) 876-5100; FAX (703) 876-5126
SUBSCRIBE ONLINE AT WWW.SUBMAG.COM/SUB/FW
CORPORATE HEADQUARTERS
9121 OAKDALE AVENUE, SUITE 101
CHATSWORTH, CA 91311

The business masthead can be found on Page 57

MANAGEMENT

The rise of the CIO

This month marks the sixth anniversary of the Clinger-Cohen Act of 1996, which established the position of chief information officer at federal agencies. It's been a disappointing six years, during which frustration has increased among CIOs as they struggle to earn clout with agencies' senior management circles and help use information technology to support business process change.

But times are changing.

Anthony Principi, secretary of the Department of Veterans Affairs, has given John Gauss, the agency's CIO, IT budget and management control. The reason, Principi said, was because many in the agency were resisting the VA's enterprise architecture plan and the cybersecurity initiatives, which are aimed at plugging holes in VA information systems. Such authority is what one former federal CIO called "a dream" for anyone in that position.

Traditionally, that's where this kind of authority has been — in CIOs' dreams. These responsibilities are exactly what CIOs and their supporters have been calling for since the Clinger-Cohen Act was signed into law Aug. 8, 1996. Without the resources or authority to affect buying or management decisions, CIOs have been caught between a rock and a hard place.

Federal management experts have said what was needed was a commitment from the top — the agency head. Principi stepped up to give his agency's CIO authority and, in doing so, shows other agency secretaries what needs to be done. It is a bold move, and one that is sorely needed.

Principi understands that IT will help transform the VA. He also understands that he must place a lot of the responsibility for reforming the agency in the hands of the CIO. Many agencies should watch for how this management story unfolds. Of course, not all decisions will be the right ones, but giving the CIO the space to succeed or fail on his or her own terms is a good place to start. Principi's decision will likely result in a more effective, streamlined and secure VA. ■

Online poll
Does your CIO have enough clout to make things happen?
Take our survey at www.fcw.com.

ILLUSTRATION/JOHN KLOSSNER

MANAGEMENT

BRIEFING

VA spruces up security act

Agency tightens system, personnel management

BY JUDI HASSON

Only 18 months ago, the Department of Veterans Affairs received a failing grade for its cybersecurity efforts.

Reports from the inspector general's office criticized the agency for failing to protect its computer environment. Congress was up in arms over disclosures that it was a cakewalk to hack the VA's systems. And VA officials did not even know how many renegade gateways had been set up to get into the VA computer system.

In a remarkably short period of time, the VA has cleaned up its act.

"When I got here, this place — cybersecurity — was pretty chaotic," said Bruce Brody, the VA's cybersecurity chief since March 2001. "There was nothing but bad news."

But Brody had some strong supporters who resolved to fix the problem. Backed by VA Secretary Anthony Principi, who has promised to create one VA, and chief information officer John Gauss, Brody has made changes that are becoming the model for other agencies facing cybersecurity threats.

"With the support of the secretary and the leadership of the CIO and his team, we have come a long way," Brody said. "But much remains to be done, and we are working very hard to do it."

It is no easy task. There are more than 200 unauthorized and unprotected gateways into the VA's central cyber infrastructure, built by employees in the field with no authority to do so. It was "uncontrolled," Brody said. And VA officials had no idea how big VA cyberspace was.

"They sprouted like a thousand flowers booming," Brody said. "There was no consistent security policy. Wherever someone wanted a gateway, there was a gateway."

The VA launched the Enterprise Cyber Security Infrastructure Project to find the gateways and secure them. In the next two years, the VA will create standardized hardened gateways that will be centrally managed and monitored by VA security operations centers.

In October, the VA will begin closing down the unauthorized gateways. In the meantime, the cybersecurity office is requiring tighter firewalls and periodic testing to make sure hackers cannot get in.

"By September 2004, there will only be a single-digit number of exit gateways...and no other external connections," Brody said.

Gateways aren't the only problem within the VA, although it has been one of the biggest headaches. The agency has worked to develop a cutting-edge enterprise architecture plan and standardize programs throughout its network, which reaches more than 160 hospitals. Last month, the VA awarded a contract to manage its nationwide security services around the clock. It is putting a national virtual private network in place in October. The VPN will enable the agency to encapsulate, encrypt and then send data to a specific destination.

"Veterans records are more secure than they have been in the past," Brody said. "They are not as secure as they will be in the future."

Matt Roland of Gartner Inc., a market research firm, said that good information technology security is a property of an environment, not the property of a product or technology.

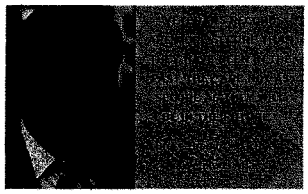
"A lot of organizations focused on deploying firewalls and antivirus software," he said. "Now there is an increased emphasis on establishing management processes around these technologies."

It appears the VA has turned a corner. In August, Principi consolidated IT management and budget functions under the CIO, a move that Congress has sought for seven years. The order also consolidates cybersecurity functions, which includes centralizing the $50 million cybersecurity budget in Brody's office.

Art Wu, staff director of the House Veterans' Affairs Committee's Oversight and Investigations Subcommittee, said the VA's actions should "expedite and facilitate VA's compliance under" the Government Information Security Reform Act.

The VA is "definitely on the right track," according to Shannon Kellogg, vice president for information security programs at the IT Association of America.

The agency is looking at security in a "holistic fashion, a multi-tiered process," and that makes all the difference, Kellogg said. ■



TIGHTENING UP

The Department of Veterans Affairs has done the following to protect its systems:

- Launched the Enterprise Cyber Security Infrastructure Project to find unauthorized gateways to the agency's systems and shut them down.
- Required tighter firewalls and periodic security testing to ensure hackers cannot get in.
- Awarded a contract in August for around-the-clock nationwide managed security services.
- Built a national virtual private network.
- Centralized the $50 million cybersecurity budget in the VA cybersecurity chief's office.

VA'S INFORMATION TECHNOLOGY SECURITY PROGRAM

TESTIMONY OF
THE HONORABLE RICHARD J. GRIFFIN
INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS

HOUSE COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

September 26, 2002

Mr. Chairman and Members of the Subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs' (VA) Information Technology (IT) security program. Our work continues to identify serious Department-wide vulnerabilities in IT security. As a result, we concluded from our audit results that the Department must continue to designate information security as a material weakness area under the Federal Manager's Financial Integrity Act (FMFIA).

Since our March 13, 2002 testimony to this Subcommittee, we completed a second national audit of VA's IT security program. A draft report has been provided to the Department for review and comment. The audit found that the Department has a number of initiatives in process that will provide the opportunity to improve VA's information security posture.

Key Department actions include:

- Establishment of a VA-wide security plan; and the required policies, procedures, and guidelines mandated by the Government Information Security Reform Act (GISRA).
- Implementation of VA-wide anti-virus protection.
- Staffing information security officer positions.
- Prioritization of Department-wide security remediation efforts.
- Centralization of the Department's IT security program under the Office of the Chief Information Officer (CIO).

While progress has been made, much work remains to implement key IT security initiatives, establish a comprehensive integrated VA-wide security program, and fully comply with GISRA. Our audit work continues to identify significant security vulnerabilities that represent an unacceptable level of risk to VA operations and its mission of providing healthcare and delivering benefits to the Nation's veterans.

Significant information security vulnerabilities continue to place the Department at risk of:

- Denial of service attacks on mission critical systems.
- Disruption of mission critical systems.
- Unauthorized access to and improper disclosure of data subject to Privacy Act protection and sensitive financial data.
- Fraudulent payment of benefits.

Penetration Tests Showed That VA Systems Need To Be Better Protected

Penetration testing completed during the past 2 years verified that VA's automated systems could be exploited to gain access to sensitive veteran healthcare and benefit information. In response to last year's testing, the Department strengthened security controls at the facilities where we conducted our testing. During this year's follow up testing at these sites, the security control measures established prevented our external penetration attempts (access to systems from outside of VA's network.). VA must implement external automated system protection measures Department-wide to adequately protect its systems and sensitive data.

Continuing automated system control vulnerabilities allowed our internal penetration testing (access to systems from inside of VA's network) to gain access to sensitive veterans' benefit and healthcare information.

The vulnerabilities exploited during this year's testing were present during our previous testing a year ago. The Department has not taken appropriate corrective action to eliminate these vulnerabilities in response to our initial findings. The nature and number of vulnerabilities found warrant immediate attention to reduce the significant exposure and high risk of an internal attack.

Industry experience shows that the risk of inappropriate access by employees/contractors is highest inside of the network. We have again provided the Department with the details of this year's penetration testing results and recommendations on how the vulnerabilities could be corrected.

VA's CIO Needed Expanded Authority Over Security Remediation Efforts

This year's security audit has shown that VA needs to take additional actions to correct information security vulnerabilities. VA's overall weak cyber security posture continues to be unacceptable and is reported as a Department material weakness. In our view, VA's overall security posture is one of the results of a lack of a unified or "One-VA" approach to information security that has lead to an ineffective approach to the implementation of necessary security improvements across the Department.

The Department's Administrations and staff offices have individually managed and controlled their information security program activities. Our security assessment results show that this decentralized management approach has not worked, with a continuing unacceptable security posture for the Department as a whole. Many security vulnerabilities identified in last year's audit remain unresolved, and additional security vulnerabilities were identified. With the exception of certain information technology acquisitions, the Department CIO did not have the authority to assure that the Department's security remediation efforts are completed. The decentralized management approach to information security management impeded the Department's ability to successfully strengthen its overall security posture.

We met with the Department CIO on July 22, 2002, and advised that we would be recommending that the Department centralize authority for the implementation of security remediation efforts to his office. This centralization of authority would include management and decision authority on all Department security remediation efforts. We had previously recommended centralized oversight in our prior year audit. On August 6, 2002, the Secretary of Veterans Affairs issued a memorandum centralizing the Department's IT security program, including authority, personnel, and funding in the Office of the Department CIO, effective October 1, 2002.

We believe that the Secretary's action will provide the opportunity to implement a "One-VA" approach to information security with implementation of necessary security improvements across the Department.

Department CIO Needs To Take Corrective Action In Several Key Areas

Based on the results of our second annual audit of VA's IT security program, we recommended that the Department CIO take the following actions:

- Complete priority security remediation efforts in the next 12 months for the following areas: (1) install intrusion detection systems nationwide; (2) complete infrastructure protection actions; (3) complete data center contingency planning; (4) complete certification and accreditation of VA systems; (5) upgrade/terminate external connections; (6) improve configuration management of VA systems; (7) move the location of the VA Central Office (VACO) data center; (8) eliminate vulnerabilities in the application program/operating system change controls; and, (9) control physical access to computer rooms. Budgetary resources necessary to accomplish the priority security remediation efforts should be requested.

- Require the Administrations to: (1) correct identified security vulnerabilities at their facilities and data centers; (2) improve security awareness at the operating levels; and, (3) highlight the need to assure compliance with existing VA information security policy, procedures, and controls.

- Require the Administrations to certify completion of the remediation of information security vulnerabilities identified by the audit and provide annual facility certification of compliance with VA security policy, procedures, and controls.

- Establish skill levels and training requirements for Department information security staff to assure that they are capable of effectively performing their assigned duties.

- Implement VA-wide policy for effective monitoring of network operations to include use of electronic scanning and penetration testing techniques.

- Establish a national clearinghouse in the Office of Cyber Security for identifying and distributing information on security patch upgrades/fixes that need to be implemented.

- Assure that the GISRA reporting database accurately reflects the status of completed Department security remediation actions.

- Address the areas of non-compliance with GISRA, Office of Management and Budget (OMB) Circular A-130, Appendix III, and Presidential Executive Order 13231 on critical infrastructure protection requirements.

Conclusion

VA needs to take additional actions to establish necessary security controls to proactively identify and prevent information security related risks and implement corrective action. As reported in our Fiscal Year (FY) 2001 information security audit and based on the work completed during the FY 2002 audit, VA still has not effectively implemented all planned security measures and has not assured compliance with established security polices, procedures, and controls requirements.

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

United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10 a.m. EDT
Thursday,
September 26, 2002

VA INFORMATION TECHNOLOGY

Management Making Important Progress in Addressing Key Challenges

Statement of Joel C. Willemssen
Managing Director, Information Technology Issues

GAO-02-1054T

United States General Accounting Office September 26, 2002

VA INFORMATION TECHNOLOGY Management Making Important Progress in Addressing Key Challenges

Highlights of GAO-02-1054T, testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In March of this year, GAO testified before the Subcommittee about the Department of Veterans Affairs' (VA) information technology (IT) program, and the strides that the Secretary had made in improving departmental leadership and management of this critical area–including the hiring of a chief information officer.

At the Subcommittee's request, GAO evaluated VA's new IT organizational structure, and provided an update on VA's progress in addressing other specific areas of IT concern and our related recommendations pertaining to

- enterprise architecture,
- information security,
- the Veterans Benefits Administration's replacement compensation and pension payment system and maintenance of the Benefits Delivery Network, and
- the government computer-based patient record initiative.

What GAO Found

Since our March testimony, VA has made important progress in its overall management of information technology. For example, the Secretary's decision to centralize IT functions, programs, and funding under the department-level CIO holds great promise for improving the accountability and management of IT spending–currently over $1 billion per year. But in this as well as the other areas of prior weakness, the strength of VA's leadership and continued management commitment to achieving improvements will ultimately determine the department's degree of success. As for its progress in other areas:

- *Enterprise architecture.* The Secretary recently approved the initial, "as is" version of this blueprint for evolving its information systems, focused on defining the department's current environment for selected business functions. VA still, however, needs to select a permanent chief architect and establish a program office to facilitate, manage, and advance this effort.
- *Information security.* Steps have been taken that should help provide a more solid foundation for detecting, reporting, and responding to security incidents. Nonetheless, the department has not yet fully implemented a comprehensive computer security management program that includes a process for routinely monitoring and evaluating the effectiveness of security policies and controls, and acting to address identified vulnerabilities.
- *Compensation and pension payment system.* While some actions have been taken, after more than 6 years, full implementation of this system is not envisioned before 2005; this means that the 3.5 million payments that VA makes each month will continue to depend on its present, aging system.
- *Government computer-based patient record initiative.* VA and the Department of Defense have reported some progress in achieving the capability to share patient health care data under this program. Since March, the agencies have formally renamed the initiative the Federal Health Information Exchange and have begun implementing a more narrowly defined strategy involving a one-way information transfer from Defense to VA; a two-way exchange is planned by 2005.

This is a test for developing highlights for a GAO report. The full testimony, including GAO's objectives, scope, methodology, and analysis, is available at www.gao.gov/cgi-bin/getrpt?GAO-02-1054T. For additional information about the testimony, contact Joel C. Willemssen (202-512-6253) or at *willemssenj@gao.gov*. To provide comments on this test highlights, contact Keith Fultz (202-512-3200) or email HighlightsTest@gao.gov.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to take part in your discussion of the Department of Veterans Affairs' (VA) information technology (IT) program. Information technology continues to play an integral and substantial role in helping VA effectively serve our nation's veterans, with the department spending more than a billion dollars annually in support of its information technology operations. As you are well aware, however, the department has been challenged in its efforts to effectively manage its information technology to produce results and achieve optimal agency performance.

Our testimony last March noted important strides by the Secretary of Veterans Affairs to improve the department's IT leadership and management, including the hiring of a chief information officer (CIO) to lead the program and a commitment to reform how the department uses information technology.[1] Since that time, the Secretary has taken additional steps toward achieving improvements in key areas of IT performance, including recently announcing a realignment of the way in which the department is organized to carry out its information technology mission.

At your request, we will discuss today this new organizational structure and resulting changes in the role of VA's CIO. In addition we will provide an update of the department's progress since March in addressing specific weaknesses in its overall information technology program, including the status of its actions to

- develop an enterprise architecture,
- improve information security,

[1]U.S. General Accounting Office, *Progress Made, but Continued Management Attention Is Key to Achieving Results,* GAO-02-369T (Washington, D.C.: Mar. 13, 2002).

- implement the Veterans Benefits Administration's (VBA) veterans service network (VETSNET) replacement compensation and pension payment system and maintain the existing Benefits Delivery Network, and
- implement jointly with the Department of Defense and Indian Health Service the government computer-based patient record initiative.

In conducting this work we analyzed relevant documentation and interviewed key agency officials to identify and assess VA's decisions and actions since March to improve its information technology management. We reviewed available documentation discussing the department's plans and strategies for realigning its information technology structure. We also examined its enterprise architecture strategy as well as steps being taken to strengthen computer security management departmentwide. Further, we conducted site visits at the Veterans Benefits Administration's regional office in Salt Lake City to assess the current use of VETSNET in processing compensation and pension benefits claims; and at the VA medical center in Washington, D.C., to observe data retrieval capabilities of the Federal Health Information Exchange (formerly the government computer-based patient record initiative). We performed our work in accordance with generally accepted government auditing standards, in August and September of this year.

RESULTS IN BRIEF

Over the past 6 months, VA has shown clear progress in addressing some of the critical weaknesses that have plagued its management of information technology. The Secretary of Veterans Affairs and other top agency leaders have continued to make important strides in improving key areas of IT performance. Nonetheless, some aspects of the department's information technology environment continue to be particularly challenging and to require substantial management attention. As the department proceeds, ensuring sound project management and oversight will continue to be essential to advancing its efforts.

Accountability for its information technology investments should be well served by VA's recently announced realignment of its information technology structure. Although yet to be finalized, the Secretary's decision to centralize information technology functions, programs, and funding under the department-level CIO shows promise for improving IT accountability and enabling the department to implement its One VA vision.[2] The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively capture and manage its IT spending.

Beyond its actions to establish greater accountability in this area, the department continues to make important progress in developing its departmentwide enterprise architecture—the blueprint for evolving its information systems and developing new systems that optimize their mission value. The Secretary recently approved the initial version of VA's enterprise architecture, focused on defining the department's current, "as is" and desired, "to be" target environments for selected business functions. Nonetheless, VA must still accomplish critical actions to ensure successful completion of its architecture. For example, to achieve a sound program management structure, it needs to select a permanent chief architect and establish a program office to facilitate, manage, and advance this effort.

In another critical area, the department continues to make progress in strengthening its information security. It has taken actions that should help provide a more solid foundation for detecting, reporting, and responding to security incidents. Among these actions, it has contracted to expand departmentwide incident response and analysis capabilities, including enhancing security monitoring and detection. Nonetheless, the department has not yet fully implemented a comprehensive computer security management program that includes a process for routinely monitoring and evaluating the effectiveness of security policies and controls and addressing identified vulnerabilities. Further, VA's offices self-report computer security weaknesses, and it lacks an independent component to ensure the accuracy of reporting and validation of corrective actions taken.

[2]According to the department, the "One VA" vision describes how it will use information technology in versatile new ways to improve services and enable VA employees to help customers more quickly and effectively. It stems from the recognition that veterans think of VA as a single entity, but often encounter a confusing, bureaucratic maze of uncoordinated programs that put them through repetitive and frustrating administrative procedures and delays.

Conversely, the department is not making as much progress in addressing the challenges associated with implementing its VETSNET compensation and pension replacement payment system. Specifically, after more than 6 years, the department still has significant work to accomplish, and could be several years from fully implementing the system. Complete implementation is not anticipated until 2005, thus requiring continued reliance on the aging Benefits Delivery Network to provide the more than 3.5 million payments that VA must make to veterans each month.

Finally, VA and DOD have made some progress in achieving the capability to share patient health care data begun under the government computer-based patient record (GCPR) initiative. This progress was achieved as part of a substantially revised, scaled-down strategy. As part of this new strategy that the two agencies have now implemented, clinicians in VA medical facilities throughout the country have access to health information on more than a million separated service personnel.

IT REALIGNMENT INCREASES AUTHORITY AND OVERSIGHT OF VA's CHIEF INFORMATION OFFICER

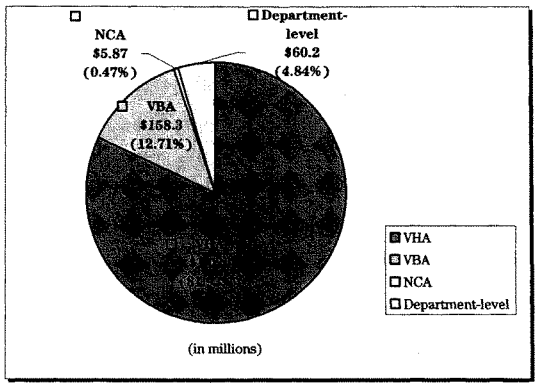
Successful implementation of VA's information technology program requires strong leadership and management to help define and guide the department's plans and actions. The Paperwork Reduction Act of 1980 and the Clinger-Cohen Act of 1996[3] articulate the importance of CIOs in promoting improvements in their agencies' work processes and making sound investment decisions that effectively align IT projects with the organization's business planning and measurement processes. To be successful in this role, CIOs must build credible organizations and develop and organize information management capabilities to meet agency mission needs.

With the hiring of a department-level CIO in August 2001, VA took a significant step toward addressing critical and longstanding weaknesses in its management of information technology. Our prior work has highlighted some of the challenges that the CIO faced as a result of the way

[3]44 U.S.C. 3506 and P.L. 104-106, Section 5125, respectively.

in which the department was organized to carry out its information technology mission.[4] Among these challenges was that information systems and services were highly decentralized, with the VA administrations and staff offices controlling a majority of the department's information technology budget. As illustrated in figure 1, out of the approximately $1.25 billion fiscal year 2002 information technology budget, the Veterans Health Administration (VHA) oversaw approximately $1.02 billion, VBA approximately $158.3 million, and the National Cemetery Administration (NCA) approximately $5.87 million. The remaining $60.2 million was controlled at the department level.

Figure 1: Breakdown of VA's $1.25 Billion Information Technology Budget (fiscal year 2002)



Source: GAO analysis.

In addition, our testimony in March noted that there was neither direct nor indirect reporting to VA's cyber security officer—the department's senior security official—thus raising questions about this person's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. The more than 600

[4] U.S. General Accounting Office, *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist,* GAO-01-550T (Washington, D.C.: Apr. 4, 2001) and GAO-02-369T.

information security officers in VA's three administrations and its many medical facilities throughout the country were responsible for ensuring the department's information security, although they reported only to their facility's director or to the chief information officer of their administration.

Given the large annual funding base and decentralized management structure, it is crucial that the CIO ensure that well-established and integrated processes for leading, managing, and controlling investments are commonplace and followed throughout the department. The Secretary has recognized weaknesses in accountability for the department's information technology resources and the consequent need to reorganize how information technology is managed and financed. Accordingly, in a memorandum dated August 6, 2002, he announced a realignment of the department's information technology operations. According to the memorandum, the realignment will centralize information technology functions, programs, workforce personnel, and funding into the office of the department-level CIO. In particular, several significant changes are being made:

- The CIOs in each of the three administrations—VHA, VBA, and NCA—have been designated deputy CIOs and will report directly to the department-level CIO. Previously, these officials served as component-level CIOs who reported only to their respective administrations' undersecretaries.
- All administration-level cyber security functions have been consolidated under the department's cyber security office, and all monies earmarked for these functions have been placed under the authority of the cyber security officer. Information security officers previously assigned to VHA's 21veterans integrated service networks will now report directly to the cyber security officer, thus extending the responsibilities of the cyber security office to the field.
- Beginning in fiscal year 2003, the department-level CIO will assume executive authority over VA's IT appropriations.

The realignment had not been finalized at the conclusion of our review, thus its full impact on VA's mission and the CIO's success in managing information technology at the department level could not yet be measured. Nonetheless, in pursuing these reforms, the Secretary has demonstrated the significance of establishing an effective management structure for building credibility in the way information technology is used, and has taken a significant step toward achieving a "One VA" vision.

The Secretary's initiative also represents a bold and innovative step by the department, and is one that has been undertaken by few other federal agencies. For example, as part of our review, we sent surveys to the 23 other major federal agencies, seeking information on the organization and reporting relationships of their department- and component-level CIOs. Of the 17 agencies that responded, 8 reported having component-level CIOs, none of which reported to the department-level CIO. Only one agency with component-level CIOs reported that its department-level CIO had authority over all IT funding.

As the realignment proceeds, the CIO's success in managing information technology operations will hinge on effective collaboration with business counterparts to guide IT solutions that meet mission needs. Guidance that we issued in February 2001 on the effective use of CIOs in several leading private and public organizations provides insight into three key factors contributing to CIO successes:

- First, senior executives embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making.
- Second, effective CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. While placement of the CIO position at an executive management level in the organization is important, effective CIOs earn credibility and produce results by establishing effective working relationships with business unit heads.
- Third, successful CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy

structures, and available IT skills, this understanding is necessary to ensure that the CIO's office is aligned to best serve the needs of the enterprise.[5]

VA's new organizational structure holds promise for building a more solid foundation for investing in and improving the department's accountability over information technology resources. Specifically, under the realignment the CIO assumes budget authority over all IT appropriations, including authority to veto proposals submitted from sub-department levels. This could have a significant effect on VA's accountability for how components are spending money, as we have previously noted the department's inability to adequately capture all of its IT costs.[6]

As the first step toward gaining accountability for information technology investments, the CIO is attempting to determine what expenditures have been incurred in fiscal year 2002. Since VA's annual budget submissions to OMB have not included a specific line item for information technology operations, the CIO has asked each administration to provide accurate information identifying the costs incurred by each of them for this fiscal year. According to the CIO, preliminary results showed that certain non-IT costs, such as for users' personnel, had been included in the total expenditures, while some IT costs, such as for IT personnel and telecommunications, had been excluded. The CIO's goal is to compile cost data that accurately reflect the department's information technology expenditures.

In the absence of a budget line item, the CIO is requiring each facility to develop "spend plans" for fiscal year 2003 IT funding. These plans are expected to serve as a control mechanism for information technology expenditures during the year and will be administered by each facility, with the CIO retaining veto power over them. The plans have been designed to provide the CIO with investment cost details at a departmentwide level, allowing for a portfolio-based project selection process and lessening duplication of effort. Once the plans are implemented, the CIO

[5]U.S. General Accounting Office, *Maximizing the Success of Chief Information Officers: Learning From Leading Organizations,* GAO-01-376G (Washington, D.C.: February 2001).

[6]U.S. General Accounting Office, *VA Information Technology: Progress Continues Although Vulnerabilities Remain,* GAO/T-AIMD-00-321 (Washington, D.C.: Sept. 21, 2000).

anticipates being able to compare planned and actual expenditures and to uncover the details of specific projects.

PROGRESS TOWARD DEVELOPING AN ENTERPRISE ARCHITECTURE CONTINUES, BUT ADDITIONAL WORK NEEDED

Developing and implementing an enterprise architecture[7] to guide VA's information technology activities continues to be an essential and challenging undertaking. VA and other federal agencies are required to develop and implement enterprise architectures to provide a framework for evolving or maintaining existing and planned IT, in accordance with OMB guidelines.[8] In addition, guidance issued last year by the Federal CIO Council,[9] in collaboration with us, further emphasizes the importance of enterprise architectures in evolving information systems, developing new systems, and inserting new technologies that optimize an organization's mission value. Overall, effective implementation of an enterprise architecture can facilitate VA's management by serving to inform, guide, and constrain the information technology investment decisions being made for the department, and subsequently decreasing the risk of buying and building systems that are duplicative, incompatible, and unnecessarily costly to maintain and interface.

As depicted in figure 2, the enterprise architecture is both dynamic and iterative, changing the enterprise over time by incorporating new business processes, new technology, and new capabilities. Depending on the size of the agency's operations and the complexity of its environment, enterprise architecture development and implementation require sustained attention to process management and agency action over an extended period of time. Once implemented, the enterprise architecture must be kept current through regular maintenance.

---

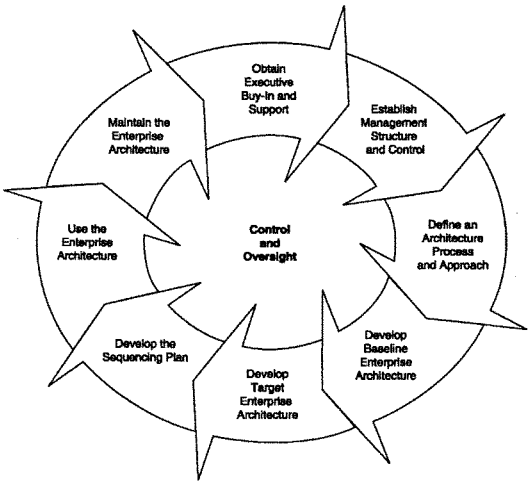
[7]An enterprise architecture is a blueprint for systematically and completely defining an organization's current (baseline) operational and technology environment, and a roadmap toward the desired (target) state. It is an essential tool for effectively and efficiently engineering business processes and for implementing their supporting systems and helping them evolve.

[8]OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: Nov. 30, 2000).

[9]Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (Washington, D. C.: February 2001).

Periodic reassessments are required to ensure that it remains aligned with the department's strategic mission and priorities, changing business practices, funding profiles, and technology innovation.

Figure 2: The Enterprise Architecture Process



Source: *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, 2001

When we testified last March, VA had taken a number of promising steps toward establishing some of the core elements of an enterprise architecture. Among other actions, it had obtained executive commitment from the Secretary, department-level CIO, and other senior executives and business teams that is crucial to raising awareness of and leveraging participation in developing the architecture. VA had also chosen a highly recognized framework to organize the

structure of its enterprise architecture.[10] Further, it had begun defining its current architecture, an important step for ensuring that future progress can be measured against such a baseline, and it was developing its future (target) telecommunications architecture.

Nonetheless, at that time we noted that VA still faced many more critical tasks to successfully develop, implement, and manage its enterprise architecture. One of the key activities that required attention was the establishment of a program management office headed by a permanent chief architect to manage the development and maintenance of the enterprise architecture. In addition, the department needed to complete a program management plan delineating how it would develop, use, and maintain the architecture. Further, although VA had developed a baseline application inventory to describe its "as is" state, it had not completed validating the inventory or developing detailed application profiles for the inventory, including essential information such as business functions, information flows, and external interface descriptions.

VA Has Expanded Its Initial Enterprise Architecture Development Work

Over the past 6 months, VA has made substantial strides toward instituting its enterprise architecture program. For example, in April it issued its fiscal year 2002 One VA enterprise architecture implementation plan, which will be used to align integrated technology solutions with the department's business needs. And in July, the CIO issued a mandatory directive prescribing departmentwide policy for the establishment and implementation of an integrated One VA enterprise architecture and to guide the development and management of all of VA's IT assets.[11] VA also finalized its enterprise architecture communications plan that will be used to help business and IT management and staff develop a corporate model of customer service.

[10]Among the experts that VA consulted was John Zachman, author of "A Framework for Information Systems Architecture," referred to as the Zachman framework (*IBM Systems Journal*, vol. 26(3), 1987). This framework provides a common context for understanding a complex structure and enables communication among those involved in developing or changing the structure.

[11]Department of Veterans Affairs, *Department of Veterans Affairs (VA) Enterprise Architecture (EA)*, VA Directive 6051 (Washington, D.C.: July 12, 2002).

More recently, on September 5, the Secretary approved the initial version of the department's One VA enterprise architecture. VA officials describe the architecture as a top-down, business-focused document that provides a blueprint for systematically defining and documenting the department's desired (target) environment. The document provides a high-level, overarching view of the department's "as is" enterprise business functions and key enabling functions.[12] VA's work to develop the "as is" view revealed the complexities of its baseline information systems, work processes, and supporting infrastructure. For example, it identified over 30 independently designed and operated data networks, over 200 independent external network connections, over 1,000 remote access system modem connections, and a total of 7,224 office automation servers that are currently part of the baseline environment.

The enterprise architecture document also incorporates high-level versions of a sequencing plan, technical reference model, and standards profile—all of which are critical to ensuring the complete development and implementation of the architecture. A sequencing plan serves as a systems migration roadmap to provide the agency with a step-by-step process for moving from the baseline to the target architecture. The technical reference model provides a knowledge base for a common conceptual framework, defines a common vocabulary and set of services and interfaces, and serves as a tool for the dissemination of technical information across the department. The standards profile, used in conjunction with the technical reference model, assists departmental components in coordinating the acquisition, development, and interoperability of systems to accomplish the department's enterprise architecture program goals.

Further, VA has integrated security practices into the initial version of its enterprise architecture. These security practices provide a high-level description of the baseline and target distributed systems architectures for major elements of the department's cyber security infrastructure.

[12]Enterprise business functions are externally focused functions involving direct interactions with veterans across the enterprise, such as providing medical care benefits, vocational rehabilitation, and employment benefits. Key enabling functions are those necessary to support the enterprise business functions, such as eligibility and registration, and enable smooth operation of the overall enterprise both internally and externally.

Continued Commitment to Developing VA's Enterprise Architecture Is Essential

Even with notable progress, VA must nonetheless complete a number of additional actions to fully implement and effectively manage its enterprise architecture. With the Federal CIO Council's guide as a basis for analysis, table 1 illustrates the progress that the department has made since March in accomplishing key enterprise architecture process steps, along with examples of the various critical actions still required to successfully implement and sustain its enterprise architecture program.

Table 1: VA's Progress in Developing, Implementing, and Using an Enterprise Architecture as of September 2002

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Obtain executive buy-in and support			
Ensure agency head buy-in and support	✓		
Issue executive enterprise architecture policy	✓		
Obtain support from senior executive and business units	✓		
Establish management structure and controls			
Establish technical review committee	✓		
Establish capital investment council		Drafted the Information Technology Integrated Management Guide, which lays out the integration of VA's EA, capital planning, investment, and project management functions Completed integration of its capital planning, investment, and project management functions, and uses it to evaluate IT projects	Finalize and issue the Information Technology Integrated Management Guide
Establish EA executive steering committee	✓		

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Appoint chief architect		Acting chief architect continues to fill position Recruitment effort for permanent chief architect continues; position expected to be filled in early 2003	Hire a chief architect with requisite core competencies
Establish EA program management office		Filled five positions in EA program management office Additional position advertisements being prepared, full staffing of office anticipated by the end of calendar year 2002	Fully staff the EA program management office with experienced architects to manage, control, and monitor development of the EA
Appoint key personnel for risk management, configuration management and quality assurance (QA)		Risk manager and configuration manager positions have not been filled, and VA does not plan to fill them The Enterprise Architecture Council will perform risk and configuration management and the Information Technology Board will perform QA functions	Ensure that adequate staffing occurs and functions are performed Establish an independent, objective entity to perform QA
Establish enterprise architecture core team	✓		
Develop EA marketing strategy and communications plan	✓		
Develop EA program management plan			Develop and finalize a plan that will delineate actions to develop, use, and maintain the EA, including management control and oversight
Initiate development of enterprise architecture	✓		
Define architecture process and approach			
Define intended use of architecture	✓		
Define scope of architecture	✓		
Determine depth of architecture	✓		
Select appropriate EA products	✓		

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Select products that represent business of enterprise	✓		
Select products that represent agency technical assets	✓		
Evaluate and select framework	✓		
Select EA tool set	✓		
Develop baseline enterprise architecture			
Collect information that describes existing enterprise		Version 1.0 of VA's EA includes high-level descriptions of its baseline enterprise architecture business functions and key enabling functions from the planners' business owners' designers' and builders' viewpoints.	Continue development of the enterprise architecture to fully describe and document all current business functions and the technology infrastructure
Generate products and populate EA repository[b]		Repository established on VA's intranet Web site is populated with data on the planners' and owners' views of VA's architecture In FY 2003 VA plans to assess the need to develop a new repository and the contents of that repository	Complete population of the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models		Enterprise Architecture Council subject matter experts reviewed, validated, and refined models contained in version 1.0 of the enterprise architecture Council membership included representatives from VA's technical and business lines	Have subject matter experts continue to assess the enterprise architecture products for accuracy and completeness

Steps in the enterprise architecture (EA) process*	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Develop target enterprise architecture			
Collect information that defines future business operations and supporting technology: • strategic business objectives • information needed to support business • applications to provide information • technology to support applications		Version 1.0 of VA's enterprise architecture contains high-level descriptions of VA's enterprise business functions and key enabling functions from the planners' and business owners' views of the Zachman framework	Continue to decompose and further define key elements of the target architecture
Generate products and populate EA repository		Repository established on VA's intranet Web site is populated with data on the planners' and owners' views of the VA architecture In FY 2003 VA plans to assess the need for another repository and the contents of that repository	Complete population of the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models		Subject matter expert review of version 1.0 of the enterprise architecture carried out by members of the Enterprise Architecture Council from VA's technical and business lines	Have subject matter experts continue to assess the enterprise architecture products for accuracy and completeness
Develop sequencing plan			
Identify gaps		July 8, 2002 sequencing plan contained in version 1.0 of EA provides a high-level overview of how VA will migrate from the current to the target architecture	Future version of the sequencing plan should identify gaps to assess the state of legacy systems, technology maturity, acquisition opportunities, and fiscal reality of the transition
Define and differentiate among legacy, migration, and new systems			Address all activities in this step
Plan migration			Address all activities in this step
Approve, publish, and disseminate EA products			Address all activities in this step

Steps in the enterprise architecture (EA) process*	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Use enterprise architecture			
Integrate EA with capital planning and investment control and systems life cycle processes		Drafted the Information Technology Integrated Management Guide, which lays out the integration of VA's EA, capital planning, investment, and project management functions Implemented the integrated capital planning, investment, and project management functions, and uses then to evaluate IT projects	Finalize and issue the Information Technology Integrated Management Guide
Train personnel		Developing a project manager training curriculum Used the annual department CIO conference to conduct an overview of the department's EA effort	Ensure that members of all EA decision-making bodies are trained in the EA process, the relationship of the EA to the capital planning and investment control process, and the system life cycle; EA training should also be provided to current and future IT project managers
Establish enforcement processes and procedures		Published the following documents, which relate to enforcement of EA processes and procedures: • VA Directive 6051 • VA EA Strategy, Governance, & Implementation • One-VA EA Implementation Plan: FY 2002 • One-VA Enterprise Architecture (version 1.0)	Develop precise definitions and criteria for compliance as well as different levels of compliance
Define compliance criteria and consequences			Address all activities in this step
Set up integrated reviews			Address all activities in this step
Execute integrated process			Address all activities in this step
Initiate new and follow-up projects			Address all activities in this step

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed as of September 2002	Examples of actions VA has taken or planned since March 2002	Examples of key actions yet to be performed
Prepare proposal			
Align project to EA			
Make investment decision			
Execute projects			Address all activities in this step
Manage and perform project development			
Evolve EA with program/project			
Assess progress			
Complete project			Address all activities in this step
Deliver product			
Assess architecture			
Evaluate results			
Consider other uses of EA			
Maintain enterprise architecture			Address all detailed activities in this step
Maintain EA as enterprise evolves			
Reassess EA periodically			
Manage projects to reflect reality			
Ensure business direction and processes reflect operations			
Ensure current architecture reflects system evolution			
Evaluate legacy system maintenance requirements against sequencing plan			
Maintain sequencing plan as integrated program plan			
Continue to consider proposals for EA modifications			

[a] Chief Information Officer Council.
[b] A repository is an information system used to store and access architectural information, relationships among the information elements, and work products.

Source: GAO analysis.

As the table indicates, immediate attention still needs to be focused on acquiring a permanent chief architect to manage the development and maintenance of the enterprise architecture.

Currently, the chief technology officer serves as the acting chief architect while the department recruits someone to fill the position on a permanent basis. According to the acting chief architect, VA anticipates filling the position in early 2003. The enterprise architecture program management office likewise needs to be fully staffed. As of September 6, 5 of the office's 16 positions had been filled. Officials expect this office to be fully staffed by the end of this year. Instituting a permanent chief architect with the requisite core competencies to lead the enterprise architecture development and fully staffing the enterprise architecture program office to support the effort, will provide vital components of management and oversight necessary for a successful enterprise architecture program.

Two quality assurance roles—those of risk manager and configuration manager—also still need to be filled. At the conclusion of our review, VA's Enterprise Architecture Council was performing risk and configuration management and its Information Technology Board was performing quality assurance functions. However, Federal CIO Council guidance recommends that the CIO make risk and configuration management the explicit responsibilities of individuals designated for those roles. The guide further recommends that the CIO establish an independent quality assurance function to evaluate the enterprise architecture.

VA must also still develop a program management plan to delineate how it will develop, use, and maintain the enterprise architecture. Such a plan is integral to providing definitive guidance for effectively managing the enterprise architecture program.

Beyond these actions, VA must continue to enhance the enterprise architecture that it has begun instituting. For example, additional work is needed to fully develop the baseline and target architectures to encompass all of the department's business functions, identify common areas of business, and eliminate duplication of processes across the organization through business process reengineering. As the initial version of the enterprise architecture notes, significant process duplication exists across the department. For example, VA identified eight different ways in which registration and eligibility are determined in the "as-is" (baseline) architecture. Nonetheless, although VA recognized opportunities for integrating and consolidating the

department's duplicate processes and functions, its initial enterprise architecture document lacked any specific guidance on how and when consolidation and integration will take place.

Also, important to the success of an enterprise architecture effort is a fully-developed enterprise architecture repository.[13] Such a system serves to highlight information interdependencies and improves the understandability of information across an organization. It also helps to significantly streamline change control by establishing linkages among the information, facilitating impact analyses, and providing for ready evaluations of change proposals. Although VA's enterprise architecture repository contains information reflecting the views of its business planners and owners, the department still needs to completely populate the repository with data that describe the interrelationships among all information elements and work products. The acting chief architect stated that, in fiscal year 2003, the department will assess its need for a different system to serve as the EA repository.

As establishment of the enterprise architecture proceeds, VA also will need to further refine its sequencing plan to identify differences between baseline and target architectures and gaps in the process, and to assess the state of legacy, migration, and new systems, and budget priorities and constraints. In addition, the acting chief architect noted that the current version of the technical reference model is generic and will require further development. Such customization is important in order to provide VA with consistent sets of service areas and interface categories and relationships used to address interoperability and open systems issues and serve as a basis for identifying, comparing, and selecting existing and emerging standards and their relationships. Such a document can also be used to organize infrastructure documentation.

According to VA officials, actions to refine and build upon the enterprise architecture are ongoing, and the department plans to issue an interim revision to the initial document within 4 to 6 months, and a completely new version by July 2003. The Enterprise Architecture Council will be responsible for developing these products. As the enterprise architecture management program moves forward, the department must ensure that it continues to sufficiently address and

[13]A repository is an information system used to store and access architecture information, relationships among the information elements, and work products.

complete all critical process steps outlined in the federal CIO guidance within reasonable time frames. With enhanced management capabilities provided by an enterprise architecture framework, VA should be able to (1) better focus on the strategic use of emerging technologies to manage its information, (2) achieve economies of scale by providing mechanisms for sharing services across the department, and (3) expedite the integration of legacy, migration and new systems.

INFORMATION SECURITY CONTINUES TO REQUIRE TOP MANAGEMENT ATTENTION

VA's information security continues to be an area of significant concern. The department relies extensively on computer systems and telecommunications networks to meet its mission of providing health care and benefits to veterans. VA's systems support many users, its networks are highly interconnected, and it is moving increasingly to more interactive, Web-based services to better meet the needs of its customers. Effectively securing these systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive medical information, and ensure the reliability of its financial data.

As this subcommittee is well aware, VA has faced long-standing challenges in achieving effective computer security across the department. Since 1998 we have reported on wide-ranging deficiencies in the department's computer security controls.[14] Among the weaknesses highlighted was that VA had not established effective controls to prevent individuals from gaining unauthorized access to its systems and sensitive data. In addition, the department had not provided adequate physical security for its computer facilities, assigned duties in a manner that segregated incompatible functions, controlled changes to its operating systems, or updated and tested its disaster recovery plans. Similar weaknesses have been confirmed by VA's inspector general, as well as through the department's own assessments of its computer security

[14]U.S. General Accounting Office, *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure,* GAO/AIMD-98-175 (Washington, D.C.: Sept. 23, 1998) and GAO-02-369T.

controls in response to government information reform legislation.[15] As evidence, since September 2001, VA has self-reported approximately 27,000 control weaknesses related to physical and logical access, segregation of duties, system and application controls, and continuity of operations. As of August 31, 2002, according to VA, about half (14,000) of these weaknesses remained unresolved.

Contributing significantly to VA's computer security problems has been its lack of a fully implemented, comprehensive computer security management program—essential to managing risks to business operations that rely on its automated and highly interconnected systems. Our 1998 report on effective security management practices used by several leading public and private organizations[16] and a companion report on risk-based security approaches in 1999[17] identified key principles that can be used to establish a management framework for more effective information security programs. This framework, depicted in figure 3, points to five key areas of effective computer security program management—central security management, security policies and procedures, risk-based assessments, security awareness, and monitoring and evaluation. Leading organizations we examined applied these key principles to ensure that information security addressed risks on an ongoing basis. Further, these principles have been cited as useful guidelines for agencies by the Federal CIO Council and incorporated into the council's information security assessment framework,[18] intended for agency self-assessments.

---

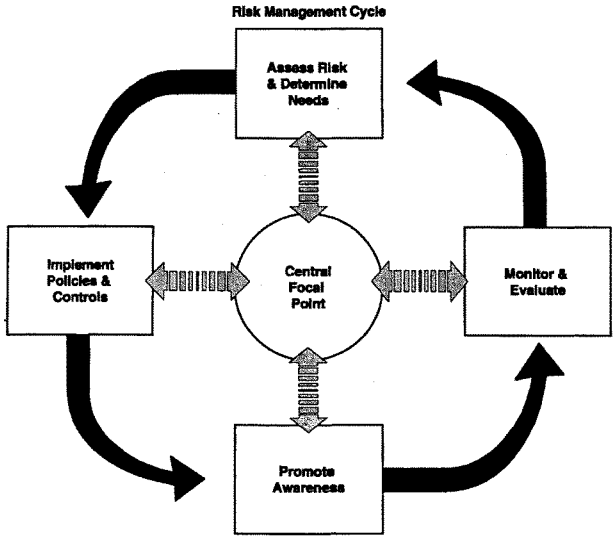
[15]The government information security reform provisions of the fiscal year 2001 Defense Authorization Act (P.L. 106-398) require annual agency program reviews and annual independent evaluations for both non-national security and national security information systems.

[16]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[17]U. S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D. C.: November 1999).

[18]Chief Information Officers Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000).

Figure 3: Information Security Risk Management Framework



Source: GAO/AIMD-98-68.

When we testified before the subcommittee in March, VA had begun a number of actions to strengthen its overall computer security management posture. For example, the Secretary had instituted information security standards for members of the department's senior executive service to provide greater management accountability for information security. In addition, VA's cyber security officer had organized his office to focus more directly on the critical elements of information security control that are defined in our information systems controls audit methodology.[19] The cyber security officer also had updated the department's security

[19] U.S. General Accounting Office, *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

management plan, outlining actions for developing risk-based security assessments, improving the monitoring and testing of systems controls, and implementing departmentwide virus-detection software and intrusion-detection systems. The plan placed increased emphasis on centralizing key security functions that were previously decentralized or nonexistent, including virus detection, systems certification and accreditation, network management, configuration management, and incident and audit analysis.

Nonetheless, while VA had completed a number of important steps, its security management program continued to lack essential elements required for protecting the department's computer systems and networks from unnecessary exposure to vulnerabilities and risks. For example, while the department had begun to develop an inventory of known security weaknesses, it had not instituted a comprehensive, centrally managed process that would enable it to identify, track, and analyze all computer security weaknesses. Further, the updated security management plan did not articulate critical actions that VA would need to take to correct specific control weaknesses or time frames for completing key actions.

Progress Continues, But Actions Still Needed To Achieve a Comprehensive Security Management Program

Since March, the department has taken important steps to further strengthen its computer security management program. For example, the cyber security officer has updated and expanded the department's information security policies and procedures, placing increased emphasis on better securing and overseeing the department's computer environment. More recently, as discussed earlier, VA's realignment of its information technology resources placed administration and field office security functions more directly under the oversight of the department's CIO.

VA has also acted to help provide a more solid foundation for detecting, reporting, and responding to security incidents. For example, it has contracted to acquire an expanded departmentwide incident response and analysis capability, to include enhanced security monitoring and detection. Further, it has enhanced its computer virus detection program by providing technical training to operational staff and distributing antivirus patches for known

viruses to affected systems. In addition, VA has initiated a multiyear project intended to consolidate, protect, and centrally manage external connections to its critical financial, medical, and benefits systems. This project, with full implementation planned for September 2004, is expected to reduce the approximately 200 external computer network connections that the department now relies on to about 10. By reducing these connections, VA should be better positioned to effectively reduce its risk of unauthorized access to its critical systems.

As was the case last March, however, VA's actions have not yet been sufficient to fully implement all of the key elements of a comprehensive computer security management program. In assessing the department's recent corrective actions relative to our information security risk management framework, VA still needs to accomplish a number of critical tasks that are essential to successfully achieving a comprehensive and effective computer security management program. Table 2 summarizes the steps that VA still needs to accomplish in order to fully implement a comprehensive program.

Table 2: Actions Needed to Ensure a Comprehensive Computer Security Management Program

Important elements of a computer security management program[a]	Actions needed as of March 2002	Actions VA has taken since March 2002	Actions still needed
Central security management function to guide and oversee compliance with established policies and procedures and review effectiveness of the security environment	Ensure that full-time security officers or staff with primary duty for security are assigned to information security officer (ISO) positions and clearly define their roles and responsibilities Develop guidance to ensure authority and independence of security officers Develop policies and procedures to ensure departmentwide coordination of security functions	Established a tracking mechanism to identify security officers and the systems under their respective purview at each location VA Secretary centralized the department's IT program, including authority, personnel, and funding, in the Office of the Chief Information Officer	Ensure that full-time security officers or staff with primary duty for security are assigned to all ISO positions and clearly define their roles and responsibilities In conjunction with VA's centralization of the IT program, develop policy and guidance to ensure (1) authority and independence for security officers and (2) departmentwide coordination of security functions
Security policies and procedures that govern a complete computer security program and integrate all security aspects of an organization's environment, including local area networks, wide area networks, and mainframe security	Refocus department policy to address security from an interconnected VA systems environment perspective in addition to that of individual systems Develop and implement technical security standards for mainframe and other systems and security software	Developed policies to address external connections and standards for public key infrastructure authentication	Develop specific policy to address security interconnectivity of all internal and external VA systems Develop and implement technical security standards for mainframe and other systems and security software
Periodic risk assessments to assist management in making decisions on necessary controls to help ensure that security resources are effectively distributed to minimize potential loss	Include best minimum standards or guidance for performing risk assessments in methodology Develop guidance for determining when an event is a significant change and explaining the level of risk assessment required for these system changes		Include best minimum standards or guidance for performing risk assessments in methodology Develop guidance for determining when an event is a significant change and explaining the level of risk assessment required for these system changes
Security awareness to educate users about current information security risks, policies, and procedures	Establish a process to ensure program compliance		Establish a process to ensure program compliance

Important elements of a computer security management program[a]	Actions needed as of March 2002	Actions VA has taken since March 2002	Actions still needed
Monitoring and evaluating computer controls to ensure their effectiveness, improve them, and oversee compliance	Develop specific requirements for conducting a compliance review program		Develop specific requirements for conducting a compliance review program
	Develop an ongoing program for testing controls to include assessments of both internal and external access to VA systems; expand current tests to identify unauthorized or vulnerable external connections to VA's network	Initiated a multiyear project to consolidate, protect, and centrally manage external connections to VA systems	Develop an ongoing program for testing controls to include assessments of both internal and external access to VA systems; expand current tests to identify unauthorized or vulnerable external connections to VA's network
	Establish a process for tracking the status of security weaknesses, corrective actions taken, and independent validation of the corrective actions	Developed a process for tracking the status of computer security weaknesses and corrective actions taken	Develop a process to independently validate corrective actions taken
	Develop a process for routinely analyzing the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve security	Developed an ad hoc approach for identifying computer control weaknesses for review	Develop a process that emphasizes routinely analyzing the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve security
	Develop a proactive security incident response program to monitor user access for unusual or suspicious activity	Awarded contract for an expanded security incident response and analysis program to include security monitoring and detection capability for external user access activities Enhanced computer virus detection program by providing technical training to operational staff and distributing antivirus patches	Develop a proactive security incident response program to provide for both internal and external monitoring of user access to identify unusual or suspicious activities

[a]GAO/AIMD-98-68.

Source: GAO.

The department's critical remaining actions include routinely monitoring and evaluating the effectiveness of security policies and controls and acting to address identified weaknesses. These tasks aid organizations in cost effectively managing their information security risks rather than reacting to individual problems after a violation has been detected. We have previously recommended that VA establish a program involving ongoing monitoring and evaluation to ensure the effectiveness of its computer control environment. An effective program framework would include a description of the scope and level of testing to be performed, specific control areas to be tested, the frequency of testing, and the identity of responsible VA units. In addition, testing and evaluation would include penetration tests and reviews of the computer network, as well as compliance reviews of all computer control areas, including logical and physical access controls; service continuity tests; and system and application integrity and change controls performed on a scheduled basis.

VA has begun placing greater emphasis on controlling its security risks; however, its current framework does not yet include some of the essential elements required to achieve a formal program for monitoring and evaluating computer controls. For example, while the department has conducted some tests of its control environment, including penetration tests and reviews of its computer network, this effort has largely been performed in an ad hoc manner, rather than as part of a formal, ongoing program. Further, while VA has established a departmental process for assessing computer controls, the process relies on VA's offices to self-report computer control weaknesses, with no independent validation component to ensure the accuracy of reporting.

Similarly, an effective computer security management program should include a process for ensuring that remedial action is taken to address significant deficiencies and that it provides steps to analyze weaknesses reported for identifiable trends and vulnerabilities, and to apply appropriate countermeasures as needed. Although VA has established a system for tracking corrective actions, it has not developed a process for independently validating or reviewing the appropriateness of the corrective actions taken. Further, the department currently lacks a process to routinely analyze the weaknesses reported, limiting its effectiveness at identifying systemic problems that could adversely affect critical veterans information systems departmentwide. Finally, although VA has developed a framework for addressing departmentwide computer

security, it has not yet established a mechanism for collecting and tracking performance data, ensuring management review when appropriate, or providing for independent validation of program deliverables. Until it addresses all key elements of a comprehensive computer security management program and develops a process for managing the department's security plan, VA will not have full assurance that its financial information and sensitive medical records are adequately protected from unauthorized disclosure, misuse, or destruction.

VBA REMAINS FAR FROM FULL IMPLEMENTATION OF THE VETSNET COMPENSATION AND PENSION REPLACEMENT SYSTEM

Mr. Chairman, we continue to be concerned about the slow progress that VBA is making in implementing the VETSNET compensation and pension replacement system. As you know, VBA currently relies on its aging Benefits Delivery Network to deliver over 3.5 million benefits payments to veterans and their dependents each month.[20] The compensation and pension replacement effort grew out of an initiative that VBA undertook in 1986 to replace its outdated BDN and modernize its compensation and pension, education, and vocational rehabilitation benefits payment systems. After several false starts and approximately $300 million spent on the overall modernization, the administration revised its strategy in 1996 and began focusing on modernizing the compensation and pension (C&P) payment system.

VBA has now been working on the C&P replacement initiative for more than 6 years, but continues to be far from full implementation of the new payment system. As we reported last March, long-standing, fundamental deficiencies in VBA's management of the project hindered successful development and implementation of the system. For example, the initiative was proceeding without a project manager, and VBA had not obtained essential field office support for the new software being developed. In addition, users' requirements for the new system had not yet been assessed or validated to ensure that VETSNET would meet business needs; and testing of the system's functional business capability, as well as end-to-end testing to ensure that

[20]Parts of the Benefits Delivery Network were developed in the 1960s.

accurate payments would be delivered, still needed to be completed. Finally, VBA had not developed an integrated project plan to guide its transition from BDN to the new system.

This past June, we recommended that, before approving any new funding for the replacement system, the Secretary should ensure that actions are taken to address our long-standing concerns about VBA's development and implementation of the system. These recommended actions included (1) appointing a project manager to direct the development of an action plan for, and oversee the complete analysis of, the current system replacement effort; (2) finalizing and approving a revised C&P replacement strategy based on results of the analysis and implementing an integrated project plan; (3) developing an action plan to move VBA from the current to the replacement system; and (4) developing an action plan to ensure that BDN will be available to continue accurately processing benefits payments until the new system is deployed.[21] The department concurred with our recommendations, and stated that actions were either under way or planned to implement them.

Actions Taken in Recent Months

Since our March testimony and subsequent recommendations, VBA has acted to further its development and implementation of the C&P replacement system. Among these actions VBA began recruiting a full-time project manager in June, and, according to the deputy CIO for VBA, expects to fill this position by the end of this month. In addition, to obtain field office and program support, in late March VBA formalized an implementation charter that established a VETSNET executive board and a project control board.[22] These entities are expected to provide decision support and oversee progress on the implementation. VBA has also begun revalidating functional business requirements for the new system. Its July 10, 2002 status report called for

[21]U .S. General Accounting Office, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results,* GAO-02-703 (Washington, D.C.: June 12, 2002).

[22]The executive board meets monthly and consists of VBA's chief financial officer, deputy chief information officer, director of compensation and pension service, and director of field operations. The project control board meets weekly and comprises representatives from the Office of Information Management, Compensation and Pension Service, Office of Resource Management, Field Operations, and the Program Analysis and Integrity Office. It is codirected by a business project manager and a technical project manager.

validating the majority of its requirements by the end of this month, and to complete all requirements validation by January 2003. The report also identified actions needed to transition VBA from the current to the replacement system. Further, in July VBA hired a contractor to obtain support for testing the VETSNET system applications. The contractor has been tasked with conducting functional, integration, and linkage testing, as well as software quality assurance for each release of the system applications.

Much Work Remains

Nonetheless, VBA still has significant work to accomplish, and completing its implementation of the new system could take several years. All but one of the software applications comprising the new system still need to be fully deployed or developed, and VBA is currently processing only nine benefits claims using its new software products.[23] As described in VA's August 2002 Compensation and Pension Replacement System Capital Asset Plan, the C&P replacement strategy incorporates six software applications: (1) Share, (2) Modern Award Processing - Development, (3) Rating Board Automation 2000, (4) Award Processing, (5) Finance and Accounting System, and (6) Correspondence. These applications are being designed to support the processing of initial benefits claims for service-connected disabilities, as shown in table 3.

[23]As part of a pilot test in February 2001, VBA began processing ten original benefits claims using its new software. However, according to VBA, one veteran included in the pilot moved to West Virginia, and his payment is now being delivered by the BDN.

Table 3: C&P Replacement System's Support of Initial Disability Claims Processing

C&P Replacement System Software Application	Initial Disability Claims Processing and Benefit Payment Functions
Share (establishment)	*Establish the claim*—regional office enters basic information provided by the veteran into a computer system and sets up a claim file folder
Modern Award Processing – Development (MAP-D)	*Develop the claim*—regional office reviews the claim file folder for military service and medical information, requests and obtains missing information, and assesses information to determine basic eligibility
Rating Board Automation 2000 (RBA 2000)[a]	*Rate the claim*—regional office analyzes the veteran's service records and service and private medical records and determines the veteran's level of disability
Award Processing (AWARD)	*Authorize the claim*—regional office reviews previous work on the claim, approves the initiation of benefit payments, and notifies the veteran of the decision
Finance and Accounting System (FAS)	*Pay beneficiary*—regional office enters data into computer system to generate and make payment to veterans
Correspondence	*Notify veteran*—regional office sends letters informing veterans of the status of actions to process their claims

[a]The Search and Participant Profile application is used in conjunction with RBA 2000 and pulls information from the corporate database when reopened claims are rated and is transparent to the user. Until recently, this application had been counted separately.

Source: GAO analysis.

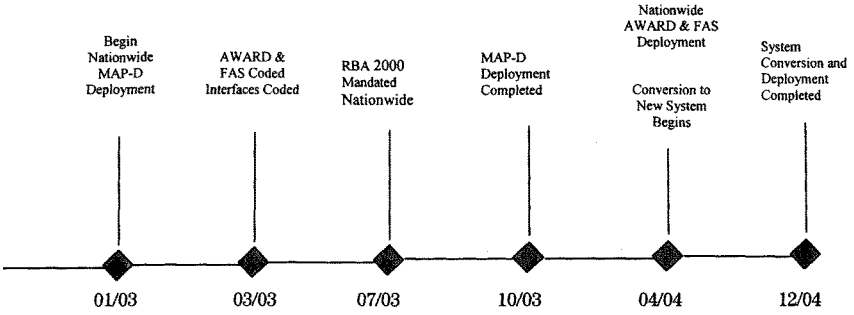
VBA still has numerous tasks to accomplish before these software applications can be fully implemented. Although, last year, the administration implemented its rating board automation tool (RBA 2000), it will not require all of its regional offices to use this software until July 2003. In addition, our recent follow-up work determined that two of the software products continue to be in various stages of deployment. Specifically, among the 57 regional offices that are expected to benefit from the replacement system, only 6 are currently using Share to establish a claim; VBA still needs to implement the tool in the 51 other regional offices. In addition, only two regional offices—Salt Lake and Little Rock—have pilot-tested and are currently using MAP-D to assist in the development of most compensation claims. VBA still needs to implement this tool in 55 other regional offices. Full implementation is currently estimated for October 2003.

Further, three software applications—AWARD, FAS, and Correspondence—continue to require development. According to VBA officials, when implemented, AWARD will record award

lecisions and generate, authorize, and validate on-line awards for veterans and interface with Correspondence to develop the notification letter for the veteran. FAS will provide the accounting benefits payments functions and will include an interface with the Department of the Treasury.

VBA expects to complete software coding for AWARD and FAS by March 2003. Based on its most recent estimates, it expects to begin nationwide deployment of the two systems in April 2004. Once these activities are accomplished, VBA plans to begin its conversion to the new system, with a completion date currently set for December 2004. Figure 4 depicts VBA's current time line for the full implementation of the system.

Figure 4: VBA's Time Line for Completing and Implementing the Compensation & Pension Replacement Payment System (as of July 2002)



◆ Milestone
Source: Veterans Benefits Administration.

Maintaining Benefits Delivery Network Operations Is Critical to Ensuring Continued Payments to Veterans

Given its current schedule for implementing the C&P replacement system, VBA will have to continue relying on BDN to deliver compensation and pension benefits payments until at least the beginning of 2005. However, with parts of this system nearing 40 years old, without additional maintenance, BDN's capability to continue accurately processing benefits payments is uncertain. Our concerns have been substantiated by the VA claims processing task force, which in its October 2001 report warned that the system's operations and support were approaching a critical stage and that its performance could potentially degrade and eventually cease.[24]

Since March, VBA has taken steps to help ensure that BDN can be sustained and remains capable of making prompt, uninterrupted payments to veterans. For example, VBA has (1) completed an upgrade of BDN hardware, (2) hired 11 new staff members dedicated to BDN operations, and (3) successfully tested a contingency plan. Further, according to VBA's deputy CIO, the administration has developed an action plan outlining strategies for keeping BDN operational until the replacement system is implemented. Nonetheless, the risks associated with continual reliance on BDN remain—one of the system's software applications (database monitor software) is no longer supported by the vendor, nor is it used by any other customer.

GOVERNMENT COMPUTER-BASED PATIENT RECORD INITIATIVE HAS CHANGED NAME, GOALS, STRATEGY

Finally, Mr. Chairman, I would like to provide updated information on VA's progress, in conjunction with the Department of Defense (DOD) and the Indian Health Service (IHS), in achieving the ability to share patient health care data as part of the government computer-based patient record (GCPR) initiative. As you know, the GCPR project was developed in 1998 out of VA and DOD discussions about ways to share data in their health information systems and from

[24]The claims processing task force was formed in May 2001, when the Secretary of Veterans Affairs asked a group of individuals with significant experience to assess and critique VBA's compensation and pension organization, management, and processes, and to develop recommendations to significantly improve VBA's ability to process veterans' claims for disability compensation and pensions.

efforts to create electronic records for active duty personnel and veterans. IHS became involved because of its experience in population-based research and its long-standing relationship with VA in caring for the Indian veteran population, as well as its desire to improve the exchange of information among its facilities.

GCPR was originally envisioned to serve as an electronic interface that would allow physicians and other authorized users at VA, DOD, and IHS health facilities to access data from any of the other agencies' health facilities by serving as an electronic interface among their health information systems. The interface was expected to compile requested patient information in a temporary, "virtual" record that could be displayed on a user's computer screen.

Last March we expressed concerns about the progress that VA, DOD, and IHS had made toward implementing GCPR. We testified that the project continued to operate without clear lines of authority or a lead entity responsible for final decision-making. The project also continued to move forward without comprehensive and coordinated plans, including an agreed-upon mission and clear goals, objectives, and performance measures. These concerns were originally reported in April 2001,[25] when we recommended that the participating agencies (1) designate a lead entity with final decision-making authority and establish a clear line of authority for the GCPR project, and (2) create comprehensive and coordinated plans that included an agreed-upon mission and clear goals, objectives, and performance measures, to ensure that the agencies can share comprehensive, meaningful, accurate, and secure patient health care data. VA, DOD, and IHS all agreed with our findings and recommendations.

Our March testimony also noted that the scope of the GCPR initiative had been narrowed from its original objectives and that the participating agencies had announced a revised strategy that was considerably less encompassing than the project was originally intended to be. Specifically, rather than serve as an interface to allow data sharing across the three agencies' disparate systems, as originally envisioned, a first (near-term) phase of the revised strategy had called only

[25]U.S. General Accounting Office, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing,* GAO-01-459 (Washington, D.C.: Apr. 30, 2001).

for a one-way transfer of data from DOD's current health care information system to a separate database that VA hospitals could access.

Subsequent phases of the effort that were to further expand GCPR's capabilities had also been revised. A second phase that would have enabled information exchange among all three agencies had been re-scoped to enable only a bilateral read-only exchange of data between VA and IHS. Plans for a third phase involving the expansion of GCPR's capabilities to public and private national health information standards groups were no longer being considered for the project, and there were no plans for DOD to receive data from VA.

GCPR is Proceeding Under a New Name and Strategy

In May, VA and DOD proceeded with implementing the revised strategy. It finalized a memorandum of agreement that designated VA as the lead entity in implementing the project and formally renamed the project the Federal Health Information Exchange (FHIE) Program. According to program officials, FHIE is now a joint effort between DOD and VA that will enable the exchange of health care information in two phases. The first phase, or near-term solution, is to enable the one-way transfer of data from DOD's existing health care information system to a separate database that VA hospitals can access. Nationwide deployment and implementation of the first phase began in late May of this year, and was completed in mid-July.

FHIE was built to interface with VA's and DOD's existing systems. Specifically, electronic data from separated service members contained in DOD's Military Health System Composite Health Care System are transmitted to VA's FHIE repository, which can then be accessed through the Computerized Patient Record System (CPRS) in VA's Veterans Health Information Systems and Technology Architecture (VISTA). Clinicians are able to access and display the data through CPRS remote data views.[26] The data currently available for transfer include demographic[27] and

[26]The CPRS remote data views is an application that allows authorized users to access patient health care data from any VA medical facility.

[27]The demographic information consists of patient name, DOD eligibility category, Social Security number, address, date of birth, religion, primary language, sex, race, and marital status.

certain clinical information, such as laboratory results, outpatient pharmacy data, and radiology reports on service members that have separated from DOD.

The final phase of the near-term solution is anticipated to begin this October. According to VA and DOD officials, this phase is intended to broaden the base of health information available to VA clinicians through the transfer of additional health information on separated service members. This additional information is expected to consist of discharge summaries;[28] allergy information; admissions, disposition, and transfer information; and consultation results that include referring physicians and physical findings. Completion of this final phase of FHIE is scheduled for September 2003. VA and DOD have budgeted $12 million in fiscal year 2003 ($6 million for each agency) to cover completion and maintenance of the near-term effort.

VA and DOD Report Success in Implementing the First Phase of FHIE

FHIE is currently available to all VA medical centers, and according to program officials, is showing positive results. The officials stated that, presently, the FHIE repository contains data on almost 2 million unique patients. This includes clinical data on over 1 million service personnel who separated between 1987 and 2001. The data consist of over 14 million lab messages, almost 14 million pharmacy messages, and over 2 million radiology messages.

Program officials stated that the quick retrieval and readability of data contained in the FHIE repository has begun providing valuable support to VA clinicians. They stated that FHIE is capable of accommodating up to 800 queries per hour, with an average response rate of 14 seconds per query. For the week beginning July 29, 2002, VA clinicians made 287 authorized queries to the database. In addition, when a clinician at a VA medical facility retrieves the data transmitted from DOD, the data appear in the same format as the data captured in CPRS, further facilitating its use. During a demonstration of the data retrieval capability, a clinician at VA's Washington, D.C., medical center told us that the information provided through FHIE has proven particularly valuable for treating emergency room and first-time patients. He added that

[28] Discharge summaries will include inpatient histories, diagnoses, and procedures.

additional data anticipated from the second phase of FHIE should prove to be even more valuable.

VA and DOD Developing
Interoperable Health Systems

Beyond FHIE, VA and DOD have envisioned a long-term strategy involving the two-way exchange of clinical information. This initiative has been termed HealthePeople (Federal). According to VHA's CIO and the Military Health System CIO, VA and DOD are jointly implementing a plan that will result in computerized health record systems that ensure interoperability between DOD's Composite Health Care System II and VA's HealtheVet VISTA to achieve the sharing of secure health data required by their health care providers.[29] In order to accomplish this objective, the two agencies intend to standardize health and related data, communications, security, and software applications where appropriate. As part of HealthePeople (Federal), IHS is also expected to be actively involved in helping to develop national standards and compatible software applications to further the standardization of data, communications, and security for health information systems. When our review concluded, VA and DOD had just begun this initiative, with a focus on addressing the standardization issue. At that time, they anticipated implementing this exchange of clinical information by the end of 2005.

* * * * *

In summary, Mr. Chairman, VA continues to make important progress toward improving its management of information technology, with the attention and support of its executive leadership contributing significantly to ongoing actions to improve key areas of IT performance. The restructuring of responsibility and accountability directly to the CIO is a particularly important step—one that could set the stage for VA truly achieving its One-VA vision. In addition, actions aimed at further developing the department's enterprise architecture and improving computer security management continue to help solidify the IT foundation necessary

[29]Both of these systems are currently under development.

to guide VA's development and protection of critical information systems and data that are vital to its mission. Finally, although under a revised, scaled-down initiative, VA and DOD have made some progress in achieving the capability to share health care data on military personnel and veterans. Yet, challenges remain. Ensuring that the enterprise architecture will be fully implemented and sustained beyond the current leadership necessitates that the department establish a program management structure to guide and oversee this critical initiative. Completing its comprehensive computer security management program is also essential to ensure that the department can effectively safeguard its assets and sensitive medical information. Further, the urgency that VA faces in replacing its aging BDN continues to grow, while much must be accomplished before full implementation of the compensation and pension replacement system. Instituting the necessary processes and controls to guide VA's information technology programs and investments will be vital to ensuring that the department does not fall short of its goals of enhancing operational efficiency and, ultimately, improving service delivery to our nation's veterans.

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

CONTACTS AND ACKNOWLEDGMENTS

For information about this testimony, please contact me at (202) 512-6253 or by e-mail at willemssenj@gao.gov. Individuals making key contributions to this testimony include Nabajyoti Barkakati, Nicole Carpenter, Kristi Dorsey, David W. Irvin, Min S. Lee, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, and Charles M. Vrabel.

(310441)

Statement of

Dr. John A. Gauss

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 26, 2002

Good morning, Mr. Chairman and members of the Subcommittee. On behalf of the Secretary of Veterans Affairs, I am pleased to have this opportunity to come here today and update you on the progress the Department has made in strengthening our Information Technology program, and specifically address issues relating to:

- VA's Enterprise Architecture;
- VA's Cyber Security program;
- The recent realignment of the Department's IT structure; and,
- Issues raised at the March 13, 2002, IT hearing.

On March 13, 2002, I appeared before this Subcommittee and gave you my personal commitment to reform the way VA uses information technology. I committed to:

- Publishing an approved Enterprise Architecture Implementation Plan by no later than 30 April 2002;
- Ensuring that networks and systems we depend upon are made secure and available;
- Personally overseeing VETSNET to ensure its progress meets the projected time of being ready to deploy by April 2004 or recommending to the Secretary that the effort be terminated; and,
- Conducting a deployment review for the Government Computer Based Patient Records (GCPR) program to ensure a quality product can be effectively deployed.

With respect to Enterprise Architecture (EA), the Department published a detailed Implementation Plan on April 22, 2002, and undertook the development

of the initial version of the One-VA Enterprise Architecture. As a result of successfully executing the Implementation Plan, the Secretary approved version 1.0 of the One-VA Enterprise Architecture on September 5, 2002. It provides a clear pathway for the transformation of both business processes and Information Technology to support these business processes across the Department.

Version 1.0 of the One-VA EA establishes ten Enterprise Business Functions (EBFs) and seven Key Enabling Functions (KEFs) that provide a top-level view of the Department's operations from a top-down, business-focused perspective. These EBFs and KEFs are as follows:

Enterprise Business Functions
- Compensation
- Pension
- Vocational Rehabilitation & Employment
- Education
- Insurance
- Home Loan Guaranty
- Memorials & Burial
- Medical Care
- Medical Education
- Medical Research

Key Enabling Functions
- Finance and Accounting
- Acquisition & Materiel Management
- Information Technology
  - Telecommunications
  - Cyber Security
  - Data Center COOP
- Human Resources
- Training & Education
- Registration & Eligibility
- Contact Management

Several of these EBFs and KEFs were identified as significant opportunities for functional consolidation and integration to collapse redundant processes and the duplicative IT systems that support them and implement a transformational, One-VA approach to dealing with veterans. These include Registration and Eligibility that will collapse eight separate business processes into one, and Contact Management that will provide a single multi-media face for the Department in interacting with veterans and collapse five redundant business processes into one. They also include the Health Data Repository (HDR), which will set the foundation for transforming VA medical care from "facility centric" to "patient centric" health care.

From the perspective of Information Technology Infrastructure to support the EBFs and KEFs, the One-VA EA describes the distributed computing model and technical architecture for the future. The top layer of the model represents how data and applications will interrelate in the future. It is where VA will implement the functional consolidation described previously in One-VA Registration and Eligibility, Contact Management and Health Data Repository.

The layer below the data/applications layer represents corporate and regional computing services to store the data and run the applications. VA will consolidate corporate data center operations to establish a single corporate data center distributed across three widely dispersed locations. These three locations

will operate under a single management structure and be linked with one another with high performance data telecommunications so they appear logically as a single entity. They will provide Continuity of Operations (COOP) support for electronic data vaulting, applications restart and business process restart in the event of a disaster. Regional data centers will also support the EA's distributed computing model in transitioning VA from a "facility centric" computing environment to a "network centric" computing environment to support mid-tier and office automation capability. In the end state, this effort will remove many servers from end user facilities and replace them in regional locations with COOP capability designed in. This will lead to significant reduction in hardware costs for the future, reduce the skills required at the local level to operate and maintain the capability, and significantly enhance our cyber security posture.

The next lower layer in the distributed computing model is for cyber security functions to protect the computing infrastructure against cyber attack. The bottom layer is a One-VA national data network. We are well on our way to implementing the One-VA data network and the Cyber Security functions to protect our computing environment.

Specific progress since the last hearing follows:

- The Department of Veterans Affairs "One-VA Enterprise Architecture Implementation Plan: FY 2002" was approved on April 22, 2002;
- The Secretary approved the Department of Veterans Affairs "One-VA Enterprise Architecture Version 1.0" on September 5, 2002;
- Staffing has been approved for the Enterprise Architecture Office and recruitment for these positions is underway; and,
- The position for an SES level Chief Architect has been approved and recruitment for this position is underway.

As I discussed in my March 13, 2002, testimony before this Subcommittee, our current data network is overly complex, too expensive for the performance it provides, and does not have an enterprise-wide network management capability. This complexity and lack of network management capability seriously impede our ability to properly secure and assure network services. To correct these deficiencies, we have embarked on a project to re-architect our data network and change the network from a circuit-based network to a performance-based network. The VA Strategic Management Council reviewed and the Deputy Secretary has approved executing the first phase of this project. The detailed Business Case Analysis, Cost Benefit Analysis, Return on Investment Analysis, and Analysis of Alternatives were completed. These analyses showed that converting our data network from a circuit-based network to a performance-based network will:

- Simplify the complexity;
- Substantially improve performance in support of our EA efforts;
- Establish a network management capability;
- Significantly improve the security and assurance of service; and,

- Provide savings to our current data network budget.

Phase I of this project involved the transfer of responsibility for the Operations & Maintenance of the data network backbone to SPRINT, one of the FTS2001 telecommunications providers. Phase I also involves standardizing equipment and software configurations across the data network backbone. Phase I will be complete by the end of this month. Since transferring this responsibility to SPRINT in April 2002, we have significantly improved network backbone effective throughput and reliability. The next phase of this project will optimize the network's backbone performance. We will start this optimization next week.

With respect to cyber security, the Department has made significant progress in correcting the deficiencies identified by our Office of Inspector General (OIG) and the General Accounting Office (GAO). This year, the Department fielded one of the largest anti-virus capabilities in the world, as well as awarded a multi-year contract to significantly enhance the VA's central incident response capability.

VA recently established a global anti-virus capability to protect the over 140,000 desktops connected to VA's Intranet from malicious attack. To date, over two million viruses have been successfully detected and eradicated. This effort is continuing through providing additional role-based training to ensure that IT personnel are knowledgeable about associated equipment operating characteristics and maintenance requirements; hardening servers consistent with optimized site configuration; and, establishing an Anti-virus analytical and warning capability. This capability uses an automated tool that, within minutes of a virus attack on a VA computer, can identify the incident by virus type, version, and specific location of the equipment under attack. When a virus attack is detected, a warning is concurrently sent to the VA Central Incident Response Capability (VA-CIRC), which will issue a Department-wide anti-virus alert.

After a rigorous several-month effort, a contract to significantly upgrade the capabilities of our VA-CIRC was awarded during July. The contract winner, which is now known as the VA Security Team, or VAST, is a consortium of five small businesses, led by SecureInfo Corporation. There are three large companies that are under subcontract to provide specific niche services when required. In the near future, this enhanced VA-CIRC capability will become the nucleus of all VA information and Internet security operations nationwide, providing such global services as firewall management and Intrusion Detection System (IDS) monitoring.

The VA anti-virus program will be integrated with the enhanced VA-CIRC capability, and associated vendor releases, security bulletins, security alerts, and patch distribution will be tailored for the specific existing configuration of each VA facility. This will afford immediate management attention to priority issues, instead of the current situation wherein IT staff and security personnel must evaluate all alerts for relevancy to their operations. The VA-CIRC has begun

testing the effectiveness of facility-implemented security controls through vulnerability and penetration scanning tests. This exemplifies the total "cradle to grave" solution that is required to effectively address emerging threats to VA's networks on an expedient basis.

In addition to the anti-virus and VA-CIRC efforts, the Department is continuing to deploy other specifically focused initiatives developed during the past year to correct IT security weaknesses identified in our annual Government Information Security Act (GISRA) self-assessment survey process. These programs include our Enterprise Cyber Security Infrastructure Project (ECSIP), the Information Security Technology Certification and Accreditation Program (ITSCAP), and our newly-established Cyber Security Professionalization and Compliance Programs.

The ECSIP program, which was discussed during the March testimony, will implement Department-wide intrusion detection, and firewall capability with a concurrent significant reduction in external network gateways. This project, which was approved by the Department's Strategic Management Council in February 2002, coincides with VA's telecommunications network modernization. As part of the project, we plan to systematically collapse the over 200 existing external network gateways in VA into a more manageable number and efficient structure. Concurrent with this effort, Department-wide IDS capability will be incrementally deployed on a strategic basis to provide significantly increased security protections for these gateways. The IDS effort will include real-time analytical incident support, as well as information sharing capabilities regarding emerging threats and vulnerabilities. Design and implementation efforts for this standardized architecture and configuration are underway and we anticipate deploying the initial capability during the first quarter of calendar year 2003.

ITSCAP, the Department's comprehensive Certification and Accreditation (C&A) process, will ensure that IT systems undergo a rigorous security review prior to being authorized to process sensitive data. An accompanying ITSCAP Handbook of procedures and guidance, which articulates the specific actions, document reviews, and required analyses associated with the C&A process, places increased emphasis on the system and/or major application security plan, and on physical security, through a "site-specific" accreditation process.

The Department's newly-established Cyber Security Professionalization Program (CSPP) will provide general and role-specific training, career progression, and incentives targeted toward development of a highly skilled and motivated cadre of VA cyber security practitioners. In addition to existing VA Information Security Officer (ISO) training modules, other elements being considered for inclusion in the CSPP include: training and testing specific to Federal and VA guidelines for IT security; training and testing specific to topical areas included in industry-recognized professional certifications; and, career development opportunities through formalized position descriptions which delineate a range of ISO skill levels to support Department-wide career paths.

Additionally, the CSPP will provide professional certifications for those VA employees who meet stringent qualifications through combinations of training, testing, and experience. The Department will maintain pertinent information on individual cyber security practitioner certification status, evaluate the proficiency of current credential holders on a periodic basis, and take appropriate action to suspend and/or revoke cyber security practitioner credentials for any individual who fails to adhere to established standards.

A Compliance Program will provide independent verification of adherence to Department security policies and procedures through continual assessment of documentation archived in the Department's GISRA database, and subsequent periodic site visits to verify and test related IT security control implementation. The results of these reviews will be provided to facility directors and Department senior management personnel to ensure that personnel initiate prompt action to correct identified deficiencies. Additionally, the reviews will be used to develop a process for routinely identifying trends and vulnerabilities, and applying appropriate countermeasures to improve security.

The Secretary approved the establishment of the professionalization and compliance programs to respond to concerns expressed by the OIG regarding the unevenness of reporting in the Department's GISRA database, as well as to preclude instances such as the one that occurred in the Indianapolis Medical Center this past spring.

In summary of our cyber security efforts, we are building a strong foundation for our IT program, but much remains to be done.

In a memorandum signed by the Secretary on August 6, 2002, he directed that all IT personnel and resources be centralized under the Office of Information and Technology. The first action I took was to assign the Administration Chief Information Officers to be Department Deputy CIOs for Health, Benefits and Memorial Affairs. Further, the senior IT manager in each Central Office staff office that operates and maintains IT networks and equipment now report directly to me.

Initially, I have focused on establishing a clear, unambiguous reporting chain for the Department's cyber security efforts. We have developed an organizational structure that combines the cyber security staff elements of the Administrations with the Central Office's Cyber Security staff, thereby creating a single integrated cyber security program office for the Department. Further, field Information Security Officers (ISOs) at the VHA VISN level and at the VBA Network Service Center (NSC) level will become direct reports to the Office of Cyber Security early next fiscal year. Within each hospital, regional office and at each cemetery, the ISOs will report directly to their respective facility director rather than the inconsistent manner of reporting in the past. The VISN and NSC ISOs will provide functional cyber security direction to the facility ISOs, and conduct

periodic inspections of the Cyber Security activities at each facility under their purview. The facility ISOs will be required to submit weekly reports as to each facility's cyber security health and welfare.

With respect to financial accountability, I am requiring financial execution plans, or spend plans, to be submitted to me for approval prior to the start of each fiscal year. These spend plans define what work will be done, who will do the work, how much will be spent and when it will be spent. I am pleased to report that I have received these spend plans for fiscal year 2003 that cover the planned IT expenditures for each administration. I am also pleased to report that the quality of these spend plans far exceeded my expectations for the initial submission. These spend plans will give my office the opportunity to drill down into each planned expenditure to ensure that they will not only satisfy mission need but will also comply with the recently published version 1.0 of the Enterprise Architecture. Although the quality of the initial spend plan submissions far exceeded my expectations, some spend plans require additional work to provide a greater degree of detail. This work will be completed prior to the end of the calendar year.

I have convened a group of senior leaders from the Department to develop a detailed reorganization package to submit to the Secretary no later than November 1, 2002. This reorganization package will provide the detail associated with the specific centralization of authority from an organizational perspective, and provide detailed staffing descriptions for each of the organizational elements. In addition to the reorganization of the cyber security functions discussed above, the group will help me determine how best to consolidate duplicative staff functions, centralize the reporting responsibilities of our data centers and our IT system development activities, and consolidate the Central Office IT networks and computing facilities.

Concerning VETSNET, as I committed to you at the last hearing, I have been personally overseeing the progress of this effort along with the Under Secretary for Benefits. On June 17, 2002, the Secretary received a comprehensive review of our plans to correct the Department's outstanding IT deficiencies as reported by the General Accounting Office. This review included a detailed discussion on VETSNET. Required actions to be completed by the end of September include:

- Selecting a full time VETSNET project manager to have the responsibility and accountability for cost, schedule and performance for the completion of this effort;
- Contracting for an independent test activity to ensure that the system will meet all of its performance requirements;
- Validating that all of the performance requirements are correct (except for reports that are due by the end of the calendar year); and,
- Conducting a review of the readiness of the program to meet the April 2004 date that was promised at the last hearing.

I am pleased to report that these actions are complete and, in conjunction with the Under Secretary for Benefits, we have recommended to the Secretary that we continue the VETSNET effort in FY2003.

With respect to the Government Computer Based Patient Records (GCPR) program, we have re-baselined and re-scoped the program to address issues identified in a 2001 GAO report. We have renamed GCPR to be the Federal Health Information Exchange (FHIE) program. The re-baselined FHIE program uses an existing VA application called the Computerized Patient Record System (CPRS) as a fundamental building block. CPRS enables a clinician to access clinical data from any VA health facility. FHIE is a database that receives DoD clinical data (an exception being physician notes which are not electronically available from DoD at this time). CPRS is the application that enables VA to import clinical data from the FHIE database in addition to clinical data available within VA.

On April 26, 2002, I chaired a review of the FHIE test results to determine whether or not the first phase of FHIE is ready for deployment. Based on the results of this review, I determined that FHIE was ready to deploy on May 27, 2002. Deployment of this first phase of FHIE was completed in July 17, 2002. Future investment in FHIE will enhance functionality based on clinician feedback once operational.

On May 3, 2002, the Deputy Secretary, Department of Veterans Affairs, and the Under Secretary (Personnel and Readiness), Department of Defense signed a Memorandum of Agreement (MOA) for the Federal Health Information Exchange Governance and Management. This MOA:

- Replaces original GCPR documents signed in 1998;
- Renames GCPR to Federal Health Information Exchange (FHIE);
- Designates VA as the lead agency for FHIE (formerly GCPR);
- Revises goals and objectives to be aligned with the current strategy and direction of the project; and,
- Commits executive level support necessary to adequately manage the project.

I believe that the issues addressed in the April 2001 GAO report on GCPR have been addressed by the above actions.

I hope I have provided some insight as to the progress that has been made since the March 13, 2002, hearing. I believe these efforts demonstrate our very strong commitment, at all levels, to building an effective information technology program for the long-term. With your assistance, we will be able to continue on this path forward to ensure our continued ability to service the health and benefit requirements of our veteran population and their dependents.

Thank you for this opportunity to discuss these very important IT issues. I will be happy to answer your questions.

CHAIRMAN BUYER TO DEPARTMENT OF VETERANS AFFAIRS

Questions for the Record
House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
September 26, 2002
Hearing on VA Information Technology (IT) Initiatives

1. Please provide the total expenditures, including personnel costs, related to the VETSNET project for the last seven years. Please list these figures by fiscal year.

(In Thousands)	96 Actual	97 Actual	98 Actual	99 Actual	00 Actual	01 Actual	02 Actual	Total To Date
Non-payroll	2,062	2,285	3,222	2,700	3,421	6,765	8,864	**29,319**
Payroll	781	1,277	1,012	1,009	1,066	1,479	2,161	**8,785**
Total Cost	**$2,843**	**$3,562**	**$4,234**	**$3,709**	**$4,487**	**$8,244**	**$11,025**	**$38,104**

2. GAO stated in its report that "VA's offices self-report computer security weaknesses, and it lacks an independent component to ensure the accuracy of reporting and validation of corrective actions taken." How do you plan to address this issue?

Overall, the Department has made significant progress in implementing the reporting provisions of the Government Information Security Reform Act of 2000 (GISRA), through developing appropriate methodologies to identify, prioritize and remediate IT security control weaknesses. However, analysis of information contained in the Department's GISRA database indicates that some self-reported progress may be overly optimistic, or may not accurately reflect the current security status of some IT systems. Therefore, the VA Office of Cyber Security has established a review and inspection division to validate the accuracy of self-reported information in the GISRA database, and to conduct external and internal penetration testing to ensure that previously identified vulnerabilities have been adequately remediated. These processes will ensure the integrity of GISRA-related information as the Department moves rapidly forward in efforts to improve its overall IT security posture.

3. Please articulate VA's specific goals relating to the implementation of the One-VA Enterprise Architecture in FY 2003. Secondly, please provide the Committee an outline of VA's timetable for full-scale implementation of the One-VA IT Architecture.

The One-VA Enterprise Architecture v1.0 published in September 2002 lays out a logical model for the overall target One-VA Enterprise Architecture in section 5.1 and a corresponding sequencing plan in section 6.1. Enterprise Architecture by its fundamental nature is a continuous improvement process and as such is never done. Nonetheless, these sections of the One-VA Enterprise Architecture

v1.0 address the issue of specific goals and timetables for implementation of the One-VA Enterprise Architecture as developed thus far. The logical model presented in section 5.1 identifies several key elements of infrastructure as follows:

- Telecommunications Infrastructure
  - *Telecommunications Modernization Project (TMP),*
- Cyber Security Infrastructure
  - *Enterprise Cyber Security Modernization Project (ECSIP),*
  - *Authentication and Authorization Infrastructure (AAI) Project,*
- Corporate and Regional Data Processing with Continuity Of Operations (COOP)
  - *Corporate Data Center Integration (CDCI) Project.*

Each of these infrastructure elements has one or more key projects associated with it to implement the corresponding element of the One-VA Enterprise Architecture. These projects, discussed in the One-VA Enterprise Architecture sections 5.2 to 5.4, are also identified in the sequencing plan in section 6.1.

Section 5.1 also identifies the top-level model for the distributed applications and data environment that will be supported by these infrastructure elements. Within that distributed applications and data environment, there are several key projects addressed within the One-VA Enterprise Architecture as follows:

- *One-VA Registration and Eligibility Project,*
- *One-VA Contact Management Project,*
- *VistA HealtheVet Health Data Repository (HDR) Project,*
- *Core Financial and Logistic System (CoreFLS) Project.*

The following discussion addresses each of these key infrastructure and applications/data layer projects by providing a brief description, key goals, and projected timelines for FY 2003 to FY 2005. (No attempt is made here to project beyond FY 2005.) The discussion of these projects is followed by a summary of the future evolution of the One-VA Enterprise Architecture through the continuous improvement process adopted by VA.

Project: *Telecommunications Modernization Project (TMP)*
Description: The Telecommunications Modernization Project is intended to evolve from VA's current state of over 30 loosely federated independent networks to a single, high performance wide area data network capable of supporting enterprise wide applications and support Service Level Agreements (SLAs) for performance and reliability at every service delivery node on the network. It was initiated in FY 2002 as a re-baseline of multiple pre-existing network efforts across the Department.
Goals / Timelines:

FY 2003: Optimize the core of the One-VA Wide Area Network (WAN) to support regional service delivery to all VA facilities, and to support Service Level Agreements for every service delivery point. Establish an around the clock Network Coordination Center (NCC) to continuously monitor the health of the network and take proactive action to resolve service delivery problems.
FY 2004: Extend service delivery from the optimized core to all VA facilities to complete the project.
FY 2005: Operations and sustainment.

Project: *Enterprise Cyber Security Infrastructure Project (ECSIP)*
Description: ECSIP will implement network protection devices and services such as firewalls, network intrusion monitors, and Virtual Private Networks (VPNs) to secure the boundary of the VA enterprise. ECSIP will implement a framework for Public Key Infrastructure (PKI), and implement a 24x7x365 Central Incident Response Center and Security Operations Centers to manage and control all network protection devices. It will also perform periodic penetration testing of VA networks, facilities, and applications to identify and resolve security weaknesses before they can be exploited by outside parties. ECSIP was initiated in FY 2002 as a re-baseline of multiple pre-existing cyber security efforts across the Department.
Goals / Timelines:

FY 2003: Implementation of a Central Incident Response Center with 24x7x365 operations. Complete prototype implementation and evaluation, followed by initial production deployment of hardened network gateways at three VA corporate data centers. Initiate migration of external network and Internet connections to one of these corporate gateways and shut down other interconnections. Establish two Security Operations Centers to monitor network protection devices and perform periodic penetration testing. Certify and accredit anti-virus servers that provide on-line virus protection VA-wide.
FY 2004: Complete production deployment of hardened network gateways at the remaining corporate and regional data processing centers as required to fully protect the boundary of the VA enterprise. Complete migration of external network connections and Internet connections to one of the corporate or regional data processing center gateways, and shut down other external network and Internet connections. Continue operations and sustainment
FY 2005: Operations and sustainment (prevent, detect and react).

Project: *Authentication and Authorization Infrastructure (AAI) Project*
Description: AAI will establish and maintain a standards-based authentication and authorization infrastructure that will enhance/replace simple User ID and Password logon access control security with stronger authentication through digital certificates and smart cards; and provide centralized management and control of network and application user access rights – the types of data and applications that a user may read, write, and/or update. AAI is a proposed FY 2004 new initiative.
Goals / Timelines:

FY 2003: Implement a pilot of the authentication and authorization infrastructure (AAI) at the Austin Automation Center corporate data center.
FY 2004: Update the proposed AAI with "Lessons Learned" from the pilot implementation, and initiate the production AAI implementation.
FY 2005: Continue the AAI implementation (target FY 2006 completion).

Project: *Corporate Data Center Integration (CDCI) Project*
Description:
The CDCI project will implement an improved continuity of operations (COOP) for VA corporate applications that currently operate at the Austin Automation Center (AAC), the Hines Information Technology Center (ITC), and the Philadelphia ITC. The project will significantly improve recovery time from a systems outage and reduce potential loss of data for mission critical and essential systems by providing electronic data vaulting and applications restart capability across the three locations. The current 72 hours will be shortened to 12 hours or less. The project supports the goal of ensuring VA information assets are adequately protected against loss. It also satisfies Presidential Decision Directive (PDD) 67 requirement for essential processes to be available within 12 hours or less of an emergency event. The CDCI project is being done under the auspices of a Franchise Fund activity, the AAC, and is not an appropriated funding initiative.
Goals / Timelines:

FY 2003: Complete Operational Engineering Model (OEM) acceptance testing of technology needed to support protection of data and recovery of operations within the PDD 67 timeframe. Establish configuration and event management policy and procedures for use at the three centers.
FY 2004: Complete production implementation of OEM for all mission critical and essential systems.
FY 2005: Operations and sustainment.

Project: *One-VA Registration and Eligibility Project*
Description: The One-VA Registration & Eligibility process consolidates the eight distinct, line-of-business-centered processes currently in use within VA to register veterans and make eligibility and entitlement determinations into a veteran-centered integrated process. A key element of this approach is integration with the DoD's Defense Manpower and Data Center and the DEERS system to ensure efficient bi-directional flow of information on veterans between VA and the DoD. This integration will provide, for the first time, a single unified view of active, retired, reserve and separated members to both VA and the DoD. One-VA Registration and Eligibility is a proposed FY 2004 new initiative.
Goals / Timelines:

- **FY 2003:** Prototype implementation and evaluation (limited scope and scale within Education, Medical Care and Memorial Affairs business lines).
- **FY 2004:** Integration and deployment into VA central R&E processing centers for initial business lines.
- **FY 2005:** Integration and deployment into VA central R&E processing centers for second increment of business lines.

Project: *One-VA Contact Management Project*
Description: In order to accomplish the goals of One-VA both in veteran perception and in increased internal workflow efficiency, the development of One-VA National Contact Management is both strategic and critical. A comprehensive contact management solution will incorporate the primary functionality of an inbound and outbound call center and provide expanded service to include website support, email response, US mail inquiry response, targeted and bulk mailing. One-VA Contact Management will execute in parallel with One-VA Registration and Eligibility. One-VA Contact Management is a proposed FY 2004 new initiative.
Goals / Timelines:

- **FY 2003:** Prototype implementation and evaluation (limited scope and scale within Education, Medical Care and Memorial Affairs business lines).
- **FY 2004:** Integration and deployment into VA central R&E processing centers for initial business lines.
- **FY 2005:** Integration and deployment into VA central R&E processing centers for second increment of business lines.

Project: *VistA HealtheVet Health Data Repository (HDR) Project*
Description: HDR will hold individual patient medical records that delineate all aspects of a patients care across the continuum within VHA. The data will be comprised of demographics, patient centered data (e.g., medications, test results); encounters (e.g., purpose of visit, education, procedures, diagnosis) discharge summaries, etc. A perpetual store representing the veteran's medical history will be managed via HDR. HDR is an ongoing project.
Goals / Timelines:

FY 2003: Technical strategies for the development of HDR will be defined and published. A HDR prototype will be designed and deployed. Based on prototype evaluation, the HDR design, including the completion of the lexicon/data mapping, will be completed.

FY 2004: Development and integration of the HDR will be completed. Initial population of the HDR with VAMC data will be initiated and continue throughout FY 2004.

FY 2005: The HDR Database population will be completed. The Data Mart/Data Warehouse implementations for HDR will also be completed. The repository will enter production operations by the end of CY 2005.

Project: *Core Financial and Logistics System (CoreFLS) Project*
Description: The new Core Financial and Logistics System (CoreFLS) is being implemented by VA to resolve repeat reportable conditions, e.g., lack of an integrated financial system. CoreFLS includes: Accounting and Budget, Contracting and Purchasing, Asset Management, and Inventory. CoreFLS will provide financial information in a timely and useful fashion to: (1) support management's fiduciary role; (2) support the legal, regulatory and other special management requirements of VA; (3) support budget formulation and execution functions; (4) support fiscal management of program delivery and program decision making, (5) comply with internal and external reporting requirements, including, as necessary, the requirements for financial statements prepared in accordance with the form and content prescribed by the Office of Management and Budget (OMB) and reporting requirements prescribed by the Joint Financial Management Improvement Program (JFMIP), Treasury; and others as established by law; and (6) monitor the financial management system to ensure the integrity of financial data. CoreFLS is an ongoing project based on commercial software.
Goals / Timelines:

FY 2003: Continue to execute Systems Development and Integration Phase. This will require the continuation of system configuration and refinement of training and change management plans to help prepare end-users for the change and maximize successful implementation of CoreFLS.

FY 2004: Complete Systems Development and Integration and commence System Deployment and Implementation of CoreFLS which will involve migrating existing numerous disparate VA financial and logistics systems to a fully integrated financial and logistics system that supports contemporary best business, financial, and logistics management practices.

FY 2005: Continue System Deployment and Implementation of CoreFLS (targeting a mid FY 2006 completion).

While there are many IT Projects in the VA IT Portfolio, these eight projects play foundational roles in the One-VA Enterprise Architecture v1.0 as defined to date. The four Infrastructure projects will provide fundamental services to virtually every other IT project within the portfolio. Three of the remaining four applications and data layer projects (One-VA Registration and Eligibility, One-VA Contact Management and CoreFLS) will provide functional consolidation of processes and functions implemented today repeatedly and duplicitatively across the Department, and will provide the basis for an integrated data environment across the Enterprise as called for in Section 5.1 of the One-VA Enterprise Architecture v1.0. The final applications and data layer project, Health Data Repository, will accomplish this same task of establishing an integrated data environment for clinical histories within the medical care arena. As such, many of the other development initiatives will make use of the integrated data and the services provided by these foundational projects.

The One-VA Enterprise Architecture itself is continuing to evolve since VA is implementing Enterprise Architecture as a continuous improvement process, with version 1.0 approved by the Secretary in September 2002 serving as the initial baseline. A second update is underway to be published in FY 2003 as version 2.0, which will accomplish several objectives. Version 2.0 will clean up remaining review comments from version 1.0. Additionally, version 2.0 will expand the scope in both breadth and depth over the initial baseline (i.e., greater depth for foundational areas identified in version 1.0 and discussed above, as well as expansion to other functional areas of foundational importance and to be prioritized in the Department's FY 2005 budget submission). Finally, version 2.0 will continue the theme established in version 1.0 of coupling Enterprise Architecture to key Departmental processes; namely planning and budgeting, project execution and Project Management Oversight.

CHAIRMAN BUYER TO U.S. GENERAL ACCOUNTING OFFICE

Inited States General Accounting Office
Vashington, DC 20548

November 5, 2002

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

Subject: *Veterans Affairs: Subcommittee Post-Hearing Questions Concerning the Department's Information Technology Management*

This letter responds to your October 10, 2002, request that we provide answers to questions relating to our testimony of September 26, 2002.[1] At that hearing, we discussed the Department of Veterans Affairs' (VA) progress in improving its overall management of information technology, including the centralization of information technology functions, programs, and funding under the department-level chief information officer (CIO). We alsc discussed the department's progress since last March in developing an enterprise architecture, improving information security, and managing important information systems initiatives being pursued by the Veterans Benefits Administration (VBA) and the Veterans Health Administration (VHA). Your questions, along with our responses, follow.

1. *On page 19, the GAO testimony stated that VA must also still develop a program management plan to delineate how it will develop, use, and maintain the enterprise architecture. GAO stated that such a plan is integral to providing definitive guidance f effective management of the enterprise architecture program. According to Dr. Gauss, VA has developed and will implement version 1.0 of the One-VA Enterprise Architectur which establishes ten enterprise business functions and seven key enabling functions. Does GAO agree that these business and enabling functions provide the management tools necessary to start the process for implementing VA's enterprise architecture?*

The Federal CIO Council's guidance on enterprise architecture[2] advises organizations to develop a set of controls to help them successfully manage the process of creating, changin and using an enterprise architecture. These controls are intended to promote sound management of the enterprise architecture project through the use of plans, products, and requirements, including the program management plan that we referred to in our testimony. In particular, a program management plan would articulate critical factors guiding work on the architecture, including a work breakdown structure detailing the tasks and subtasks

[1]U.S. General Accounting Office, *VA Information Technology: Management Making Important Progress in Addressing Key Challenges*, GAO-02-1054T (Washington, D.C.: Sept. 26, 2002).

[2]Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (Washington, D.C.: February 2001).

necessary to acquire, develop, and maintain the architecture; resource estimates for funding, staffing, training, workspace requirements, and equipment needs; and a roadmap for the initiation and completion of key project tasks. As our testimony noted, VA lacked such a management plan to support its enterprise architecture effort.

While the enterprise business functions and key enabling functions are essential components of the architecture that VA is developing, they cannot be considered a primary tool for managing the enterprise architecture effort. Rather, these business and enabling functions are the products of VA's efforts to develop the baseline, or "as-is," and identify the target, or "to-be," components of its enterprise architecture. Specifically, enterprise business functions are externally focused functions involving direct interactions with veterans across the enterprise, such as providing medical care benefits, vocational rehabilitation, and employment benefits. Key enabling functions are those necessary to support the enterprise business functions, such as eligibility and registration, and enable smooth operation of the overall enterprise both internally and externally.

As the CIO Council's guidance notes, one of the initial steps in developing an enterprise architecture is describing the enterprise as it currently exists, including business functions and information flows. By identifying the business and enabling functions, VA has set the stage for moving toward and measuring progress against its target architecture. Nonetheless, while these functions represent an important accomplishment in VA's development of its enterprise architecture, they do not satisfy the department's need for a program management plan to help provide a sound foundation for managing the development, implementation, and use of the architecture.

2. *Concerning VETSNET, GAO testified that "after six years the VA still has significant work to accomplish, and could be several years from fully implementing the system." In GAO's opinion, how have veterans benefited from this program, considering the significant capital that has been dedicated to this program?*

Although VBA has spent more than $40 million on developing the VETSNET compensation and pension replacement system since 1996, veterans have not yet received measurable benefits from this initiative. At the time of our testimony, VBA was using its new software products to deliver benefits payments to only 9 of the more than 3 million compensation and pension benefits recipients on its rolls.[3] Benefits payments to all other recipients continued to be made via the department's aging Benefits Delivery Network. Moreover, subsequent to our testimony, VBA officials told us that at the beginning of this month they intended to convert the processing of the nine benefits payments being made with the new software to the Benefits Delivery Network. An official explained that the February 2001 pilot test using the new VETSNET software had in essence been a proof of concept exercise to demonstrate

[3]As part of a pilot test in February 2001, VBA began processing ten original benefits claims using its new software. However, according to VBA, one of the ten veterans subsequently moved outside of the area covered by the pilot test and now receives his payments via the Benefits Delivery Network.

that the software could deliver benefits payments. He stated that this exercise has now been completed.

VBA still has numerous tasks to accomplish before its software applications comprising the compensation and pension replacement system can be fully implemented and capitalized upon. As our testimony noted, all but one of the six software applications constituting the new system[4] still need to be fully deployed or developed. Specifically, two applications—Share, which is used to establish a claim, and Modern Award Processing-Development, which is used to help develop a claim—still need to be implemented in the majority of VBA's 57 regional offices.[5] In addition, three applications continue to require development and, according to VBA officials, are not expected to be fully deployed until December 2004. At that time, Award Processing will be expected to record award decisions; generate, authorize, and validate on-line awards; and interface with a correspondence application to develop notification letters to veterans. The Finance and Accounting System will be expected to perform accounting and benefits payments functions and interface with the Department of the Treasury.

Beyond these applications that VBA must still deploy and/or develop, it faces the more immediate task of ensuring that the one application already deployed—Rating Board Automation 2000—is utilized to its full potential. When implemented in November 2000, this application was expected to assist veterans service representatives in rating benefits claims. However, according to a VBA official, some regional offices indicated that rather than improve service delivery, use of the software tool actually resulted in longer processing times. Given the department's backlog of compensation and pension benefits claims, the undersecretary for benefits subsequently suspended the requirement for regional offices to use the software until its backlog had been reduced. At the time of our testimony, VBA did not plan to require its regional offices to fully utilize this software until July 2003.

3. *Since VA has been given the lead in making the renamed Federal Health Information Exchange (FHIE) a reality, what must be done to assure successful implementation?*

Successful implementation of FHIE will largely depend on the extent to which consistent and effective project management and oversight exists to guide the initiative. In April 2001,[6] we recommended that the participating agencies—VA, the Department of Defense (DOD), and

[4]The six software applications constituting the replacement system are Share, Modern Award Processing-Development, Rating Board Automation 2000, Award Processing, Finance and Accounting System, and Correspondence.

[5]Among the 57 regional offices that are expected to benefit from the replacement system, only 6 currently use Share to establish a claim; only 2 offices (Salt Lake and Little Rock) have pilot-tested and currently use Modern Award Processing-Development to assist in developing most compensation claims.

[6]U.S. General Accounting Office, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Data Sharing*, GAO-01-459 (Washington, D.C.: Apr. 30, 2001).

the Indian Health Service—take various actions to strengthen the management and oversight of the government computer-based patient record (GCPR) project (the predecessor strategy). These steps included (1) designating a lead entity with final decision-making authority and (2) creating comprehensive and coordinated plans that included an agreed-upon mission and clear goals, objectives, and performance measures to ensure that the agencies could share comprehensive, meaningful, accurate, and secure patient health care data. We reiterated the need for VA to implement these recommendations in our June 2002 report,[7] and also made additional recommendations that the participating agencies (1) revisit the original goals and objectives of the GCPR initiative to determine if they remained valid and, where necessary, revise the goals and objectives to be aligned with the current strategy and direction of the project; and (2) commit the executive support necessary for adequately managing the project and ensure that sound project management principles are followed in carrying out the initiative. VA concurred with these recommendations.

The actions that VA and DOD took in response to the recommendations resulted in a revised strategy whereby patient data would be exchanged and a common health information infrastructure and architecture comprised of standardized data, communications, security, and high-performance health information systems would be developed. VA and DOD intend to accomplish this with two initiatives. The first, FHIE, is focused on DOD providing information to VA clinicians. A second initiative, referred to as HealthePeople (Federal), is intended to allow the two-way exchange of clinical information, with an emphasis on establishing a common health information infrastructure and architecture. VA and DOD have stated that they plan to complete this initiative by the end of 2005.

Along with designating VA as the lead agency for FHIE, VA and DOD took actions to improve project management that should continue to help guide this initiative to a successful outcome. For example,

- goals and objectives have been revised and aligned with the new FHIE strategy;
- a permanent project manager has been assigned to the initiative, and he is using project management software to facilitate the monitoring of assigned tasks;
- executive-level reviews are being conducted for systems development and deployment approval;
- weekly testing and technical meetings are being held; and
- monthly interagency in-process reviews are being conducted by VA's Deputy CIO for Health and DOD's CIO for Military Health Systems.

VA and DOD officials reported that the nationwide deployment and implementation of the first phase of FHIE was successfully completed in July. The first phase has enabled the one-way transfer of demographic information,[8] laboratory results, outpatient pharmacy data, and

[7]U.S. General Accounting Office, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO-02-703 (Washington, D.C.: June 12, 2002).

[8]The demographic information consists of patient name, DOD eligibility category, Social Security number, address, date of birth, religion, primary language, sex, race, and marital status.

radiology reports for separated service members from DOD's Military Health System Composite Health Care System to VA's FHIE repository. Clinicians throughout VHA now have access to over 14 million lab messages, almost 14 million pharmacy messages, and over 2 million radiology messages on over 1 million service personnel who separated between 1987 and 2001.

A second, final phase of FHIE began in October and is intended to make additional health information—in-patient histories, diagnoses, and procedures; allergy information; admission, disposition, and transfer information; and consult results—available to VA clinicians. This phase will rely on the existing technology supporting phase 1, and thus will only involve adding data to the existing repository. Completion of the final phase is scheduled for September 2003.

As VA and DOD proceed with implementing the final phase of FHIE and move forward with Health*e*People (Federal), providing consistent project management and oversight will continue to be essential for successful project completion. As such, sustained adherence to the program management structure that VA and DOD have already put in place will be critical. Moreover, these agencies can further strengthen their management and oversight through the use of performance measures to gauge the progress and effectiveness of their efforts.

4. *The VA testified that Healthe*Vet-Vista *should be implemented by the end of 2005. In GAO's opinion, is this timetable realistic? Please elaborate.*

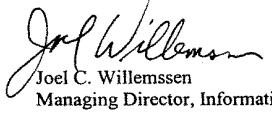
As noted, beyond FHIE, VA and DOD have envisioned a long-term strategy—Health*e*People (Federal)—involving the two-way exchange of patient health care information. This exchange is expected to depend on the successful interoperability, and resultant sharing of secure health care data, between DOD's Composite Health Care System (CHCS) II and VA's Health*e*Vet VISTA, both of which continue under development.

At this time, we are unable to determine whether plans for implementing this long-term strategy are realistic. When our review concluded, VA and DOD had just begun this initiative, and program officials stated that they had not completed an implementation plan. Until DOD's CHCS II and VA's Health*e*Vet VISTA have been fully developed and a plan detailing the work tasks, resources, and completion milestones for Health*e*People (Federal) has been developed and made available for our review, we will not have a basis for assessing VA's potential for implementing this initiative by the end of 2005.

We requested comments on a draft of this letter from the Department of Veterans Affairs, but none were provided.

We are sending copies of this letter to the Secretary of Veterans Affairs and other interested parties. Should you or your office have any questions on matters discussed in the letter, please contact me at (202) 512-6253. I can also be reached by e-mail at willemssenj@gao.gov.

Sincerely yours,



Joel C. Willemssen
Managing Director, Information Technology Issues

○