VA'S INFORMATION TECHNOLOGY INITIATIVES

HEARING

BEFORE THE

SUBCOMMITTEE OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MARCH 13, 2002

Printed for the use of the Committee on Veterans' Affairs

Serial No. 107–23

U.S. GOVERNMENT PRINTING OFFICE
85–342PDF WASHINGTON : 2003

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
STEPHEN E. 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

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
RONNIE SHOWS, Mississippi
SHELLEY BERKLEY, Nevada
BARON P. HILL, Indiana
TOM UDALL, New Mexico

Patrick E. Ryan, *Chief Counsel and Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

STEPHEN E. BUYER, Indiana, *Chairman*

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

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

CONTENTS

March 13, 2002

VA'S INFORMATION TECHNOLOGY INITIATIVES

WEDNESDAY, MARCH 13, 2002

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

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

Present: Representatives Buyer, Boozman, and Carson.

OPENING STATEMENT OF CHAIRMAN BUYER

Mr. BUYER. Today the Subcommittee on Oversight and Investigations of the Veterans' Affairs Committee will come to order.

We will be holding our fourth hearing to receive an update on the Department of Veterans Affairs information technology programs and the progress made in fulfilling the requirements of the Clinger-Cohen act of 1996 to develop an enterprise architecture plan.

Since our previous IT hearing last April, Secretary Principi has taken several decisive steps to move towards a One-VA.

First, he chose a CIO for the Office of Information Technology. It's a formidable task. We thank the gentleman for accepting the challenge, and Secretary Principi assembled the VA Enterprise Architecture innovation team to rapidly develop a plan. The team issued a report in August of 2001, providing a strategy to ensure that VA operates under a fully integrated system called the One-VA system.

This 90-day report stated, quote, "The mission of VA's enterprise architecture is to develop and implement an evolutionary high-performance One-VA information technology architecture aligned with our program/business goals that enables enterprise-wide data integration. VA's enterprise architecture will enable us to provide an accessible source of consistent, reliable, accurate, useful, and secure information and knowledge to veterans and their families, our workforce and stakeholders, to support and effectively deliver services and benefits enabling effective decisionmaking and understanding our capabilities and accomplishments."

If that is not a sentence fragment, I have never seen it.

"The enterprise architecture will support VA's overall strategic goals."

That was their quote.

These are laudable goals. However, we would like to know how the VA's plan on making it accessible, reliable, and secure. In particular, we hope to hear how you plan to execute this plan. Specifically, what is your business plan and what are the definitive milestone dates to accomplish the plan?

President Bush has made IT one of his top priorities, and his budget reflects his strong commitment to overhauling or outright replacing our current technology on a government-wide basis. The VA will receive $1.35 billion IT for fiscal year 2003, a whopping 15 percent increase over last year's funding level, and that is what brings us to this point of the hearing.

We want to know if the VA is investing their IT money wisely. VA now has a CIO in place and finally has an architecture plan that we have been requesting for 5 years. However, a plan is only good if it can be executed. We need to know what obstacles you foresee and how you plan to work through the VA's organizational land mines, cultural bias, the turf battles, and the inherent inertia. Furthermore, how does it address storage protection of VA's information systems?

We would like to hear how the VA dealt with the vulnerabilities identified in our previous hearings. Congress has pumped almost a billion dollars per year into VA's IT programs for the past decade, and we want to know how VA can proceed in this One-VA concept.

Today, we hope to hear what the progress has been with the VA's integrated systems architecture plan, VBA's VETSNET claims processing program, cyber security, VHA's Decision Support Systems, and the Government Computer-Based Patient Records Program.

Having a plan of action is vitally important. Implementing the plan and making it a reality will require a tremendous amount of vigilance on the part of the Secretary, the CIO, and senior managers. We all recognize that the VA has its challenges, but they are not insurmountable. The VA is a complex multi-faceted organization, and those in charge of its IT operation will be required to stay focused and undeterred.

We believe the VA can meet these challenges. What we hope to learn today is what the time-lines are in terms of achieving the fully integrated One-VA system. Basically, we want to know, is this going to be a couple of years or is this going to be another 16 years?

Also, I thought I would note, the background memo you sent out, this memo you sent out to the committee—I found this ironic. You wrote, "Currently, the VA has separate systems with multiple data centers, technology, CIOs, and networks and vendor products, which often result in duplication, replication, and redundancy."

I yield to Mrs. Carson for any comments she would like to make.

OPENING STATEMENT OF HON. JULIA CARSON

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

I, too, would like to welcome our guests and witnesses for today's hearing.

Congressional oversight of Department of Veterans Affairs progress in implementing information technology integration and security architectures under One-VA is of great importance. No single management tool is as equipped to enhance the delivery and accessibility of VA services in a cost-effective manner.

Mr. Chairman, I used those same words in my letter to you last September when I requested a reasonable delay in the IT hearing then scheduled for October 2001. At that time, the VA's much anticipated Enterprise Architecture had not been released, and the Office of Cyber Security was not yet official.

Your postponement of this hearing until today allows us to now determine if the VA is off to a fresh start, uniting and linking critical functions among the Administrations, or if they are retreating from the many challenges of "One-VA."

They have now had sufficient time to select their direction and to take their first steps. This One-VA horse has been allowed to say in the barn far too long. We must now see if it can run.

First, let me congratulate VA leadership for publishing the Enterprise Architecture for Strategy, Governance, and Implementation. This document now provides guidance to all aspects of VA's IT initiative. This parent document allows us to evaluate its many IT offspring, VA-wide.

I think the Enterprise Architecture for VA may be one of the best documents of its type in government. It is an outstanding effort. It captures not only the essence of Clinger-Cohen, GPRA, and other Federal IT guidance; it captures the spirit of that guidance and presents it logically. It tells a story, it makes sense, even from a layman's perspective. Congratulations on a job well done.

For the IT architecture to serve as a tool to bring about One-VA, it must link directly to the mission of VA. In its own words on page 14, quote, "The VA Strategic Plan must drive VA's Enterprise Architecture and the Enterprise Architecture must define the supporting information systems required to achieve that plan," end quote. In other words, this is not a, "which-came-first-the-chicken-or-the-egg," scenario. Defining the mission comes first.

You cannot have an IT architecture to support the mission unless you have first defined that mission. You cannot provide IT support to a business plan without first knowing the business processes that require support. You cannot break out the mission-value of IT assets without tying their relative value to the organization's mission. These are bedrock concepts.

You also have to implement a plan once you write it. This is the difficult part of the process. If the desired outcome is defined as 2 percent inspiration and 98 percent perspiration, the writing of the plan gets you up to the 4 percent range, there is a long way to go.

To implement this plan, the CIO and the Secretary will have to overcome organizational inertia and change existing culture. These both have classically protected the parochial interests of the three Administrations—VBA, VHA, and NCA—over the interests and overall mission of VA.

As Dr. Kappelman, our witness on panel one so eloquently observes, "Historically, VA has optimized the parts and sub-optimized the whole."

I agree with him that shifting VA's focus to a focus on the whole will take patience, help, and guidance.

Writing a strategic business plan does not guarantee success. It merely outlines the envisioned method for achieving success; it defines goals. These goals and methods must be well articulated to serve as the foundation for the IT architecture.

It is the job of VA to define One-VA as it devolves through the Administrations to every field-level activity. It is the job of the CIO to craft architecture to meet that need. It is also the job of the CIO to guide the implementation of that plan all the way back to the field-level activities, and Mr. Chairman, implementing IT enterprise architecture to support One-VA, the Secretary must empower the CIO to have full control of the architecture implementation process.

The CIO must employ a method, for example, that can compare and contrast the relative worth of IT assets, both new and legacy systems, and promulgate that method in a non-parochial environment to create a One-VA IT balanced scorecard. The Enterprise Architecture sets the stage for this action. The principal actors must have the reach to bring about successful a outcome.

Thank you very much, Mr. Chairman, for allowing me to have my say.

Mr. BUYER. Thank you.

Mr. Boozman, do you have any comment?

Mr. BOOZMAN. No.

Mr. BUYER. Thank you.

We will have the first panel, recognize Leon Kappelman, Ph.D., Director of Information Systems Research Center at the University of North Texas.

We have your statement, and with no objection, it will be submitted into the record, and we will welcome your testimony.

STATEMENT OF LEON A. KAPPELMAN, DIRECTOR, INFORMATION SYSTEMS RESEARCH CENTER, UNIVERSITY OF NORTH TEXAS

Mr. KAPPELMAN. Thank you very much, Mr. Chairman. Thank you so much for inviting me to testify today.

Last year, I had the honor of facilitating over 20 of VA's senior IT and business leaders from all of the administration and department staff offices, in forming what came to be known as the Enterprise Architecture Innovation Team. For 15 days and five very long weekends, they created and unanimously endorsed that strategic enterprise architecture document that you just mentioned that Secretary Principi approved last September.

I also participated in analyzing VA's project management practices. I had the privilege in October and then again just a few weeks ago of facilitating two working conferences attended by more than 200 of VA's senior IT managers.

The short story is, in these past 10 months, I really have seen a profound and significant change, positive, in how VA manages IT, but these are just the first critical steps in what the members of the committee have already acknowledged is a very long road.

In the cover letter to the Secretary that accompanied the enterprise architecture document, John Zachman, who I would consider the godfather of enterprise architecture, wrote—and this is a quote—"This is not a project. It is a process. It is different from the industrial age past. It is the information age present. Here is some advice that may help you institutionalize VA's enterprise architecture: (a) Do not underestimate the difficulty and complexity. This will take time and determination. This is a new way of life, a revolution in thinking, a discipline. Change of this magnitude takes perseverance. Do not be discouraged. (b) Make executive education and technical training a continuous process. It is easy to forget long-term issues in the short-term stress of daily life, and (c) remember, there is still much to learn and discover and many opportunities to create advantage and value," end quote.

VA has set a high bar for itself. They worked hard to put that plan together, but VA is massive in size, enormously complicated, and highly decentralized. They have significant workforce development concerns and a long, long history of independent parts that, quite frankly, do not work very well together.

VA could use some things from Congress, too, and I humbly offer you the following suggestions:

First, hold them accountable, but understand and honor their long-term vision. Please do not make the mistake of demanding short-term IT accomplishment without long-term relevance, because this will only lead to re-work, scrap, replace, and enterprise disintegration, and we have all seen enough of that.

Secondly, provide policy guidance and assistance. They really are entering new ground here, as they strive to achieve One-VA. Historically, as the good lady just pointed out, they have optimized the parts and sub-optimized the whole. One-VA and Clinger-Cohen both say shift that balance to optimizing the whole through massive integration, but this is not just a technical change. This is an organizational change, and they need your patience, they need your help, and they really will need some guidance in how to do some of this.

Third, provide funding for these changes. Resources are needed, especially for the things they have never done before. I'm not talking about IT projects. They will stand or fall on their own merits. There is a real need, however, for additional funding for VA's IT central office, for the Office of the Chief Enterprise Architect, as well as for the establishment of a VA-wide project management office, but all of this will be for naught if there is not funding and acknowledgement of the significant effort in education, training, and organizational culture change required to realize One-VA.

These are not IT issues. These are VA issues, and they will require the active involvement of VA's business and IT personnel, the assistance of change management professionals, and the continued support and involvement of engaged and competent leadership.

Fourth, be realistic. If you want VA to perform at commercial best practice, then you have to realize that you are asking them to do it with about 70 percent of the funding average of commercial IT and about half the staff.

At the two working conferences, for the first time ever, more than 200 professionals responsible for the various pieces of the VA IT pie worked together face to face to create a shared vision for One-VA and IT's role in achieving it. It was about enterprise architecture and cyber security, project management, network infrastructure, workforce development, performance measurement, and fulfilling VA's role in homeland security.

It was not about business as usual but, rather, a significant change in mind-set from one of disintegration and fear to one of collaboration, trust, and accountability, but the vision and hard work of 200 managers, no matter how senior, does not suddenly transform an enterprise with over 4,000 IT professionals, several hundred thousand personnel, millions of customers, and a budget greater than the GDP of 75 percent of the countries in the world.

This is not a project. There is no silver bullet. This is a new way of life for VA, and such change can only happen incrementally, and we are all part of it.

Thank you very much.

[The prepared statement of Mr. Kappelman, with attachment, appears on p. 31.]

Mr. BUYER. Mr. Boozman, there is a vote on approving the journal. I am going to go ahead and stay. I'm not going to—I know it is an important vote, extremely important. I am sure you stayed up all night and read it.

One thing I couldn't help—as I was reading your background, I noticed some of the other enterprises that you had—that your work had included, and these are some very large companies. I mean I see Ameritech, J.C. Penney, Kraft, Coca-Cola, GTE, Texaco, Treasury Department of Canada, the United Nations, Wells Fargo, World Bank, CIA, Cigna, Computer Associates. I mean the list goes on and on.

What I want to ask is—obviously, they are all similar but yet different. And with the VA, with these three stovepipe operations and the cultural biases, the differences. Sometimes they do not even communicate, talk to each other, do not even know how to, nor care. Have you seen some similarities out there in other companies that have been there a long time, like a Coca-Cola, they have the bottlers over here and distributions over there? Help me out in some of the similarities yet differences.

Mr. KAPPELMAN. The issues are similar, as you point out. In many ways, VA is like a university. You know, universities have a tenured workforce. The VA has that. So, that creates its own particular set of issues, but in general, the situation is very similar.

Mr. BUYER. So, you would agree with me, a challenge but not insurmountable.

Mr. KAPPELMAN. Oh, not insurmountable at all, but needs to be, you know, taken on with a good plan, good measures to—you know, how are we going to know we are really making progress so we do not end up with 16 years and we are not sure where we got, where we know on a regular basis what kind of progress is being made.

Mr. BUYER. I will take to heart—your third recommendation—you talked about funding. I hold you to no numbers here today, but give me sort of an idea. When we look at this and go we want to make a 15 percent increase in this kind of a budget—I know your counsel to us is be patient, be responsive. You know, we just do not have open checkbooks here on behalf of the American taxpayer, but you are correct, we want to make sure that we transform the system. What am I looking at?

Mr. KAPPELMAN. I have not looked at their budget numbers, so I really cannot make any——

Mr. BUYER. Give me an idea of this—I will not hold you to this, but I will hold you to this testimony. These are a lot of companies that you reshaped their architecture, their IT systems. So, given the monies that they were spending, what it took to transform before they could get into things that made them productive and the cost savings, how much of a boost, on average, have these systems required?

Mr. KAPPELMAN. Okay. For none of those organizations did I do organization-wide enterprise architecture. They were more specifically focused issues that I was helping them deal with.

Mr. BUYER. Did any of them do it system-wide?

Mr. KAPPELMAN. However, in—commercial IT—we have different rules of thumb that we can apply, and each rule of thumb, you know, is based on averages. So, you have to be cautious in applying averages to any specific situation. You have to understand the issues of that particular enterprise, but in general, we tend to replace about one-third of IT a year.

So, you know, if we had a good estimate of what VA's total asset base of technology was and what it had cost to put it there, then we could estimate that they are going to spend about a third of that a year maintaining it and keeping it going forward.

Mr. BUYER. When you say they replace one-third a year, is that during the implementation of the plan?

Mr. KAPPELMAN. Of significant change, but what we find is that number tends to hold up pretty well over the long run, too.

So, for example, Delta Airlines recently went through a similar process. They looked at it and they said, okay, well, we have about $3 billion worth of technology that we manage, and the person they had asked to do that went to the board and said, look, if you really want this to happen, it is going to take a billion dollars a year to make it work, and with the commitment of the board, which you people really represent in this case, then it could be done.

I do not know what that number is for VA, but there are intelligent ways to come up with those estimates.

Mr. BUYER. If a major part of the budget is for the maintenance and support of existing systems, what have you seen? I am looking at all the different players of a team to actually make transformation a reality. Whether it is education of the executives or the workforce, but you know, you have got a support staff out there—i.e., contractors, contracts in place, and some may agree with what is going on and some do not and it is all about the dollar and they have in fighting and companies do not like each other. Give me some idea of what we are walking into with some existing companies out there.

Mr. KAPPELMAN. It is probably no different—I have no idea, but it is probably no different than what we're walking into in—look, VA has close to 200 entities that basically are separately budgeted. You know, they are independently—they have separate control, it is local control of those funds, and there is all kinds of little pieces of, you know, local controlled—little clumps of technology. Any kind of organizational change of this kind of magnitude that is trying to even just centralize standardization, put controls on decision-making—you are messing with people's security and power, and you have to be sensitive to that.

You just have to be sensitive to, you know, what I am sure a lot of you already know, just the good issues of organizational change management, the psychology of that. I am sure it is not that much different with the vendor community.

When we first started the enterprise architecture thing, all these vendors started approaching us about—you know, they wanted to make presentations as if what we were doing was figuring out some technical thing, and it was not about technology, you know. It had a lot to do with it, but it was not technical decisions we were making, we were making strategic decisions, but they felt very threatened and they wanted to, you know, have their voices heard.

I am sure it is not going to be much different now, but, you know, if the plans change, then I am sure that the vendors can be worked with, just like if the plans change, I am sure the internal personnel can be worked with, but it needs to be done intelligently, thoughtfully, and you know, people's needs have to be met.

Mr. BUYER. Let me switch gears, the last question before I yield. If you are working with a company in the private sector, you can hook in their commitment to the plan because they are going to be there for a little while. So, my question is about the continuity that you can have and the commitment toward a plan when you are in government and people are moving in and out of the system.

So, if you worked with some of the other government systems, in particular the Canadian Treasury and others, I mean I look at this one and say we have been fiddling and doing maintenance with these kinds of systems for over 16 years here in the United States, and we're spending a lot of money, and I do not want the ebb and flow of different administrations changing what we are trying to do. Can you give me some counsel?

Mr. KAPPELMAN. Big issue.

Mr. BUYER. Continuity is what I am focused on.

Mr. KAPPELMAN. It is not unlike when democracy comes to a country that has never had it before. You know, we can change some structures at first, and that is kind of the stage VA is at now, but there is—but that is just the institutions, the structural things. There is also a lot of education of the people that has to happen, and there are a lot of things that do not happen until they experience it and they realize the benefits of this new way.

So, that is kind of what is happening at VA. There is a lot of need for education. Yes, the structural stuff is happening, but there is a big need for education. There is a big need for learning this new language of enterprise architecture and learning how to communicate learning this new language, and some of it is about inventing some of the language. We do not have good tools, good graphical ways of representing some of these things, that they need to have the dialogue between IT people and business people.

One of the things we did at this last conference was people made presentations, and in their presentations, they would have a graphic of some aspect of VA or some aspects of its technology, and one of the things we did was we tried to see how those things fit into this framework that they have chosen to help them organize this language. This framework is really like a grammar, and so, now they are starting to invent the words in the vocabulary. So, what we know is people are already doing some of this, but they do not realize how it fits into this grammar.

So what we did is we looked at some of these graphics, and we said, well, we think this one goes here, and this one is, you know, useful for architecture, and this one is more useful for implementation.

So learning that language and experiencing it—one of the other things we realized at this last conference was the IT people might make a first draft of what they think the business process is or something, but then they have to go to the business person and verify it.

Mr. BUYER. All right. Wait a second. You have jumped into the weeds.

Mr. KAPPELMAN. All right.

Mr. BUYER. I do not want to get lost in your high weeds. My question is more—it is a much larger level here. We here in Congress, and particularly this committee, on a bipartisan basis, has no interest in the micro-management of the systems, but we do have our oversight responsibilities on government efficiencies. We want to make sure that certain acts passed by Congress are implemented and we are being watchful.

So when you testify to us that you want to make sure that we implement this plan and we properly fund it and education is in place, continuity, to make sure that, even though you have ebbs and flows of leadership that come in and out, I am trying to figure out and be helpful here to the VA on what modeling or what do they need to do to make sure that it does not matter who moves in and out of that system, that when they come into it, that part of that executive educative function that you are talking about, that they move into these things, that you just do not come in from the outside and you bring with you that experience they had at Westinghouse or, you know, at GTE or—it does not matter. They come in. They are educated. I just did not know what kind of thoughts you had on it.

Mr. KAPPELMAN. How do you institutionalize a change of this magnitude? It needs to become how business is done. It needs to become the language. Part of it is that institutional piece, that they, you know, create some structures and new decisionmaking bodies, but part of it is what they learn to experience. Partially it's training and they learn new things, but it is also the fact that people work together and actually start using these tools to make decisions, and they find out that they are getting better. In other words, they find out that doing it this way led to a better result.

You know, people go back to the old ways if they do not see the new ways as beneficial. So, this will happen through experience and training and helping them deal with all of these changes.

Mr. BUYER. All right. Ten seconds or less——

Mr. KAPPELMAN. All right.

Mr. BUYER. What is the time-line to actually get something like this implemented, do you think? One year, 2 years, 3 years, 4 years, 5 years, 6 years? When commitment is made.

Mr. KAPPELMAN. At some level, this never ends. However—because this becomes a new way of life.

Mr. BUYER. I understand.

Mr. KAPPELMAN. All right. Three to 5 years, they can accomplish an enormous amount.

Mr. BUYER. All right. Thank you.

I would now yield to Mrs. Carson for any questions she may have.

I ask unanimous consent that Ms. Carson's counsel may ask questions of the witness. Hearing no objection, I now yield.

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

Dr. Kappelman, I am going to follow up on a line of questioning that the chairman broached concerning change management and the role of change in the organization. The enterprise architecture is a major change for any organization that it comes through. This marriage of strategy and business plan, to the supporting IT architecture is a large pill for some folks to swallow.

So let me start off with a hypothetical dealing with organizational culture and organizational behavior. In a hypothetical organization, your task is to design an HR management system, an organizational chart, so to speak, for the organization. This organization has very powerful component parts in the sub-strata, which have a history of tremendous independence. You go out and you hire a CIO, a well-qualified CIO, to manage this plan.

Can you give me an idea of what he is going to find in the typical organization trying to push a major change through like this?

Mr. KAPPELMAN. Resistance.

Mr. SISTEK. How will that manifest itself?

Mr. KAPPELMAN. Well, you know, people do it in different ways. They will—sometimes it is overt, sometimes it is covert. The question becomes how do you deal with it, and realizing that there are early adopters to a change and there some late adopters to a change, those that are more skeptical and they want to see how things play out.

Mr. SISTEK. But let us say time is important. We do not want to take two decades to implement this change. What kind of tools—and I think you partially addressed this in your testimony—what kind of tools would you give this CIO? What type of authorities? What type of responsibilities? How far would his reach be, to quote Mrs. Carson's last statement?

Mr. KAPPELMAN. You have got to tie it to the money, and you have to tie it to the fact that their business people support the change, because the IT people go back to their little pieces of the enterprise, and if the business person is not on board for this, then it is no longer important. Nobody really does what is not important to their boss. So, unless the business people are also engaged, it is difficult to bring about these changes.

In other words, the business person is going to want one thing to happen, and if the CIO is saying, well, do something else, you know, you have these two conflicting authorities. So, management needs to be synchronized, on the one hand.

Secondly, it needs to be tied to budgeting, how projects get approved, how things get funded. If they do not comply with architecture, if they do not comply with security, if they do not comply with these other things, then they should not get funding.

Mr. SISTEK. Okay.

So, back to the organizational chart. Where do the lines from the CIO lead?

Mr. KAPPELMAN. Right now——

Mr. SISTEK. Hypothetical organization.

Mr. KAPPELMAN. Hypothetical? If you are going to have One-VA, you need to have central authority.

Mr. SISTEK. Thank you.

Second question deals with performance measurement systems: How do we know when we reach One-VA? How do we know when we get there? How do we know that the information technology overlay is working? Do we use some form of Six Sigma quality architecture overlay to this? How do we define success?

Mr. KAPPELMAN. Those metrics need to be determined, but some of them we knew about. We knew we wanted—you know, when they wrote that plan, the idea that a veteran could go to one interface and have contact with all VA services, that they could move from one hospital to another and not have to fill out forms again, you know, we knew some of the things that they wanted to achieve, but some of those metrics are yet to be defined.

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

Mr. BUYER. Mr. Boozman?

Mr. BOOZMAN. No questions.

Mr. BUYER. Thank you. Appreciate your testimony.

Mr. KAPPELMAN. It is an honor; I appreciate it.

Mr. BUYER. For our next panel, what we are going to do is we are going to combine panels two and three. So if Dr. McClure, Director of Information Technology Management Issues at the U.S. General Accounting Office, and the Honorable Richard Griffin, Inspector General, Department of Veterans Affairs, and those whom may be accompanying you—I have the written statements of the GAO and the IG of the Department of Veterans Affairs, your statements will be submitted for the record, and ask for you to present your testimony, introduce your guests.

STATEMENTS OF DAVID L. McCLURE, DIRECTOR OF INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY VALERIE MELVIN, ASSISTANT DIRECTOR FOR ACCOUNTING AND INFORMATION MANAGEMENT ISSUES, U.S. GENERAL ACCOUNTING OFFICE; AND RICHARD GRIFFIN, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY STEPHEN L. GASKELL, DIRECTOR, CENTRAL OFFICE OPERATIONS, DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF DAVID L. McCLURE

Mr. MCCLURE. Good morning, Mr. Chairman, I am Dave McClure, the Director for IT Management Issues at GAO, and with me today is the Assistant Director in charge of IT Audits, Ms. Valerie Melvin. We are happy to be here this morning and share with you our assessment of where VA is with several of the issues that we have been talking about.

In the testimony that we gave last April, we did begin to point out some signs of progress. We remain concerned about particular areas within VA's information management technology. I would like to share those with you today and be as straightforward as possible.

Let me start with the topic that Dr. Kappelman was discussing with you, and that is enterprise architecture.

The department is laying a very good foundation for an integrated enterprise architecture, something that we have been recommending to VA since 1998. As we have said in the past, this is a very important blueprint for evolving its information systems and optimizing them for the mission—the areas of the department. It is a formidable exercise. It is not anything that can be done without attention, time, and resources.

Executive management attention to VA's enterprise architecture I think is to be applauded. Some of the steps that have been taken over the last 11 months of getting executive commitment, involvement, buy-in, participation in the development of this enterprise architecture are really beyond what we see in many other agencies.

The appointment of a CIO, the recruiting of a chief architect are critical in continuing the progress in this area.

We have a table in my written statement that provides you with an assessment of where VA is in its implementation of its enterprise architecture. This analysis is based upon guidance that has been issued by GAO, OMB, and the Federal CIO Council. I think it paints for you a real marker of where VA actually is in its implementation of its management of this process.

It is clear that there have been many things that have occurred in the last 11 months that are extremely positive. There has been a chief architect that has been focused on this, not permanent but acting. There has been a governance structure that has been put in place, and there have been many of the beginning steps of defining the as-is architecture, both from a logical and technical perspective.

There are many other things, though, that remain to be done. That should be abundantly clear from looking at that table. We are many—we have many steps to go down this road before we actually can claim success, and as Dr. Kappelman indicated, this is an evolutionary, ever-changing, iterative, dynamic process that VA will be managing continually from now on.

So, we are pleased to see the executive involvement, participation in this enterprise architecture effort, but we do want to remind the committee and VA that continued management attention is essential to make sure that this continues in a very positive way.

The second area is information security. Our work and that of the IG has continued to show fundamental weaknesses in VA that place its financial, health care, benefits payment information at risk of misuse, fraud, improper disclosure, and destruction.

VA is continuing to make progress in this area, as well. At the direction of the department's cyber security officer, VA has embraced best practices guidance in this area, as well. In Table 2 of the written statement, we outline critical areas for the management of information security and show you where VA has taken actions and areas that remain to be addressed.

There are very positive developments that have occurred, again, over the last 11 months. There has been an emphasis on performance, the standards for SES, involving information security issues.

Risk assessment methodology guidelines have been established. There has been additional penetration testing of its web-sites, and there have been centralized functions put in place that VA has long needed, but there is many, many more things that need to be done and need to be addressed to ensure that fundamental security weaknesses are addressed and put in place. We would like to see specific milestones and specific actions in these areas.

You asked us, also, to comment on three systems modernizations occurring at VA—VETSNET, GCPR, and DSS, the decision support system used by VHA.

VETSNET, to start with, is a critical replacement exercise for the VA. Its existing applications on its existing infrastructure are at risk of failure. It does need to replace these as soon as possible. They are frail, they are old, and they are not actually performing as VA needs them to today.

Secondly, this is the core mission area of DBA. Therefore, the VETSNET project is critical for it to improve in the claims processing area.

VETSNET, in some form or fashion, has been going on for years, as you noted. There have been millions of dollars spent on infrastructure needs and applications associated with VETSNET. We recommend that three specific things in my written testimony be done immediately, completed on VETSNET:

A comprehensive testing of the system's functional business capability be performed. The Secretary has indicated that an audit has been conducted, but in our opinion, that audit did not cover some critical test areas to make sure that the applications are going to actually meet business needs.

Secondly, because of the elapsed time-frames that have occurred on the development of VETSNET, we think it's very important that user needs be validated once again. The applications that are associated with VETSNET are, for the most part, modernizing the as-is claims processing environment. If VA changes that claims processing environment through business process re-engineering, I think it is important to know how these applications will perform in that new environment. So, it is very important that this issue be addressed openly.

Thirdly, we think an integrated project plan needs to be put in place, something that has been missing, and we know that VA has committed itself to do in the past and in the conversations we have had in the last few days.

Real briefly, on GCPR and DSS, I think GCPR, as you know, is proceeding, but not in a way that was originally planned. The virtual patient record focus of GCPR is not what currently is being put in place. It is more of a data sharing exercise in which a one-way data transfer in the first phase will occur and is being tested between DOD and VA, has to be expanded to the Indian Health Service, as well. This is not the creation of the virtual patient record. It is a data-sharing capability. It is to be looked at as a positive development but one that is very different from the original goals of GCPR, and we would like to point that out to you.

We also believe there are still some fundamental project management weaknesses that need to be addressed with GCPR to ensure its success, and we believe, more importantly, accountability, authority, and responsibility—lead accountability, responsibility—need to be established for this tri-agency effort. That has been a problem in the past, as well.

In the use of the decision support system, this is extremely positive. We have seen continued acceptance of that executive support system to get a really good handle on the information in the hospitals on the cost of care and being able to compare cost of care across the different facilities.

It is now in use in all the VISNs, something that was not the case when we testified before you last time or the years prior to that, and we see that a continue positive acceptance of DSS, continued training and engagement by the managers in its use, is turning around the acceptance of it across the VISNs, and I believe it provides information to VHA that it did not have before, cost comparison data across the different kinds of health services. So, that is extremely positive.

In summary, I think what we would like to tell you is that VA has, indeed, made tangible progress since we last testified before you, and this level of executive commitment is extremely important, something that is missing in many other agencies. It has taken necessary steps but not sufficient steps in these areas that I have just gone over to ensure success. Continued management attention and resources need to be focused on each one of them.

We are recommending that VA focus its management activities on discipline processes, put them in place and follow them, and that is the key to seeing long-term success in any best practices-type organization, and lastly, we think the dialogue in this area across all these IT functional areas needs to begin to move to results. Once the plans, once the processes are put in place, VA needs to be held accountable for performance metrics and progress and showing that the mission areas that these systems are supporting are, indeed, improving results.

Thank you. I would be happy to answer any questions.

[The prepared statement of Dr. McClure, with attachment, appears on p. 39.]

Mr. BUYER. Thank you, Dr. McClure. Mr. Griffin.

STATEMENT OF RICHARD GRIFFIN

Mr. GRIFFIN. Good morning, Mr. Chairman. I am accompanied this morning by Steve Gaskell, the Division Director of our audit group that does the IT security audits for our organization.

Mr. Chairman and members of the subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs automated information security program. I am pleased to report that, since the committee's hearing last April, the department has named a CIO, defined an enterprise architecture, developed a VA firewall policy to protect the system from external attack, and the Secretary has recently approved a certification and accreditation policy to assure that IT systems have security reviews prior to being authorized to process sensitive information.

While we acknowledge that progress is being made, we continue to identify serious department-wide weaknesses in information security. As a result, we concluded in our recent audit of VA's consolidated financial statements for fiscal year 2001 that the department must continue to designate information security as a material weakness area under the Federal Managers Financial Integrity Act.

Our ongoing national audit of VA's information security shows that significant information security vulnerabilities continue to place the department at risk of denial of service attacks, disruption of mission-critical systems, and unauthorized access to and disclosure of sensitive financial data and data subject to privacy act protection.

Our current review revealed that many of the information system security weaknesses reported in our 2001 national audit remained unresolved and additional security weaknesses have been identified. Further action is needed to prioritize completion of key security initiatives, establish time-lines for completion, and secure necessary budget resources.

Based on our national information security audit results and discussion with officials in the Office of Cyber Security, we identified the key areas that should be considered for priority completion in the next year. Some of these areas require enforcement of existing department policy and governmental regulations while others require new hardware, software, or possibly contractor support.

Examples include intrusion detection systems, infrastructure protection, data center contingency planning, and operating system change controls.

In response to our findings, the department has identified these areas in its Government Information Security Reform Act remediation action plan for priority corrective action in the next 12 months.

Once these security initiatives are prioritized for completion, necessary budget resources will need to be secured. We recognize that the department faces a significant challenge to implement necessary security remediation actions that are estimated to require $804 million for fiscal years 2002 through 2006. This represents substantial expenditures above the levels funded in past years.

In fiscal year 2001, about $17 million was expended for cyber security program initiatives. For fiscal year 2002, about 21.4 million is budgeted for the Office of Cyber Security program initiatives. This level of funding support is significantly below the 93.2 million identified in the department's cyber security capital investment proposal.

In fiscal year 2003, the level of projected security funding requirements increases to over $132 million.

In addition to these Office of Cyber Security program expenditures, each of the department's administration budget also include program expenditures that address various security initiatives. For fiscal year 2002, these planned expenditures are significant and total approximately $34 million.

During our current national security audit, we will be reviewing individual administration security expenditures to assess the value of those expenditures in light of VA's national security priorities.

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

[The prepared statement of Mr. Griffin appears on p. 117.]

Mr. BUYER. Thank you, Mr. Griffin.

Dr. McClure, I would like you to do me a favor. I do not very often do this, but I acknowledge in the back of the testimony that you submitted to this committee, you have a team that put this together. I apologize. I got through most of it last night and finished it this morning, but your team did a remarkable job. This is a very difficult subject area, and I have requested a lot of—whether it is here or when I was on the Armed Services Committee—a lot of things from GAO, but you have got a great team here that put together a wonderful product, and will you please extend my compliments to them?

Mr. MCCLURE. I will certainly do it. Many of them are sitting with us today, and I know they are happy to hear that from you.

Mr. BUYER. This is excellent, excellent work, and you know, what I did like—because I am—believe me, I am outside my expertise, you know, and I really—I enjoyed this. This chart—whoever came up with this and designed this—it was very helpful to me to help put it together, sort of that checklist that is being done. I just want to let you know I found that to be very helpful to me, okay? Someone else may think it is very elementary, but I have a simple mind, I suppose.

One thing that I did notice—you stated that VHA has begun steps to further improve the accuracy and timeliness of its DSS data. Can you tell us what specific steps VHA has taken? How, quote, "on board" is VHA's top management in utilizing the DSS?

Mr. MCCLURE. Well, as I said, I think, if you go back over the last few testimonies that we have done, we have seen increasing use of the DSS. Three years ago, there was a question of whether all the VISNs were using it or not. There was also questions about the use of the data itself.

Our latest visits and conversations indicate that there is growing acceptance of the value of the DSS data and that some of the issues associated with the use of the system itself are now being worked out with user groups themselves, and I think that is a very positive development.

It is really a very valuable system to VHA in that, as I said, it is the only system that gives them a cost-per-episode type of ability to compare these things within facilities and across facilities. That kind of information is, I think, critical to focus on results and improvements in performance, and I think, as the system has been continuously worked upon and is being continuously used, the value—its value is being seen more and more by managers and executives within VHA.

Whether it is universally accepted or not—I do not know of any system that continuously gets universal acceptance, because there is always needs that might have to be addressed as it evolves.

Mr. BUYER. Would you be able to tell us which VISNs are using this as a critical management resource tool and which ones are not?

Mr. MCCLURE. Every VISN is using it in VA at the moment. That is a marked difference from, again, what we testified last year and the year before. Every VISN is using DSS, and again, I think part of that is the commitment and the understanding of the resource base needed to train users, to show the value of that system in doing the kinds of cost comparisons and performance comparisons that are needed across those facilities, very valuable tool in that sense.

Mr. BUYER. How would you characterize the success of the VETSNET project, and should VETSNET be terminated?

Mr. MCCLURE. I think, as I indicated, VETSNET is at a critical juncture. That is where I would put it. There are five—you know, with the five different applications—software applications that VA is working on to modernize its C&P systems with VETSNET—each one of them needs to make sure that it is looked at end to end in its ability to provide functionality for business needs.

The tests that have been conducted have not been conducted across all five of those applications. In fact, the two ones that are critical, really, for the aging BDN, the awards, and the FAS, the financial system, are still in the end stages of development. Those are critical to the replacement of some of the outdated applications on the existing network.

So, I think what we are recommending is that there be a full testing of the functional business capability of VETSNET, not just looking at its capacity issues and not just looking at stress tests but security and full business requirements being met, the user requirements being examined, because again of the passage of time and the very fact that this system is a field-based exercise. It means users in the field have to be knowledgeable, trained in the use of it, and that, I think, is very critical for its long-term success.

Mr. BUYER. Should it be terminated?

Mr. MCCLURE. I think it is too early to make a termination decision on the spot today, until these functional tests are performed and until some of these issues in which you are given specific information on them and then there can be, I think, a more informed decision about whether this should proceed or not.

Mr. BUYER. Thank you. Mr. Boozman.

Mr. BOOZMAN. I also would like to compliment you on—this is very readable and yet really provides an awful lot of useful information.

On the GCPR initiative, you state, "Nonetheless, progress on GCPR initiative continues to be disappointing," and then you outline why and kind of the things that are going on. I guess a lot of money is being spent in this area, and again, you know, you outlined some concerns. I guess the question I would have—are we asking them to do something that is just that difficult to do or is the road block that they do not want to do it? I guess my question to you is where are the road blocks? You know, what do you see as the failure in the area of this not being—in that it is disappointing, the progress that is being made.

Mr. MCCLURE. The exercise itself of being able to integrate data across three entities can be very problematic. The systems within each one of these entities—DOD, VA, and the Indian Health Service—were not originally designed to share information between them.

So you do have issues with how data is defined, how it can be used in a common fashion and still be accurate and reliable. Those are steps that really have to be done very carefully.

In addition, I think the technical solution has to be very well defined. Is this an interface? Is it something that would allow data to be manipulated by physicians and clinicians, no matter where they are housed to use it? Is it a repository, a replication of information, or is it actual data that is being used both from the service as well as veterans?

So those are issues that I think have been looked at, worked on for the last few years. The problem has been some of them have not been adequately resolved. There have been questions about leadership of the project, when you are involving three entities like this, and a very good value case being presented on what are we going to be able to do better and when can we begin doing some pilots and testing of this to show that the results are there, and those are issues that I think, to overcome these obstacles, have to be addressed with a lot of discipline.

Mr. BOOZMAN. You mentioned that the mission, you know, had been changed somewhat, you know, in what they are doing. I guess that, to me, is a fundamental problem, you know, in the sense that I guess I would say that, if the mission has been changed, how does that—I mean where is that authority coming from? You know, how do we rectify that situation?

Mr. MCCLURE. I think that is a good line of questioning to pursue. It could be that the strategy for GCPR is, indeed, changed from the virtual patient record type of approach to a data-sharing approach. I think that that needs to be articulated very clearly by the three entities involved. If not and what we are seeing is an evolution and a testing and a demonstration of the ability to share data that will then be built upon to try to achieve the original goals of GCPR, that needs to be articulated.

So some of that, I think, is where there are some uncertainties as to where we are headed long-term that would be good to get more information on.

Mr. BOOZMAN. Okay. Thank you very much.

Mr. BUYER. Thank you.

I will recognize counsel for Ms. Carson, Mr. Sistek.

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

Dr. McClure, you mentioned the fragility of the BDN system at Hines. Could you speak to where can we expect a break-down there, or can we keep patching for a longer period of time, if necessary? Clearly, it is performing an essential business function. There is some point in time where, if we lose the capability to perform that business function, we are going to be in a world of hurt. Give us a perspective of how long we can keep patching.

Mr. MCCLURE. You can keep patching it until the end of time. You can keep putting patches on it. You can keep spending money. The time-frames for the extension of BDN continue to go out. As you know, it is a reliable payment system. It is not that it is broken down and crashing at the moment. The issue is risk. How much longer can the applications survive because of their proprietary, outdated coding, and keeping the resources focused just to maintain that? I think that is an issue.

It also means that those resources being spent to maintain that environment are resources that are being taken away from the new environment that VBA needs to move toward, and that tension is going to be there until, again, VETSNET or the C&P replacement is put in place and begins—sequenced into place, I should say.

Mr. SISTEK. Dr. McClure, on page 3 of your testimony, you state, concerning the cyber security office—you state, “Moreover, VA’s current organizational structure does not ensure that the cyber security officer can effectively oversee and enforce compliance with security policies and procedures.” You elaborate on this at page 20. How would you draw the dotted lines here if you are putting together an organizational structure? I think I know the answer.

Mr. MCCLURE. Well, it is a situation that we really wanted to make sure you understood, the committee understood. Creating the Office of Cyber Security is a gigantic step forward. Having a cyber security officer is a gigantic step forward. We have numerous security positions across VA that remain unfilled. That needs to be addressed. We have others that report on a full-time, permanent basis on security issues and others that are part-time.

What is challenging in an environment such as VA’s is the fact that it is so decentralized, and one of the tools that a cyber security officer needs it not only to write policies and procedures for how security would be done but be able to follow up on enforcement and compliance, and what we are recommending is that at least the relationship between the security officers throughout VA and the cyber security office be more definite, and in that sense, there can be more accountability as to the security officers’ actions.

I do not want to imply, however, two things—one, that it should be command and control totally on security issues from that office. Security has to work in a decentralized environment, and you must have real good security, people, process, and technology throughout the enterprise. The second thing I do not want to leave the impression is that only the security folks should do security functions. The business lines have to be involved and be held accountable for the security of their systems, and I think, again, that is a separate issue from simply the security officers reporting to the Office of Cyber Security.

Mr. SISTEK. In that last comment, you refer not only to technical implementation but a cultural change that makes people more security aware, and that has been brought out in previous hearings by the chairman.

One quick question for Mr. Griffin.

In your October 24 report of last year, you reported and recommended centralized budgetary control, but the Principal Deputy Assistant Secretary for Management at the VA disagreed with that centralized budgetary control. There was discussion in the report about other measures—other control measures being put in place and that you thought that those control measures were acceptable and you considered the issue resolved and you would follow up later with the department.

That report was in October. Do you have a sense of how things are going now? Are those control measures working to assure the proper budgetary line?

Mr. GRIFFIN. We are monitoring the progress there, but our point was you cannot have, in this decentralized VA, people in the field buying whatever they want without having a focus on whether it is part of your system-wide integration. Our recommendation was, that the CFO, who sits on top of the budget process, be responsible for reviewing proposed purchases and ruling on them, so we would have somebody at a national level doing that type of review.

The decision that was made was to have the CIO be the person to review and approve from a budgetary perspective. If something comes across the CIO's desk that is totally out of sync with the system that they are trying to put in place, whether it is economical or not, if it does not fit with the system, the CIO then is in a position to disapprove the purchase.

So that is the path that was chosen, and we will continue to monitor to make sure that there is oversight on a national system-wide basis.

Mr. SISTEK. Thank you very much.

Thank you, Mr. Chairman.

Mr. BUYER. Mr. Griffin, has your office thought about establishing an office solely devoted to investigating cyber crime, such as NASA's IG office has recently established? Do you think that is a good idea or not?

Mr. GRIFFIN. We have a unit like that, sir.

Mr. BUYER. Okay.

Mr. GRIFFIN. We started a cyber unit about 18 months ago.

Mr. BUYER. Great. Working out well?

Mr. GRIFFIN. Very well.

Mr. BUYER. You need more people and resources?

Mr. GRIFFIN. Well, we trained a cadre of people. We hired some experts when we started the unit, and we have trained some of our existing criminal investigators to bring them up to speed. So far, we do not believe there is more work in that area than we can deal with, but certainly, if it appears that that is going to be the case, I will make the adjustments.

Mr. BUYER. I would like to also—Mr. Gaskell, let me thank you and your auditors for crunching the numbers and doing all the things. It does not get a lot of publicity and people do not focus on it, but you have always been very responsive to the committee's requests, and I appreciate that.

Mr. GASKELL. Thank you very much.

Mr. BUYER. Mr. Boozman, do you have anything else?

Mr. BOOZMAN. No.

Mr. BUYER. This panel is now excused. Thank you very much for your quality work.

Our last panel is the Honorable John A. Gauss, the Assistant Secretary for Information Technology, Department of Veterans Affairs.

I would like for you to introduce the guests you brought with you and their functions, and then your written testimony will be submitted for the record, and you may begin as soon as you are prepared.

STATEMENT OF JOHN A. GAUSS, ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY BRUCE A. BRODY, ASSOCIATED DEPUTY ASSISTANT SECRETARY FOR CYBER SECURITY, DEPARTMENT OF VETERANS AFFAIRS; GARY A. CHRISTOPHERSON, CHIEF INFORMATION OFFICER, VETERANS HEALTH ADMINISTRATION; K. ADAIR MARTINEZ, CHIEF INFORMATION OFFICER, VETERANS BENEFITS ADMINISTRATION; WILLIAM CAMPBELL, DEPUTY ASSISTANT SECRETARY FOR FINANCE, DEPARTMENT OF VETERANS AFFAIRS

Mr. GAUSS. Yes, sir. Thank you very much, and good morning, Mr. Chairman. I have with me the Chief Information Officer from the Veterans Health Administration, Mr. Gary Christopherson. I have the Deputy Assistant Secretary for Finance from the central office, Mr. Bill Campbell. I have the Chief Information Officer from the Veterans Benefits Administration, Ms. Adair Martinez, and I have my chief cyber security officer, Mr. Bruce Brody here at the table with me.

It is a pleasure to be here this morning and discuss some of these very important issues. Due to the length of the written statement that I submitted, I would like to briefly summarize some of the key points.

On behalf of the Secretary of Veterans Affairs, I am pleased to be here today and update you on the progress the department has made in strengthening our information technology program and specifically address issues related to enterprise architecture, cyber security, VETSNET, decision support, and the government computer-based patient records program.

Last April, the Secretary appeared before this committee and gave you his personal commitment to reform the way VA uses information technology. Those specific commitments are included in my written statement. I am pleased to report to you today that it is no longer business as usual in VA's information technology program.

With respect to enterprise architecture, the department has selected a methodology known as the Zachman framework to develop and maintain its One-VA enterprise architecture. This methodology is a systems engineering approach that requires us to define all aspects of the VA enterprise, from a business process, data, location, schedule, personnel, and requirements perspective before we begin modernizing our legacy IT systems. This work is well underway.

From a technical perspective, we have developed a technical implementation model for the future VA information technology enterprise. Companies in the private sector that have successfully modernized their IT enterprises have taken a two-prong approach to their modernization.

First, they modernize their IT infrastructure to provide a network and computing environment capable of implementing re-engineered business processes. In parallel, they re-engineer their business processes, modernize the IT used to implement those processes, and finally, implement the IT on that modern, high-performance, cost-effective infrastructure. These best commercial practices are part of our overall strategy.

Cyber security of our networks and systems is another issue that has the Secretary's highest priority and has my number one priority. In order to effectively secure our networked information, we must completely understand the topology of our data network.

Our current 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 impedes our ability to properly secure and assure network services. Further, our current network infrastructure does not support modernization of our enterprise, as previously discussed.

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. We have established department-wide priorities for security VA's computing enterprise. Our first priority is securing VA's boundaries against external attack.

As we transition to a performance-based network, we will collapse the total number of gateways to external networks to a manageable number while providing significantly increased security protection at these gateways. This and our data network efforts are key components of our approach to implementing a secure enterprise architecture and correcting cyber security deficiencies noted by our Inspector General and the General Accounting Office.

Major improvements in our cyber security posture include deployment of anti-virus software across the entire department, implementation of a VA-wide firewall policy, and development of a comprehensive certification and accreditation policy.

The specifics related to VETSNET, the decision support system, and government computer-based patient record program are contained in my written statement.

Mr. Chairman, I am very concerned about two other areas in addition to what I have talked about this morning.

First, we need to reverse the trend in IT spending. Our overall IT budget continues to grow. Even more troubling is the sustainment cost to operate and maintain in-service IT systems as a percentage of the overall budget. As we formulate the budget for fiscal year 2004, we will develop a 5-year strategy to reverse these trends in IT spending.

Second, just like other agencies, our IT workforce is aging, with a large percentage nearing retirement. To address this issue, I have launched an aggressive IT workforce initiative to develop and implement a plan for evolving the workforce, recruiting new people, and training current employees.

I hope I have provided some insight as to why it is no longer business as usual at VA. I believe these efforts demonstrate our very strong commitment at all levels to build an effective information technology program for the long term.

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

[The prepared statement of Mr. Gauss appears on p. 122.]

Mr. BUYER. I could not help but think that all the years that you gave to the country in service to the U.S. Navy, you sit before us as an admiral, retired admiral, in a position where you have no distinct line authority. So I look and say, you know, if I were an admiral and I am now brought onto a staff, how do I define what my authority is, and I sure do not want my services to be purely pastoral.

Mr. GAUSS. Yes, sir. When I was asked to submit a resume for this position, I came down, was interviewed, and talked with the Secretary, and the Secretary made it perfectly clear that he wanted this area of information technology attacked and attacked with a fervor. Further, he indicated and later published a memorandum empowering the CIO to fix these problems within VA. He further published a memo that provided the dotted-line connection for matters of IT between me and the people who are sitting here at the table, except for Mr. Brody, who is a direct report.

Clinger-Cohen gives the CIO authorities to approve the expenditure of funding, approve the planning, approve the programs, and using that authority, I believe that I can exercise a positive control over the enterprise.

During my military career, I spent 22 years in the acquisition side of the house. The acquisition side of the house is very much like how VA is organized in terms of lines of authority and the ability to influence outcome. So, this is not an environment that I am unfamiliar with.

Mr. BUYER. I hate to keep going back to your military career, but I'm trying to figure out how you actually do this when you have a position with no line authority, and even though you have—you know, you are sort of a representative here—what do you when a bureaucrat, in particular on of the—I do not know—within the benefits—you have got a bureaucrat there that tries to do an end run on you?

Mr. GAUSS. We have made some fundamental process changes at VA, Mr. Chairman, to try and prevent that.

Now, have we become foolproof? No, sir, we have not. We have put in place a tracking system to track all expenditures. Any IT expenditure and execution has to come to my staff for review and approval in execution prior to it going out the door.

I am working with the Assistant Secretary for Management to put similar controls down the contracting path and down the financial authorization path so that if someone were to say I am going to bypass this process, it is too hard, we will have checks and balances on the contracting and financial authorization end.

Mr. BUYER. I guess, Admiral, when I look at this, they have got to believe that, when the dust settles at the end of the fight, that you are standing.

Mr. GAUSS. Yes, sir.

Mr. BUYER. Right?

Mr. GAUSS. Yes, sir.

Mr. BUYER. Well, let me ask it this way. You are comfortable that the Secretary has empowered you to do what you need to do to get the job done.

Mr. GAUSS. Yes, sir, I am, and in fact——

Mr. BUYER. Okay.

Mr. GAUSS (continuing). I would not have considered applying for this without——

Mr. BUYER. We, this subcommittee, needs to know, then, who we then hold accountable, okay? Responsibility will rest with the Secretary, okay, but we need to know who we are going to talk to.

So, we are not going to go into these three stovepipes and beat them up. We are going to come to you. We are going to give you the compliments, and we will rest it all to you. If we do not like something, we are going to come to you. Is that correct with regard to this implementation of the One-VA? It is you.

Mr. GAUSS. Yes, sir. My military experience is that the Secretary is accountable for everything. He has delegated responsibility to me and accountability for that responsibility for matters of information technology, and I stand ready to assume that accountability that is commensurate with that responsibility.

Mr. BUYER. All right.

The tragedy of September 11 heightened the awareness and concerns regarding the preparedness of all Federal agencies for continuity of operations and information assurance in the event of another manmade or natural disaster. Due to the sensitive nature, I am not asking you to discuss specific vulnerabilities that you feel—are uncomfortable discussing in an open forum. However, given the importance of these two areas, in your view, are improvements needed in these areas? More directly, what specific steps are being taken to ensure that VA operations can continue in the event of a catastrophic event?

Mr. GAUSS. When I came to VA last August, I looked at the continuity of operations that was in place, the processes and procedures, and it was my view then and it is my view now that VA has not taken advantage of what technology brings to bear for continuity of operation, for quicker restoral of service.

In my opening remarks, I talked about the need to modernize our data network. With a modern, high-performance data network, we can use technology to electronically vault data to other geographic locations from our data centers and bring up restoration of service far better than the process that is in place today, which is to back it up on tapes, fly it to coop sites, send people there with it, and stand it up in 72 hours.

So, there is much to be done in that area.

Mr. BUYER. Last year, with much fanfare, VBA announced it was paying 10 veterans payments using VETSNET's C&P as the demonstration test. Have anymore claims been processed and paid using the automated VETSNET project?

Mr. GAUSS. No, sir. The intent of that demonstration was to demonstrate that the processing of claims was not tied to existing ways of doing business. There were 10 very simple claims using very rudimentary processing. Much more complex claims require additional development in those two modules left to complete that the General Accounting Office discussed in their testimony.

Mr. BUYER. When over 3 million VA beneficiaries received legislative cost-of-living increases this past January, did the 10 VETSNET beneficiaries get their increase?

Mr. GAUSS. Yes, sir, they did.

Mr. BUYER. Okay. Will you explain—was it through the system or was it by—was there a problem with it, though?

Ms. MARTINEZ. There was not any problem with it. We changed the system. We now only have nine vets being paid, because one just moved to West Virginia, and they are being paid through BDN. There was no problem with the COLA.

Mr. BUYER. Okay. But it was not sent out in January. It was reprocessed and done in February?

Ms. MARTINEZ. I was there in January, and they were doing all of the work to do it. I am not aware that it was reprocessed for February.

Mr. BUYER. All right.

I yield to Ms. Carson.

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

Dr. Gauss, in your written statement, you address the two-prong approach that private sector companies have successfully used in modernizing their IT enterprise. You state, quote, "First they modernize their IT infrastructure to provide a network and computing environment capable of implementing re-engineered business processes. In parallel, they re-engineered their business processes, modernized the IT used to implement those processes, and finally implemented the IT on the modern, high-performance, cost-effective infrastructure." Then you go on to say, "These commercial best practices are part of our overall strategy."

My question, then, Dr. Gauss, is how does the proposed VETSNET system, devised in 1985, embarked upon in 1993, and still mostly unrealized, fit into the commercial best practices schema you endorse for the VA?

Mr. GAUSS. The technology that is being used in VETSNET today that was under test, as mentioned earlier, is technology from the mid-1990s. It does client-server operations. It is not state of the art as of 2001 and 2002.

Much has been invested in that technology that I believe can be reusable in meeting the objective of shutting down that old mainframe system and get to a more modern technology framework. Sometime in the future, we will need to put some performance improvements into VETSNET, but we first have to get it operational and shut down that legacy mainframe system.

Ms. CARSON. If I may, Mr. Chairman, ask him another question—I apologize for being in and out. Sorry about that. I did have the advantage of your testimony. You had indicated that veterans are best served—are veterans best served or is the department best served by the status quo?

Now, you have some great minds here that is assembled here, but don't they all report to different under secretaries?

Mr. GAUSS. For normal reporting processes, each of the people at this table, except Mr. Brody, report to other people. However, last summer, the Secretary published a memo giving me indirect reporting with these people on matters of IT. So, I have the ability to go direct to everyone at this table to reconcile issues related to our information technology programs and architecture.

Ms. CARSON. Uniformly, then, you have one-line authority across the board and they can all feed into you so that there is some uniformity in terms of what you do?

Mr. GAUSS. We have developed that process to do that, yes.

Mr. BUYER. She asked a specific question. I mean, do you have the specific line authority? The answer is no.

Mr. GAUSS. No, sir. No. In my answer, I said that I do not have direct line authority. I have indirect authority for matters of IT, and so, I have a sub-organization within the structure where I deal directly with these people on matters of enterprise architecture, IT, and cyber security, and that is an efficiency gained over the past year, because I do not have to go to an under secretary to get it approved to go to the deputy under secretary in order to go to one of the CIOs. I pick up the phone, call direct, we work the issues, we get them solved.

Ms. CARSON. I am still having some problem with indirect, but I will leave that up to the chairman to sort all that out. Thank you very much, Dr. Gauss.

Mr. BUYER. Well, Ms. Carson, that was my concern, too. What we have here is testimony from an individual that the Secretary has chosen to lead this, and he is here before us saying I am the man that is responsible, and so, I have got some concerns, too, if I have got someone who does not have specific line authority, but if his testimony to us is that he can figure this out, he is going to make it happen, this is the person that we are going to have to work with to make sure all this gets implemented. I share your concerns, Ms. Carson.

Mr. GAUSS. Mr. Chairman, may I add, in my last job, I was the commander of a material acquisition command. I reported directly to the vice chief of naval operations. He did not provide me my money. That came from four or five different resource sponsors. My customers were four-star admiral fleet commanders. I had lots of indirect lines, and when the four-star called, I did what I needed to do.

So we are taking some of the military structural organizational constructs and applying them to our IT here. Not all of them had to go to the vice chief of naval operations to get me to do what I needed to do if I needed to help them.

Ms. CARSON. Do all the under secretaries report to you, then?

Mr. GAUSS. The under secretaries report to the Secretary. The chief information officers here at the table report directly within their administrations, but on matters of information technology, they report to me.

Ms. CARSON. So, you have the sole jurisdiction of IT.

Mr. GAUSS. Yes, ma'am.

Ms. CARSON. You are it.

Mr. GAUSS. Yes, ma'am.

Ms. CARSON. Anything that is sort of——

Mr. GAUSS. Well, the Secretary is it. On his behalf, I am it.

Ms. CARSON. Yes, I understand. The Secretary had said that, if at any point, the best interest of the veteran, are not being served, that the Secretary was prepared to change the reporting mechanism. As I understand you, your response to the chairperson, that you are ready to take full responsibility, all the hits, like in the military, if it does not work.

Mr. GAUSS. Yes, ma'am.

Ms. CARSON. Okay. It is probably engaging in another war you probably do not want to be in.

Mr. GAUSS. There might be some wars that you do not get to see in these chambers here in the process.

Ms. CARSON. Yes, we have the President of the United States on Capitol Hill. If I see him, I will tell you him you are the hit man.

Thank you very much.

Mr. BUYER. Mr. Boozman, if you will be patient with me just a second, Ms. Carson and I both are trying to figure this out, and obviously, Admiral, if you are comfortable with it, I suppose I am supposed to be, and so is Ms. Carson and this committee, but you know, when you look at what the IG has submitted to us, when you look at what GAO has submitted to us, they are complimentary, and then they put in the semicolon, however.

Mr. GAUSS. Yes, sir.

Mr. BUYER. They are complimentary, but they are also—and I will even accept the testimony of our experts over the framework for us to be patient. It is so very, very important at the beginning to make sure that the individuals who are selected are empowered and have the authority to do what they have to do. I guess I learned long ago, direct line authority is pretty important in order to get someone to be extremely responsive.

I mean if you are paying them and they know that you are rating them—let me ask that question. What input do you have with regard to rating people?

Mr. GAUSS. I have direct input to the reporting seniors of these folks for what goes into their performance evaluation.

Mr. BUYER. Okay. Then, with regard to promotions, with regard to merit bonuses, do you have input in that, also?

Mr. GAUSS. The process at VA——

Mr. BUYER. If you are working with someone in one of those administrations who is messing with you and making life difficult to get this implementation going, do you have the ability to say no, they are not entitled to a merit bonus?

Mr. GAUSS. I do not have that. The bonuses are provided at VA on an as-occurring basis. It is not like an end-of-the-year, total performance type of an award, but I certainly have input into their performance evaluations that document their performance, and should Mr. Christopherson decide that he does not want to proceed the way I wanted to, I will make this an issue with his boss, and if necessary, I will make it an issue with the Secretary.

Mr. Chairman, we have made some changes in how we operate within VA. May I recommend that we have a post-hearing question to lay out what those are specifically and then document how we believe this will work?

Mr. BUYER. All right. Thank you. Mr. Boozman.

Mr. BOOZMAN. I just want to compliment you on taking on a big job. You know, this is a big job, and I certainly think you are up to the task.

We had a report from the GAO earlier. Is there anything that you see—are there any discrepancies that you find with that, or do you feel like that they are on track with their report as to kind of what is going on with the system and where we are heading?

Mr. GAUSS. I, too, agree that the report that the GAO submitted to this hearing is an excellent piece of work, and I plan to keep that by my side as we move into the future. There are minor things that I will address separately, but they are of such insignificant magnitude, I would not want to bring them up here to this committee.

Mr. BOOZMAN. So overall, you felt like that was accurate.

Mr. GAUSS. Overall, I thought it was an excellent report and very fair and objective on where we are.

Mr. BOOZMAN. Thank you.

Mr. BUYER. Dr. Gauss, Ms. Carson and I have spent a lot of time on the whole question about your line authority, and you might say, you know, of all the things that are out there, trying to implement this One-VA system, why are we spending so much time on that?

I am not going to speak for Ms. Carson, but I do believe that the two of us—we want to make sure that you are empowered and people understand within the VA administration that everybody is looking to you to implement this, and if we receive this testimony about the—and these are my words—about the cultural bias and the inertia that is out there by some tenured individuals, using the doctor's word, we think it is pretty important, and you know, we are looking right now to the Secretary. The Secretary creates this position, brings you in. We are looking at it from the position of—we are going to evaluate.

So we would like for you to submit that to us. Please make it timely, and I think this committee, in a bipartisan basis, will evaluate whether or not we need to actually legislate a position, and I can assure you, if we actually legislate the position, we are going to give you all types of line authorities.

Now, just because I just mentioned that here this morning, you are going to hear all types of people coming in saying why that is such a bad idea. I would welcome your attentive listening to those individuals who are anxious to tell you why it is a bad idea, you know?

Mr. GAUSS. Sure.

Mr. BUYER. Because I do not know if it is a bad idea or a good idea, and earlier on I said I do not want us to be micro-managing, and we are going to do our oversight function, but I do know that it is extremely important that we have someone at the top that has direct line authority and chain of command. Admiral, if it requires us to make a legislative position to do that—the taxpayers are putting a lot of money into this, and we want to make sure of its success, and we are going to make you the captain of the One-VA ship, all right?

Mr. GAUSS. Yes, sir.

Mr. BUYER. If it requires us to actually legislate that position, I think this committee is prepared to do something like that, but we will also be a good listener. We want to evaluate what you submit to us, and we will sit down with you, we will talk with the Secretary, and we will see whether or not we should actually make this a specific position and empower you to do what is required. Billions of dollars are at stake. A lot of contracts out there are at stake.

With that, I do have one question I wanted to ask you and forgot to. On standardized software, as you go down the integrated enterprise architecture path, do you require standardized software throughout the three administrations? Is that what you are sort of looking toward?

Mr. GAUSS. In the software arena, there are some software products that are commodities, where commercial standards have emerged, where it does not matter what the brand name is on the product, it will work and be inter-operable. There are certain technologies where the power of the technology is vendor-unique and the commercial standards are very weak. It is in those cases that, in order for us to exchange information and be inter-operable, we will, unfortunately, have to standardize, and anyone who needs to use that function would have to use the standard product.

Mr. BUYER. Are there any existing problems with Microsoft at the moment, between your office and that company, existing contracts?

Mr. GAUSS. I'm sorry, sir?

Mr. BUYER. About an existing contract?

Mr. GAUSS. We had an enterprise license with Microsoft for 180,000 seats and some number of servers in the back office, and it was due for renewal, and we chose not to renew that enterprise contract. The dollar value associated for the benefit gain this fiscal year traded against patient health care did not seem like a reasonable balance, and so, we own licenses for the computers that we have. We have Windows 2000 products. We have Office 2000 products. Our licenses with Office 2000 are portable from one machine to another.

So, as we buy new computers, we will pay the GSA schedule rate of $130 per machine for a new license vice $8, and what we lose by not renewing the license is the rights to upgrade to the next generation of product should and when it be released.

Mr. BUYER. Whose decision was that?

Mr. GAUSS. It was a collaborative decision between myself, the acting under secretary for health, and we advised the Secretary of what we planned to do, and he and the deputy secretary concurred.

Mr. BUYER. A collaborative decision. I do not get that. If we empowered and created a position for you, would you be calling it a collaborative decision?

Mr. GAUSS. Yes, sir, I would, and I would because I need to have cooperation from folks. Having line authority and a hammer is an important thing to do, I will not argue that, but I still need to have cooperation from the administrations in these types of decisions that have potentially broad-reaching impacts.

Mr. BUYER. All right. Ms. Carson.

Ms. CARSON. I agree with the chairman wholeheartedly on line authority. Let me take another spin to it, just at a different perspective—not a different perspective. Do you feel comfortable—could you be very open and candid about whether or not you feel comfortable in recommending something that is probably broke and needs to be fixed? I know, oftentimes, government people have apprehension about writing down their observations. The only federal people I have seen that have no observation was the Immigration and Naturalization Service people. Do you have some reservations about doing this?

Mr. GAUSS. No, ma'am, not at all.

Ms. CARSON. Okay. You do not anticipate any repercussions about describing what is broke that needs to be fixed.

Mr. GAUSS. No, ma'am, I do not.

Ms. CARSON. Okay. Fine. Because you were going to get an opportunity to opt out of this at this time. Now you do not get that opportunity anymore. Thank you very much.

Mr. BUYER. Thank you, Ms. Carson.

Mr. Boozman, do you have any follow-up?

Mr. BOOZMAN. No.

Mr. BUYER. Dr. Gauss and the team, thank you for coming over. We are going to have some follow-up written questions that we are going to submit to you, and I would like to have the follow-up discussion with this committee and find out—and we need to make a decision.

Mr. GAUSS. Yes, sir.

Mr. BUYER. Okay? We will make a, quote, "collaborative" decision——

Mr. GAUSS. Yes, sir.

Mr. BUYER (continuing). Amongst the members of the committee on whether or not we actually create a position for you, all right?

Mr. GAUSS. Yes, sir.

Mr. BUYER. Thank you.

Mr. GAUSS. Thank you.

Mr. BUYER. The meeting stands adjourned.

[Whereupon, at 11:52 a.m., the subcommittee was adjourned.]

APPENDIX

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
U.S. House of Representatives, 107th Congress of the United States

Wednesday, March 13, 2002 Hearing

Written Statement of Leon A. Kappelman, Ph.D.
Director, Information Systems Research Center
Farrington Professor of Information Systems
Professor, Business Computer Information Systems
College of Business Administration, University of North Texas

Introduction

Mr. Chairman and esteemed Members of the House Subcommittee on Oversight and Investigations of the Committee on Veterans' Affairs, thank you for this opportunity to testify about the progress I have seen over the past 10 months in how the Department of Veterans' Affairs manages information and information technologies (IT) in support of its mission.

During May, June, and July of last year I had the honor of facilitating the efforts of over 20 of VA's senior IT and business leaders, from all Administrations and Department staff offices, in forming what came to be know as VA's Enterprise Architecture Innovation Team. Over the course of 15 days and five very long weekends, with plenty of individual time in between studying, writing, and working in small groups, they created and unanimously endorsed the document that was approved by Secretary Principi in September 2001 and that you know as VA's "Enterprise Architecture: Strategy, Governance, & Implementation." Since then I conducted an analysis and review of VA's project management practices and also had the privilege of facilitating, in October and again just a few weeks ago, two working conferences attended by more than 200 of VA's senior and technical IT managers.

The short story is that in these past 10 months I have seen a profoundly positive transformation in how VA manages IT. I remember how at first many of the members of the Enterprise Architecture Innovation Team believed that it was undesirable and impossible for VA to have a single integrated enterprise architecture. That belief was replaced by the revelation that it is not only possible but also highly desirable to have a single integrated enterprise architecture in order to manage IT to achieve the noble vision of "One-VA." And they put their new beliefs into action by laying the foundations of good IT planning and governance in their "Enterprise Architecture: Strategy, Governance, & Implementation" document. But the vision and planning of 20-some people, no matter how senior, does not suddenly transform an enterprise with over 220 thousand personnel, a budget larger than most of the world's countries, and historical roots in distinct and separate enterprises.

The next steps are well underway, as evidenced by what I experienced first hand at the two VA CIO conferences that I facilitated over the past five months. But they are steps on a long, and in some ways never-ending journey; and so, I am here today to suggest to you, the Congressional leaders who are in essence the "Board of Directors" of VA, and the elected representative of their "stockholders," the people of the United States, that your cooperation, and support may also be called for if success is to be maximized.

VA's Enterprise Architecture Innovation Team did not take the easier, softer road in creating their vision for a One-VA Enterprise Architecture. They created a new IT governance structure that is beyond the reality of VA's current organizational structure, they selected the most comprehensive and complete framework for organizing their work, they incorporated performance measurement, project management, and continuous quality improvement into their plan, and they acknowledged that a profound change in the attitudes and culture of VA would be necessary for their fundamental success. John Zachman may have said it best in the cover letter he wrote to Secretary Principi to accompany the "Enterprise Architecture: Strategy, Governance, & Implementation" document:

> I would like to take a moment now to talk about the road that lies ahead. The role of the Information Technology community in an Enterprise is not simply to build and run systems. This is what results in disintegration, "stovepipes." Rather the mission of the information folks in any Enterprise is to engineer and manufacture the Enterprise such that it is aligned with the intent of General Management and is flexible, adaptable, interoperable, integrated, lean, etc. and responsive to the Enterprise's "customer" (as well as to other Enterprise "stakeholders"). ... This is a new way of life. There is no quick fix. This is not a project. It is a "process." It is different from the Industrial Age past. It is the Information Age present! With that understanding, I would like to impart on you some advice that may help as you continue down your road to institutionalize the Department of Veterans Affairs Enterprise Architecture:
>
> - Do not underestimate the difficulty and complexity of engineering and manufacturing the most complex object yet conceived by humankind – the Enterprise. This will take time and determination.
>
> - This is a new way of life, a revolution in thinking, a discipline, an engineering process. Change of this magnitude takes time and perseverance. Do not get discouraged. ...
>
> - Make executive education and technical training a continuous process. Don't assume anything. It is easy to forget long-term issues in the short-term stress of daily life.
>
> - And remember, the state of the art is only fifty years old or so and the "playing field" still pretty level – there is still much to learn and discover, and many opportunities to create advantage and value. (John A. Zachman, July 20, 2001 letter to Secretary Principi, appended in its entirety at the end of this written testimony.)

Background and Perspective

It may be a "small world," but it is also a very complex one. And human beings have done a good job of succeeding in it. Anthropologists credit much of that success to our bigger brains, and how we've used them to develop languages, tools, and technologies. One especially useful mental technique we've developed is to seek simplifying explanations for what are often complicated realities. We find comfort, value, and usefulness in the various theories, hypotheses, models, frameworks, taxonomies, and paradigms that help us better understand and manage our world, our organizations, our technologies, and our lives. In fact, such partial truths underpin almost all of our scientific and technical progress, as we improve our understanding of reality, the "truth" if you please or what Einstein called "God's thoughts." Our simplifying mental models have their downside, however, depending on the importance of the things they leave out.

Consider this: In the "science" of 1850s' medicine, microorganisms and disease were not related and thus the death rates from infection averaged around 50% in European hospitals and contagious diseases spread easily. It's not that bacteria weren't killing people, it's just that our view of the world did not recognize what was actually occurring, until Semmelweiss, Pastuer, and Lister came along. But many years passed before this new paradigm and their discoveries were adopted as new behaviors and practices, and yet even as the 20th century began surgeons still worked in their street clothes.

IT is an enabler. IT alone doesn't make organizations more efficient, effective, or better places to work. In fact, the exact same off-the-shelf software application can be part of great success in one organization and total failure in another. It's not the technology, but how we use it. And we are still in the early stages of learning how to really use IT to enable the success of people and the organizations, societies, and economies they create. In short, we haven't really figured out yet how to get much bang for our IT bucks.

If you question that conclusion, consider the research of Paul Strassmann (former top IT executive at the Department of Defense, Xerox, and General Mills) which indicates that only about one in five businesses gets a reasonable rate of return from IT spending and that two in five actually get a negative value added from IT investments. Or if you read the IT press, I wonder if you've ever seen a list of CIO key issues that didn't have some version of "IT alignment with organization goals" in its top 5? Me either. But why, after 30 years on the top of our concerns, haven't we figured out how to do alignment? The sad fact is that we don't even have decent metrics to measure alignment. Therefore, given total quality management creator W. Edwards Deming's admonition that we cannot manage what we do not measure, it's no wonder we are still not managing alignment very well.

Consider this: The profound change in the world that we call the "industrial revolution" had its beginnings in the second half of 18th century England and came to America in 1790 when Sam Slater built the first steam-powered cotton-processing machine. In 1797 Eli Whitney pioneered standardized parts and division of labor in the manufacture of muskets. Ninety-five years later the Duryea brothers built the first gasoline-powered automobile. Still, 20 years more would pass before Henry Ford combined the moving assembly line technique with division of labor and interchangeable parts in a way that began the transformation of manufacturing as we knew it, lowering the price of the Model A from $850 in 1908 to $310 in 1926 (with some help from Frederick Taylor's 1911 publication of "Principles of Scientific Management"), and thereby transforming our socio-economic milieu.

The information age began in 1945 with the "invention" of the computer as a result of a war effort that required massive amounts of mathematical calculations, a U.S. Federal government with the vision and resources to fund the work, and the creativity of Eckert, Brainerd, and Mauchly. Information technology has made astonishing progresses over the past six decades, and many good things have come of it. But the hard evidence is scarce that all that hardware and software has actually contributed much to making organizations more profitable or better places in which to work.

Organizations are perhaps the most complex things ever created by humans, and invariably they are built and evolve in a haphazard manner. Thus, the ongoing saga of one management paradigm after another purporting to solve all of our problems. Likewise, the ongoing parade of IT silver bullets. Sure we endure, even succeed, but the waste is enormous. And IT's continuous cycles of buy, rework, and scrap, combined with absurd complexity and wretched quality, are a major component of all that squander. Consider that perhaps such inefficiency and carelessness are not altogether necessary in the information age.

What if we could engineer our systems and the organizations they serve the same way we engineer airplanes and buildings? Ever wonder why is it that 45-year old B-52s are still the backbone of the USA's strategic bomber force, or that 65-year old DC3s and 30-year old 747s still fly the world over, or that we can remodel and renovate buildings so that they provide service decade after decade, even century after century?

The answer is "architecture" – the design, engineering, and documentation of a complex artifact so that it fulfills its purpose and facilitates the coordinated activity of the various specialists required to create, maintain, and operate it. Applied to organizations, doing "architecture" is described by John Zachman, the creator of the state of the art organizing framework for enterprise architecture, a "semantic model" or "language" if you please, as the engineering and manufacturing of an enterprise that is aligned with the requirements of management, and is flexible, adaptable, interoperable, integrated, lean, and responsive to customers and other enterprise stakeholders.

I'm not 100% sure today just what "engineering and manufacturing an organization" totally means, any more than Eli Whitney in 1797 understood the full potential of standardized parts and division of labor in manufacturing, but I do know that it implies a profound a change in our thinking about organizations and the technologies IT professionals provide and manage for them. I also know that some of the best managed enterprises in the world are making the investment of time and resources to figure it out, and that the U.S. Federal government is funding the most concentrated effort in the creation of the ideas, techniques, and tools needed to make the promise of enterprise architecture and the information age enterprise a reality. Just like the Federal government provided the dollars for the research and development that led to the creation of the computer some 60 years ago.

The effort to invoke these disciplines was initiated by the U.S. Congress in 1996 through the passage of the Clinger-Cohen Act that requires, among other things, every Federal agency to have a CIO and to align IT with the business through enterprise architecture. A brilliant and forward thinking policy initiative, with commendable ongoing guidance for its implementation provided by OMB and GAO, but Clinger-Cohen was short-sighted in that it does not even consider the possibility or desirability of a government-wide enterprise architecture. The necessity of at least a basic Federal government-wide data architecture is becoming painfully clear to those charged with dealing with the world of today that requires the ever greater integration of information across Federal agencies for initiatives like e-government and homeland security (and sometimes data integration across levels of federal, state, local, and even foreign governments and the private sector). The lesson is simply that we cannot know all the details today for what tomorrow holds and there is an ever-increasing need for us all to be able to intelligently and proactively correct our course as we get new information and learn from our mistakes.

Conclusions

VA is massive in size, enormously complex, and highly decentralized. VA also has significant workforce development concerns, a long history of independent parts, and an organizational culture and structure that are not conducive to those parts working well together. VA has set the bar high for itself and by doing so can serve as the "poster child" and proving ground for the information age Federal government agency. But VA needs some things from Congress too, and I humbly offer you the following suggestions:

- Hold them accountable, but understand and honor their long-term vision: The long-term future is built upon short-term accomplishments. Please don't make the mistake of demanding short-term IT accomplishment without long-term relevance, because the result will be rework, scrap and replace. There is a need for incremental progress, but with balance. The long-term goals of One-VA and a One-VA enterprise architecture that they have set for themselves should not be sacrificed for short-term gain; although, sometimes a well planned and executed short-term compromise may be appropriate.

- Provide policy guidance and assistance: VA is entering new ground as they strive toward One-VA. The current organizational structure and budget authority of VA are not conducive to One-VA or enterprise architecture. Historically VA has optimized the parts and sub-optimized the whole. You are asking them through Clinger-Cohen, and they are asking themselves through One-VA, to shift the balance toward optimizing the whole through massive integration. They will need your patience, help, and guidance.

- Provide funding for this change: Resources are needed especially for the things that have never been done before in VA. I'm not talking about IT projects – They will stand or fall on their own merits. But there is a real need for additional funding for the VA central office IT organization and for the Office of the Chief Enterprise Architect, as well as for the establishment of a VA-wide Project Management Office. But VA is a socio-technical enterprise, made up of people and technologies, thus all of this will be for naught if there is not funding and acknowledgement of the significant effort in education, training, and organizational culture development that is required in order to realize One-VA. These are not IT issues, these are VA issues and they will require the active involvement of VA's business and IT personnel, as well as the assistance of change management professionals.

The two CIO conferences that were held since last October are indicative of the kind of change that is going on in VA. For the first time ever, the more than 200 professionals who are responsible for the various pieces of the VA IT pie came together to create a shared vision for a One-VA enterprise architecture and plans for achieving it. For the first time ever, they worked together face-to-face. For the first time ever, the parts all talked with each other and with the central office. For the first time ever, they listened to each other, and responded accordingly. And it's not just about plans for enterprise architecture, but also about cyber security, project management, network infrastructure, workforce development, performance measurement, and fulfilling VA's support to homeland security. It's not about business as usual either, but rather a profound change in the culture from one of dis-integration and fear, to one of collaboration, trust, and accountability. But even the vision and planning of 200 IT managers, no matter how senior, does not suddenly transform an enterprise with over 4,000 IT professionals, several hundred thousand other personnel, and tens of millions of customers. This is not a project. There is no silver bullet. This is a new way of life for VA, the change will happen incrementally, and we are all part of it. The question each must answer is "What part will I play in the creation of One-VA?"

If I can answer any of your questions or provide you with any additional information, I am always at your service.

Attachment: John Zachman's cover letter to Secretary Principi accompanying version 10.01 of VA's "Enterprise Architecture: Strategy, Governance, & Implementation":

Zachman International

Information Strategy and Architecture

2222 FOOTHILL BLVD. SUITE 337 • LA CAÑADA, CA 91011, USA • 1-818-244-3763 (PHONE AND FAX)

July 20, 2001

The Honorable Anthony J. Principi
Secretary, Department of Veterans Affairs
810 Vermont Avenue NW
Washington, D.C. 20420

Dear Secretary Principi:

I had the privilege of being present for the final two weekend working sessions that produced this historic milestone document, the Department of Veteran's Affairs (VA) Enterprise Architecture Strategy. I was impressed by your vision for the Department and your sense of urgency for addressing this vital issue. The Strategy has all of the attributes of a successful undertaking: Enterprise vision, business and information technology collaboration, and top management support. I was also impressed by the Department's realization that Enterprise Architecture is actually a business issue, not a technical issue. And I was extremely pleased that the 20 VA delegates to this Enterprise Architecture Innovation Team represented equal numbers of business executives and information technology executives.

The evidence of this complete business-technology collaboration was manifest in the Team's presentation to you during the final session ... with Laura Miller, *Assistant Deputy Under Secretary for Health* defining Enterprise Architecture and why it is so important, Guy McMichael, *Acting Assistant Secretary for Information Technology* discussing the long term political and business ramifications, and Ventris Gibson, *Deputy Assistant Secretary for Human Resources Management* describing the framework. I never thought I'd see the day!!

This document is insightful, coherent, comprehensive, and innovative --- a tribute to the clarity of vision and understanding that only can result from intense communication. I must also mention the gifted facilitation by a group of dedicated folks led by Professor Leon Kappelman that truly demonstrated the determination and perseverance of mountaineers on expedition. Finally, I was impressed with the stamina and commitment of the entire VA Enterprise Architecture Innovation Team. There was an intensity of participation. None were reticent to contribute. All were accepted and respected. From 7 AM in the morning 'till 12 Midnight, Thursday through Saturday weekend after weekend, the team remained focused on the "summit" of the Strategy.

I would like to take a moment now to talk about the road that lies ahead. The role of the Information Technology community in an Enterprise is not simply to build and run systems. This is what results in disintegration, "stovepipes." Rather the mission of the information folks in any Enterprise is *to engineer and manufacture the Enterprise such that it is aligned with the intent of General Management and is flexible, adaptable, interoperable, integrated, lean, etc. and responsive to the Enterprise's "customer" (as well as to other Enterprise "stakeholders").* I, in fact, suggest the name of "Information Systems" or "Information Technology" be changed to "Enterprise Engineering and Manufacturing" to set the correct perspective.

July 20, 2001 Page 2

The role of "Enterprise Engineering and Manufacturing" is to engineer and manufacture the Enterprise, and Enterprise Architecture is the essential engineering of the Enterprise before manufacturing it in order to deliver something coherent that Management needs, to minimize "scrap and rework" and to avoid "legacies." I believe that the *Long Term* Objectives of "Enterprise Engineering and Manufacturing" is to make every cell ("primitive model") of the Framework for Enterprise Architecture explicit, enterprise-wide, horizontally integrated across each row, vertically integrated down each column, at an excruciating level of detail in order to: constitute an inventory of reusable components from which the Enterprise can be "assembled-to-order," serve as a baseline for managing change (to the Enterprise), and provide the knowledge base for the Enterprise to which the external environment can be related and evaluated and from which management can derive their strategic advantage.

This is a new way of life. There is no quick fix. This is not a project. It is a "process." It is different from the Industrial Age past. It is the Information Age *present*! With that understanding, I would like to impart on you some advice that may help as you continue down your road to institutionalize the Department of Veterans Affairs Enterprise Architecture:

1. Do not underestimate the difficulty and complexity of engineering and manufacturing the most complex object yet conceived by humankind – the Enterprise. This will take time and determination.

2. This is a new way of life, a revolution in thinking, a discipline, an engineering process. Change of this magnitude takes time and perseverance. Do not get discouraged.

3. Things will have to be implemented periodically so you have to accept some risk of "scrap and rework," but build that risk and cost into the *short term* strategy. Set realistic expectations.

4. Make executive education and technical training a continuous process. Don't assume anything. It is easy to forget long-term issues in the short-term stress of daily life.

5. And remember, the state of the art is only fifty years old or so and the "playing field" still pretty level -- there is still much to learn and discover, and many opportunities to create advantage and value.

Finally, I would like to extend my congratulations to you and your blue ribbon Enterprise Architecture Innovation Team for having the vision, courage and commitment to begin this process to move this most valuable federal department, into a position to better serve our Nation's veterans and their families in the 21st century.

Thank you for inviting me to take part in this historic and notable undertaking. I wish you all the very, very best!!

John A. Zachman

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. EST
Wednesday,
March 13, 2002

VA INFORMATION TECHNOLOGY

Progress Made, but Continued Management Attention Is Key to Achieving Results

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

G A O
Accountability * Integrity * Reliability

Mr. Chairman and members of the subcommittee:

We are pleased to participate in today's continuing dialogue on the Department of Veterans Affairs' (VA) information technology (IT) program. IT is key to helping VA effectively serve our nation's veterans, and over the years, the department has expended substantial resources (more than $6 billion over the last 6 years) in support of its IT needs. As you know, however, VA has encountered persistent challenges in managing IT to produce results and improve performance.

When we testified before the subcommittee last April, a new secretary of veterans affairs had just been confirmed and an executive-level security officer had been hired.[1] To his credit, the secretary readily seized upon the seriousness of the issues that have been raised concerning VA's IT program, and committed to reforming how the department uses information technology. Since then, VA has also hired a department-level chief information officer (CIO) to lead its IT program. We view this executive leadership as a positive and significant step forward in the department's attempt to achieve better returns on its IT investments. However, VA's IT investment and management challenges are significant, and its ability to resolve them with the right combination of people, processes, and technology that are focused on achieving solid results will take sustained time, effort, and commitment.

At your request, we have been reviewing VA's continuing actions to address critical weaknesses in its overall IT program. Today, we will share with you the results of our work to date regarding VA's actions since last April to

- develop an enterprise architecture;
- improve information security;
- implement the Veterans Benefits Administration's veterans service network project that is intended to replace its existing compensation and pension payment system with a new system;
- extend the usage of, and standardize data collection for, the Veterans Health Administration's decision support system, being used to facilitate managers' and clinicians' analyses of patient care and cost of providing health care services; and
- implement jointly with the Department of Defense and Indian Health Service, the government computer-based patient record initiative,

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

which was intended to allow physicians and users to access data in each others' health information systems.

In doing this work, we analyzed relevant documentation and interviewed key agency officials to identify and assess VA's progress in implementing specific actions since April 2001 related to developing an enterprise architecture, improving information security, developing the Veterans Benefits Administration's veterans service network compensation and pension replacement system, extending usage of the Veterans Health Administration's decision support system, and advancing data sharing via the government computer-based patient record project. We performed our work in accordance with generally accepted government auditing standards, from June 2001 through March 2002.

Results in Brief

Over the past year, VA has clearly benefited from the commitment of the secretary and other top leaders to addressing critical weaknesses in the department's management of information technology. As a result of their leadership, VA has made important strides in raising corporate awareness of the department's needs and in articulating and acting upon a vision for achieving improvements in key areas of IT performance. Despite this progress, however, many aspects of VA's IT environment remain troublesome, and our message today reflects concerns that we have long viewed as significant impediments to the department's effective use of IT to achieve optimal agency performance. As such, VA has more work to accomplish before it can point to real improvement in overall program performance and be assured that it has a stable, reliable, and modernized systems environment to effectively support critical agency decisionmaking and operations.

In an area of growing importance, VA has taken key steps in laying the groundwork for an integrated, departmentwide enterprise architecture—a blueprint for evolving its information systems and developing new systems that optimize their mission value. Crucial executive support has been established and the department has put in place a strategy to define products and processes that are critical to its development. VA is also currently recruiting a chief architect to assist in implementing and managing the enterprise architecture. Significant work, nonetheless, is still required before the department will have a functioning enterprise architecture in place for acquiring and utilizing information systems across VA in a cost-effective and efficient manner. VA's success in developing, implementing, and using a complete and enforceable enterprise architecture hinges upon continued attention to putting in place a sound program management structure—including a permanent chief architect and an established program office—to facilitate, manage, and advance this effort and to be held accountable for its success. In addition, VA must continue to take steps to identify and collect crucial information describing essential business functions, information flows, strategic plans, and requirements, and produce a well-thought-out sequencing plan that considers management and organizational changes and business goals and operations. Success also hinges on having proactive management focused on ensuring that investment management and systems development and acquisition are closely linked with the enterprise architecture processes. This integration must be done in a manner that best suits the agency's particular organization, culture, and internal management practices.

Information security management is another area in which VA has taken important steps to strengthen its department-level program, including mandating information security performance standards and, thus, greater management accountability for senior executives. It has also updated security policies, procedures, and standards to guide the implementation of critical security measures. However, VA continues to report pervasive and serious information security weaknesses. Thus far, its actions toward establishing a comprehensive computer security management program have not been sufficient to ensure that the department can protect its computer systems, networks, and sensitive veterans health care and benefits data from unnecessary exposure to vulnerabilities and risks. Moreover, VA's current organizational structure does not ensure that the cyber security officer can effectively oversee and enforce compliance with security policies and procedures that are being implemented throughout the department.

Beyond these two key areas of IT management concern, VA and its administrations also have continued to pursue several critical information systems investments that have consumed substantial time and resources, with mixed success. For example, after about 16 years and at least $335 million spent on modernization, the Veterans Benefits Administration (VBA) is still far from a modernized system to replace its aging benefits delivery network, needed to more effectively support its compensation and pension and other vital benefits payment processes. VBA has not adequately addressed several longstanding concerns related to project management, requirements development, and testing—all of which raise uncertainty about whether the ongoing veterans service network (VETSNET) project will deliver a cost-effective solution with measurable and specific program-related benefits.

Conversely, the Veterans Health Administration's (VHA) managers and clinicians have made good progress in expanding their use of the decision support system (DSS) to facilitate clinical and financial decisionmaking. The use of DSS data for the fiscal year 2002 resource allocation process and a requirement that veteran integrated service network directors better account for their use of this system have both raised awareness of and promoted its utility among VHA facilities. Moreover, VHA has begun steps to further improve the accuracy and timeliness of DSS data. As VHA-wide usage of DSS progresses, sustained top management attention will be crucial to ensuring the continued success of this system.

Lastly, VA has achieved limited progress in its joint efforts with the Department of Defense and Indian Health Service to create an interface for sharing data in their health information systems, as part of the government computer-based patient record initiative. Strategies for implementing the project continue to be revised, its scope has been substantially narrowed, and it continues to operate without clear lines of authority or comprehensive, coordinated plans. Consequently, the future success of this project remains uncertain, raising questions as to whether it will ever fully achieve its original objective of allowing health care professionals to share clinical information via a comprehensive, lifelong medical record.

Promising Beginning, but VA Remains Far from Implementing an Enterprise Architecture

One of VA's most essential yet challenging undertakings has been developing and implementing an enterprise architecture to guide the department's IT efforts. An enterprise architecture—a blueprint for systematically and completely defining an organization's current (baseline) operational and technology environment and a roadmap toward the desired (target) state—is an essential tool for effectively and efficiently engineering business processes and for implementing their supporting systems and helping them evolve. Office of Management and Budget (OMB) guidelines[2] require VA and other federal agencies to develop and implement enterprise architectures to provide a framework for evolving or maintaining existing and planned IT. Guidance issued last year by the Federal CIO Council[3] 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.

As this subcommittee is well aware, VA has been attempting to develop an enterprise architecture for several years, but without much overall success. Our prior reports and testimony[4] have documented how VA's previous attempts have fallen short of their intended purpose and did not reflect an approach that would result in an integrated, departmentwide

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

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

[4] U.S. General Accounting Office, *VA Information Technology: Improvements Needed to Implement Legislative Reforms*, GAO/AIMD-98-154 (Washington, D.C., July 7, 1998); U.S. General Accounting Office, *Information Technology: Update on VA Actions to Implement Critical Reforms*, GAO/T-AIMD-00-74 (Washington, D.C., May 11, 2000); U.S. General Accounting Office, *VA Information Technology: Progress Continues Although Vulnerabilities Remain*, GAO/T-AIMD-00-321 (Washington, D.C., September 21, 2000); GAO-01-550T.

blueprint. For example, VA's earlier strategy had called for each of its administrations—VBA, VHA, and the National Cemetery Administration—to develop its own logical architecture, which likely would not have resulted in the department's having an integrated architecture, but rather, at least three separate, unrelated architectures. In addition, VA's common business lines had not been adequately involved in prior attempts to develop an architecture. In July 1998 and August 2000, respectively, we recommended that VA take actions to develop a detailed implementation plan with milestones for completing an integrated, departmentwide architecture, and that it include VA business owners in its architecture development. After assuming office last year, VA's secretary vowed to take action to address the inadequacies in the department's approach.

VA Has Taken Important Steps Toward Developing an Enterprise Architecture, But Much Work Remains

Over the past year, VA has made progress in taking specific actions to lay the groundwork for its enterprise architecture. Its most recent set of activities closely adhere to the Federal CIO Council's suggested guidance on managing the enterprise architecture program.

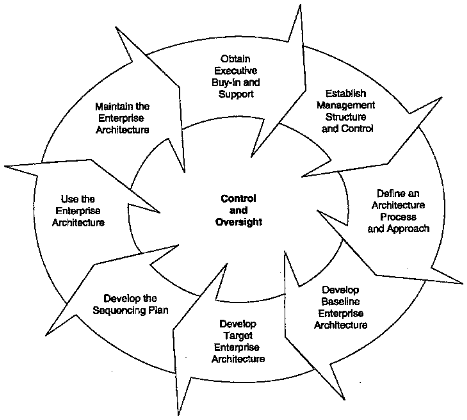
By effectively implementing an enterprise architecture, VA stands to realize a number of important and tangible benefits. For example, an enterprise architecture can

- capture facts about the department's mission, functions, and business foundation in an understandable manner to promote better planning and decisionmaking;
- improve communication among the department's business organizations and IT organizations through a standardized vocabulary; and
- provide architectural views that help communicate the complexity of VA's large systems and facilitate management of its extensive, complex environments.

Overall, effective implementation of an enterprise architecture can facilitate VA's IT management by serving to inform, guide, and constrain the 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 1, developing, implementing, and maintaining an enterprise architecture is a dynamic, iterative process of 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 requires sustained attention to process management and agency action over an extended period of time. Moreover, once implemented, the enterprise architecture requires regular upkeep and maintenance to ensure that it is kept current and accurate. Periodic reassessments are necessary to ensure that the enterprise architecture remains aligned with the department's strategic mission and priorities, changing business practices, funding profiles, and technology innovation.

Figure 1: The Enterprise Architecture Process


Obtain Executive Buy-in and Support
Establish Management Structure and Control
Define an Architecture Process and Approach
Develop Baseline Enterprise Architecture
Develop Target Enterprise Architecture
Develop the Sequencing Plan
Use the Enterprise Architecture
Maintain the Enterprise Architecture
Control and Oversight

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

A prerequisite to development of the enterprise architecture is sustained sponsorship and strong commitment achieved through buy-in of the agency head, leadership of the CIO, and early designation of a chief architect. Further, the establishment of an architectural team is necessary to define an agency-specific architectural approach and process. The cycle for completing an enterprise architecture highlights the need for constant monitoring and oversight of architectural activities and progress, and for architecture development teams to work closely with agency business line executives to produce a description of the agency's operations, a vision of the future, and an investment and technology strategy for accomplishing defined business goals. The architecture is maintained through continuous modification to reflect the agency's current baseline and target business practices, organizational goals, vision, technology, and infrastructure.

In initiating its enterprise architecture process, VA has applied key principles of the Federal CIO Council's guidance and has put in place some core elements of the council's enterprise architecture framework. For example, in the area of executive commitment, the department has obtained crucial buy-in and support from the secretary, department-level CIO, and other senior executives and business teams; this is essential to raising awareness of and leveraging participation in developing the architecture. As evidence of his commitment, last April the secretary established a team made up of VA senior management business line and information technology professionals to develop an enterprise architecture strategy. The team met on weekends over the course of about 60 days and, in August 2001, issued an executive enterprise architecture strategy that articulates the department's policy and principles governing the development, implementation, and maintenance of VA's enterprise architecture.

VA is in the process of establishing committees to manage, control, and monitor activities and progress in fully developing and implementing its enterprise architecture. For example, VA's information technology board has begun functioning as the department's enterprise architecture executive steering committee, with responsibility for directing, overseeing, and approving core elements and actions of the enterprise architecture program. As part of VA's actions to develop and advance its enterprise architecture, it has also chartered an enterprise architecture council—which when activated—is expected to assist in developing project priorities and performing management reviews and evaluations of IT project proposals. In addition, VA is in the process of establishing an enterprise architecture program management office and, over the last 8 months, has been recruiting a permanent chief architect to provide overall leadership and guidance for the enterprise architecture program. These management entities are essential for ensuring that the department's IT investments are aligned with the enterprise architecture and optimize the interdependencies and interrelationships among business operations and the underlying IT that supports them.

Further, as part of its enterprise architecture strategy, VA has chosen a highly recognized enterprise architecture framework that will be used to organize the structure of the architecture.[5] To facilitate its selection of a framework, VA consulted with experts from the private sector and

[5] 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.

borrowed lessons learned from officials involved in architecture development at other federal agencies.

VA has begun defining its current architecture, an important step for ensuring that future progress can be measured against such a baseline, and is also developing its future (target) telecommunications architecture. In addition, to assist in the management of new IT initiatives, VA is considering using a system that it has designed to link the management of its enterprise architecture program to the department's capital planning and project management. It is also considering using a Web-based tool that it has designed to collect data on business rules, requirements, and processes that will be integrated into the enterprise architecture management process.

While VA has taken several important steps forward, it is important to note that the department has many more critical work steps ahead in implementing and managing its enterprise architecture. Using the Federal CIO Council's enterprise architecture guide as a basis for analysis, table 1 illustrates some key steps that have been accomplished, along with examples of the many critical actions VA must still address to implement and sustain its enterprise architecture program. Accomplishing these remaining steps will require continued and substantial time, effort, and commitment.

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

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	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 control			
Establish technical review committee		VA's enterprise architecture council is expected to perform this function. Council has been chartered; first meeting expected March 2002	
Establish capital investment council		The capital investment review function is part of EA governance in VA's EA strategy The secretary has approved a proposal to integrate VA's EA, capital planning, investment, and project management functions	Define and set policies/procedures for new integrated process Publish the secretary's decision memorandum
Establish EA executive steering committee	✓		
Appoint chief architect		VA has an acting chief architect and is recruiting a permanent one	Hire a chief architect with requisite core competencies
Establish EA program management office		VA is in the process of establishing this office.	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)		VA plans to staff the positions of EA risk manager and configuration manager April/May 2002 VA's information technology board will perform QA	Ensure adequate staffing occurs and functions are performed Establish an independent, objective entity to perform QA
Establish enterprise architecture core team	✓		

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Develop EA marketing strategy and communications plan		VA has drafted an EA marketing plan	Finalize the marketing plan to include ongoing marketing and communications of VA's EA effort
Develop EA program management plan		VA is drafting the plan; its expected completion date is July 1, 2002	Finalize a plan that will delineate actions to develop, use, and maintain the EA, including management control and oversight
Initiate development of enterprise architecture		VA is developing baseline products, and establishing EA development and management practices.	Complete the EA program management plan to guide VA's EA efforts in developing processes and management practices, training participants, building baseline and target EA products, creating sequencing plan, and populating EA repository[b]
Define architecture process and approach			
Define intended use of architecture	✓		
Define scope of architecture	✓		
Determine depth of architecture	✓		
Select appropriate EA products			
Select products that represent business of enterprise	✓		
Select products that represent agency technical assets	✓		
Evaluate and select framework	✓		
Select EA toolset	✓		
Develop baseline enterprise architecture			
Collect information that describes existing enterprise		VA is validating its baseline application inventory; it is in the process of • developing detailed application profiles, • performing dynamic inventory modeling of baseline infrastructure, and • developing hardware and software profile information at server level	Complete baseline application inventory validation Complete detailed application profiles Complete baseline infrastructure inventory modeling Complete development of hardware and software profile information at server level Ensure that inventory includes all business functions and information flows, data models, external interface descriptions, and technical designs, specifications, and equipment inventories

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Generate products and populate EA repository			Create and populate the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models			Have subject matter experts assess the enterprise architecture products for accuracy and completeness
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		VA is collecting information and adding it to the Zachman framework to define the to-be architecture for telecommunications	Collect proposed business processes and information flows, strategic plans, modernization plans, and requirements documents; incorporate technology forecast, standards profile, and technical reference model
Generate products and populate EA repository			Create and populate the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models			Have subject matter experts assess the enterprise architecture products for accuracy and completeness
Develop sequencing plan			Address all detailed activities in this step
Identify gaps			
Define and differentiate legacy, migration, and new systems			
Plan migration			
Approve, publish, and disseminate EA products			
Use enterprise architecture			Address all detailed activities in this step
Integrate EA with capital planning and investment control and systems life cycle processes			
Train personnel			
Establish enforcement processes and procedures			
Define compliance criteria and consequences			
Set up integrated reviews			
Execute integrated process			
Initiate new and follow-up projects			
Prepare proposal			
Align project to EA			
Make investment decision			

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Execute projects			
Manage and perform project development			
Evolve EA with program/project			
Assess progress			
Complete project			
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.

Among the key activities requiring immediate attention is establishment of a program management office headed by a permanent chief architect to manage the development and maintenance of the enterprise architecture. VA has begun establishing such an office and is currently recruiting a chief architect. However, until the department has an office that is fully staffed with experienced architects and hires a chief architect with the requisite core competencies, it will continue to lack the management and oversight necessary to ensure the success of its enterprise architecture program. Further, until the department has completed an implementation plan that delineates how it will develop, use, and maintain the enterprise architecture, it will lack definitive guidance for effectively managing the enterprise architecture program.

Further, a lot of work lies ahead related to VA's efforts toward developing its baseline and target architectures. A crucial first step in building the enterprise architecture is identifying and collecting existing products that describe the agency as it exists today and as it is intended to look and operate in the future. While VA has developed a baseline application inventory to describe its "as is" state, it has not yet completed validating the inventory, or completed detailed application profiles for the inventory, including essential information such as business functions, information flows, and external interface descriptions. Similarly, to define its vision of future business operations and supporting technology, VA must still collect crucial information for its target architecture, including information on its proposed business processes, strategic plans, and requirements.

Beyond these planning and development activities, VA will also have to ensure the successful transition and implementation of its enterprise architecture. Evolving the agency from its baseline to the target architecture will require concurrent, interdependent activities and incremental development. As such, VA will need to develop and maintain a sequencing plan to provide a step-by-step approach for moving from the baseline to the target architecture. Development of this sequencing plan should consider a variety of factors, including sustaining of operations during the transition, anticipated management and organizational changes, and business goals and operational priorities. Ultimately, VA's success in using the architecture will depend on active management and receptive project personnel, along with effective integration of the enterprise architecture process with other enterprise life cycle processes.

A key aspect of VA's enterprise architecture program is the integration of security practices into the enterprise architecture. The CIO Council has articulated guidelines for doing so.[6] For example, the architecture policy should include security practices and the architecture team should include security experts. In its enterprise architecture strategy document, VA has committed to including security in all elements of its enterprise architecture. Further, VA's executive-level security officer served as a member of its architecture team. As VA moves forward in developing, implementing, and using its enterprise architecture, we would expect it to include information security details relating to the design, operations, encryption, vulnerability, access, and use of authentication processes. A commitment to building information security into all elements of its enterprise architecture program is essential to helping VA meet the challenges that it faces in protecting its information systems and sensitive data.

As VA moves forward with its enterprise architecture management program, it should ensure that remaining critical process steps outlined in the federal CIO guidance are sufficiently addressed and completed within reasonable timeframes. With the enhanced management capabilities

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

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 Challenges Continue to Require Top Management Attention

Information security continues to be among the top challenges that the department must contend with. As you know, in carrying out its mission, VA relies on a vast array of computer systems and telecommunications networks to support its operations and store the sensitive information that it collects related to veterans' health care and benefits. VA's networks are highly interconnected, its systems support many users, and the department is increasingly moving to more interactive, Web-based services to better meet the needs of veterans. Effectively securing these computer systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive veterans' health and disability benefits information, and ensure the reliability of its financial data.

Mr. Chairman, when we last testified, VA had just established a department-level information security management program and hired an executive-level official to head it.[7] VA had also finalized an information security management plan to provide a framework for addressing longstanding departmentwide computer security weaknesses. However, as our testimony noted, the department had not implemented key components of a comprehensive, integrated security management program that are essential to managing risks to business operations that rely on its automated and highly interconnected systems. This condition existed despite our previous recommendation that VA effectively implement and oversee its computer security management program through assessing risks, implementing policies and controls, promoting awareness, and evaluating the effectiveness of information system controls at its facilities.[8] As with its enterprise architecture, the Secretary expressed his intent to implement measures that would remedy existing deficiencies in the department's security program.

The effects of not having a fully integrated computer security management program in place remain evident. Since the subcommittee's hearing on this topic last April, VA and its Office of Inspector General have continued to report pervasive computer security challenges. VA's September 2001 report on compliance with recently enacted government information

[7] GAO-01-550T.

[8] U.S. General Accounting Office, *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration*, GAO/AIMD-00-232 (Washington, D.C.: September 8, 2000).

security reform legislation[9] revealed that the department had not implemented effective information security controls for many of its systems and major applications. Last October, VA's inspector general also reported that it had found significant problems related to the department's control and oversight of access to its systems, including that VA had (1) not adequately limited the access of authorized users or effectively managed user identifications and passwords, (2) not established effective controls to prevent individuals from gaining unauthorized access to its systems, (3) not provided adequate physical security to its computer facilities, and (4) not updated and tested disaster recovery plans to ensure continuity of operations in the event of a disruption in service.

Many of these access and other general control weaknesses mirror deficiencies we have reported since 1998, and that VA's inspector general continues to report as a material weakness in the department's internal controls.[10] Based largely on weaknesses of this type, last fall the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations gave VA a failing grade in computer security.[11]

Progress Being Made, But Important Elements of a Comprehensive Computer Security Management Program Still Lacking

VA's senior leadership has shown greater awareness of and concern for the severity of the department's computer security problems, and since last April has taken steps aimed at strengthening VA's overall security posture. Specifically, to provide greater management accountability for information security, the secretary has mandated information security performance standards for members of the department's senior executive service. In addition, VA's cyber security officer—the department's senior security official—has organized his office to focus more directly on the

[9] 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.

[10] Department of Veterans Affairs Office of Inspector General, *Report of the Audit of the Department of Veterans Affairs Consolidated Financial Statements for Fiscal Years 2001 and 2002* (Washington, D.C., February 27, 2002).

[11] House Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, *Computer Security: How Is the Government Doing?* 107th Cong., 1st sess., 9 November 2001.

critical elements of information systems control that are defined in our information system controls audit methodology.[12] Further, the department has adopted the National Institute of Standards and Technology's federal information technology security assessment framework to use in determining the current status of these controls and measuring the progress of information security program improvements.

The cyber security officer also recently revised the department's security management plan to update security policies, procedures, and technical standards. The updated plan outlines 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 places increased emphasis on centralizing key security functions that previously were decentralized or nonexistent, including virus detection, systems certification and accreditation, network management, configuration management, and incident and audit analysis.

Yet even with this positive direction, VA's actions do not fully address remaining problems, and are inadequate to cover the breadth of matters essential to a comprehensive security management program. Our 1998 report on effective security management practices used by several leading public and private organizations[13] and a companion report on risk-based security approaches in 1999[14] identified key principles that can be used to establish a management framework for more effective information security programs. This framework is depicted in figure 2. The leading organizations we examined applied these principles to ensure that information security addressed risks on an ongoing basis. Further, these have been cited as useful guidelines for agencies by the Federal CIO Council and incorporated into the council's information security assessment framework,[15] intended for agency self-assessments.

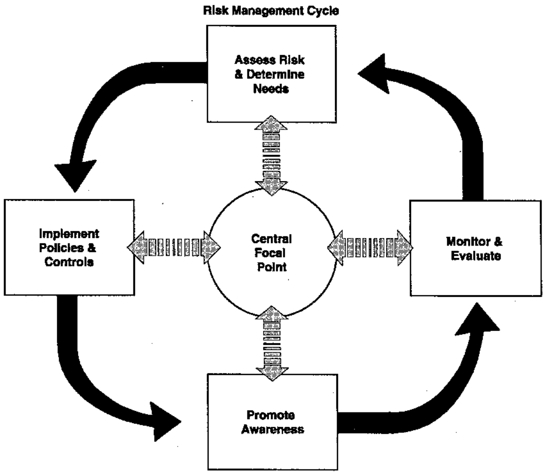
[12] U.S. General Accounting Office, *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6 (Washington, D.C., January 1999).

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

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

[15] Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C., November 28, 2000).

Figure 2: Information Security Risk Management Framework



Source: GAO/AIMD-98-68.

Using our information security risk management framework as criteria, table 2 summarizes both the actions that VA has taken and those still needed to ensure that it has a comprehensive computer security management program. As shown, while VA has completed a number of important steps, its efforts in each of the 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—have not yet included key actions that are essential for successful and effective program implementation.

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

Important elements of a computer security management program[c]	Actions VA has taken	Actions still needed
Central security management function to guide and oversee compliance with established policies and procedures and review effectiveness of the security environment	Established a department-level information security officer Began requiring full-time security officers or staff with primary duty for security at all facilities Established a CIO subcommittee to improve departmentwide coordination on security issues	Ensure full-time security officers or staff with primary duty for security are assigned to information security officer positions, and clearly define their roles and responsibilities Develop guidance to ensure authority and independence for security officers Develop policies and procedures to ensure 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	Updating department security policy and guidance Developed technical security standards for some network platforms	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
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	Developed abbreviated risk methodology as part of the Government Information Security Reform Act process Established policy requiring risk to be assessed when significant changes are made to computer systems	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

Important elements of a computer security management program[c]	Actions VA has taken	Actions still needed
Security awareness to educate users about current information security risks, policies, and procedures	Implemented a departmentwide security awareness program	Establish a process to ensure program compliance
Monitoring and evaluating computer controls to ensure their effectiveness, improve them, and oversee compliance	Issued contract for independent compliance reviews of ongoing initiatives related to security controls Performed penetration testing of its Web sites from the Internet Implemented computer virus-detection software departmentwide Began developing an inventory of security weaknesses Established a process for reporting computer security incidents and piloted intrusion-detection systems at selected locations Developed a certification and accreditation framework for its general support and major applications	Develop specific requirements for conducting 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 Establish a process for tracking the status of security weaknesses, corrective actions taken, and independent validation of the corrective actions Develop a process for 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

[c] U.S. General Accounting Office, *Executive Guide: Information Security Management,* GAO/AIMD-98-68 (Washington, D.C.: April 7, 1998).

Source: GAO analysis.

As the table illustrates, VA's security management program continues to lack essential elements required to protect the department's computer systems and networks from unnecessary exposure to vulnerabilities and risks. For example, while VA has begun to develop an inventory of known security weaknesses, it continues to be without a comprehensive, centrally managed process that will enable it to identify, track, and analyze all computer security weaknesses. Further, the updated security management plan does not articulate critical actions that VA will need to take to correct specific control weaknesses or the time frames for completing key actions. While the plan calls for monitoring VA's computer control environment to ensure compliance, the plan does not provide a framework to guide the monitoring activities by, for example, identifying the specific security areas to be reviewed, the scope of compliance work to be performed, the frequency of reviews, reporting requirements, or the resolution of reported issues.

VA also lacks a mechanism for collecting and tracking performance data, ensuring management action as needed and, when appropriate, providing independent validation of program deliverables. Without these essential elements, VA will have only limited assurance that its financial information and sensitive medical records are adequately protected from unauthorized disclosure, misuse, or destruction. Accordingly, as VA continues to improve upon its information security management, it should move expeditiously to address the gaps we are highlighting in table 2.

In commenting on the department's current security posture, VA's cyber security officer stated that efforts are planned or underway to address the actions not yet completed. He added that by August 31, 2002, the department expects to have a plan for completing all of the necessary corrective actions.

Overarching Organizational and Management Issues Could Hinder VA's Ability to Fully Address Information Security Challenges

While VA is clearly placing greater emphasis on its information security, its cyber security officer will be challenged to manage the security function on a departmentwide basis. As the department is currently organized, more than 600 information security officers in VA's three administrations and its many medical facilities throughout the country[16] are responsible for ensuring that appropriate security measures are in place. These information security officers report to their facility's director or the chief information officer for their administration. However, there is neither direct nor indirect reporting to VA's cyber security officer, thus raising questions about this official's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. Further, because VA's information security budget relies on funding by its component administrations, the cyber security officer lacks control and accountability over a significant portion of the financial resources that the security program depends on to sustain its operations.[17]

Successfully managing information security under this organizational structure, therefore, will in large part depend on the extent to which VA's business managers assume responsibility for implementing the appropriate policies and controls to mitigate risks, and work collaboratively and cooperatively with the cyber-security officer. Consequently, it will be essential for VA to hold its senior managers accountable for information security at their respective facilities and administrations. VA has taken a critical step toward achieving this by establishing security performance standards for its senior executives. These standards must be effectively applied and enforced, however, to ensure a successful outcome.

[16] VHA provides medical care at 163 hospitals, more than 800 community and facility-based clinics, 135 nursing homes, 43 domiciliaries, 206 readjustment counseling centers, and various other facilities.

[17] For example, to help support its fiscal year 2002 security program budget request of about $55 million, VA expects to receive about $22 million in funding from VHA and $12 million from the department's other administrations and offices.

Progress on the Compensation and Pension Replacement System Is Disappointing

The VETSNET compensation and pension replacement effort grew out of an initiative that VBA undertook in 1986 to replace its outdated benefits delivery network (BDN) and modernize its compensation and pension, education, and vocational rehabilitation benefits payment systems. VBA had expected these modernized systems to provide a rich source for answering questions about veterans' benefits and enable faster processing of benefits. In 1996, after experiencing numerous false starts and spending approximately $300 million on the overall modernization, VBA revised its strategy and began focusing on modernizing the compensation and pension (C&P) payment system. At that time, VBA estimated that the C&P replacement project would cost $8 million and be completed in May 1998.

Since its inception, however, VBA has been plagued with problems in carrying out the C&P replacement initiative. As detailed in the attachment, our various publications since 1996 have highlighted consistent and longstanding concerns in several areas, including project management, requirements development, and testing. Our testimony last April noted that VBA had made some progress in developing and testing software products that would become part of the system. Nevertheless, we also noted that VBA had not addressed several important issues that were key to its successful implementation, including the need to develop an integrated project plan and schedule incorporating all of the critical areas of this system development effort.[18] As our prior work has pointed out, a significant factor contributing to VBA's continuing problems in developing and implementing the system has been the level of its capability to develop and maintain high-quality software on any major project within existing cost and schedule constraints—a condition that we identified during our 1996 assessment of the department's software development capability.[19]

Critical Actions Have Not Been Taken to Ensure Successful Implementation of the C&P Replacement System

After 6 years of work—4 years beyond what its initial estimate called for—VBA has spent at least $35 million, without much demonstrable progress toward implementing the replacement system. Since last April, it has not made substantial progress in addressing the concerns raised by our earlier work. Although, last year, VBA indicated that it had implemented its rating board automation tool and had completed developing and testing its four other software products,[20] the administration stated during our recent review that two of the software products that will support its award processing and finance and accounting systems still need further

[18] GAO-01-550T.

[19] U.S. General Accounting Office, *Software Capability Evaluation: VA's Software Development Process Is Immature,* GAO/AIMD-96-90 (Washington, D.C.: June 19, 1996).

[20] The current C&P replacement strategy incorporates five software products: Search and Participant Profile, Rating Board Automation 2000, Modern Award Processing-Development, Award Processing, and Finance and Accounting System. The first product deployed in November 2000—Rating Board Automation 2000—was to assist veterans service representatives in rating benefits claims.

development. Moreover, VBA has not increased the number of payments using these new software products beyond the 10 original claims that it had pilot tested in February 2001. In addition, it continues to lack an integrated project plan and schedule that incorporate all of the critical areas of this system development activity. Further, VBA still has not obtained essential support from the field office staff that will be required to use the new software, and requirements for the new software have not yet been validated. These deficiencies are significant, given that the software application that VBA developed to assist veterans service representatives in rating benefits claims (Rating Board Automation 2000) did not meet users' needs and achieved less timely claims processing results.

At this time, VBA also is without a project manager to oversee the project. Progress made early in 2000 toward creating a project control board to manage the C&P replacement was curtailed when the project manager departed last April. Until VBA provides appropriate management and oversight for all aspects of the project's development and implementation, it will not be positioned to ensure that this project will deliver a cost-effective solution with measurable and specific program-related benefits.

Further, the schedule for implementing the replacement system continues to undergo change, resulting in additional delays. Last April, VBA had planned to deploy VETSNET in all of its 58 regional offices in July 2002. However, VBA officials have since modified the deployment time frame twice, with its latest proposal being to deploy each of the five applications separately over 2 years, beginning in June 2003. VBA management has not yet approved this latest strategy.

Studies Highlight the Need for Additional Testing and Information to Support Continued Systems Development

Last year, the secretary expressed concerns about the VETSNET project and called for an independent audit of the C&P replacement system to facilitate his decision on whether to continue the initiative. Accordingly, a contractor was hired in May 2001 to assess (1) whether the system architecture will be capable of supporting VBA's projected future workload, and (2) whether the system being developed will meet future functional, performance, and security needs. The contractor reported last September that the system architecture would be able to process VBA's projected future workload.

However, the contractor neither assessed nor reported on whether the system will meet future functional business needs, and the scope of its review did not generate sufficient information to fully evaluate and make an informed decision on whether the project should proceed. The review focused primarily on the system's ability to perform efficiently under a heavy workload, and did not include user acceptance or the functional testing that is needed to ensure that the system can fully satisfy user requirements and that deployed software can be used without significant errors. Further, the review did not fully address the security requirements for the new system. VA's department-level CIO agreed that the scope of the contractor's review had been limited to a technical review of whether VETSNET could handle the anticipated workload. He also acknowledged the need for functional testing and an integrated project plan.

Similar concerns about VBA's strategy for the C&P replacement project were also documented in an October 2001 report issued by the VA claims processing task force.[21] In its report, the task force emphasized that limited user and functional testing posed a major problem for VBA in developing and implementing its systems. The task force highlighted material deficiencies in VBA's strategic planning and its implementation and deployment of new and enhanced information technology products and initiatives, as had been pointed out in an earlier report. Further, the task force questioned whether VETSNET represented a viable long-term solution, in part because it does not provide support for a redesigned and integrated claims process across VA's administrations and offices.

In commenting on these reports' findings, VBA's CIO stated that, by the end of March 2002, her office anticipated completing a remediation plan that will address the most critical concerns identified in the contractor's review. She stated that the office is in the process of developing a statement of work to obtain contractor support to develop additional functional testing capability. The statement of work is scheduled for completion in June 2002. In addition, the CIO is negotiating with relevant VBA business groups to secure subject matter experts to validate business requirements and assist with the functional testing.

VETSNET Deployment Delays Affect the Benefits Delivery Network

If not promptly addressed, the problems and delays that have been noted in implementing the VETSNET project could have critical cost implications for the department and service delivery inefficiencies for the veteran community. In particular, without a replacement system, VA must continue to rely on the aging BDN to deliver its benefit payments, parts of which were developed in the 1960s. Although the BDN was enhanced to address year 2000 conversion issues, because of its anticipated replacement, VBA has since made only limited investments in maintaining it.

[21] The claims processing task force was formed in May 2001, when the secretary of veterans affairs asked a group of individuals with significant VA 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 veteran claims for disability compensation and pension.

Without additional maintenance, it is uncertain that the BDN will be able to continue accurately processing the many benefits payments that VBA must make.[22] In its report, the claims processing task force warned that the system's operations and support were approaching a critical stage, with the potential for performance to degrade and eventually cease. The task force recommended that the BDN be sustained and upgraded to ensure that payments to veterans would remain prompt and uninterrupted until VBA is able to field a replacement system. VBA officials have stated that they are working on a plan to address this issue. This plan is expected to include purchasing an additional mainframe computer to help extend the system's operation until 2007—the date by which new systems are planned to be operational for all three benefits payment business lines.

As you can see, Mr. Chairman, despite many years of work, VBA still has a number of fundamental tasks to accomplish before it can successfully complete development and implementation of the VETSNET project. Before proceeding with this project, VBA must assess and validate users' requirements for the new system to ensure that business needs are met. It also needs to complete testing of the system's functional business capability, as well as end-to-end testing to ensure payments are made accurately. Finally, it must establish an integrated project plan to guide its transition from the old to the new system. Until VBA performs a complete analysis of the initiative, as the secretary has indicated he would do, it is questionable whether additional resources should be expended on continued systems development activities.

VHA Continues to Expand Its Use of DSS

Unlike VBA's work on VETSNET, VHA continues to make progress in expanding overall use of its decision support system (DSS). As you know, DSS is an executive information system designed to provide VHA managers and clinicians with data on patterns of patient care and patient health outcomes, as well as the capability to analyze resource utilization and the cost of providing health care services. VHA completed its implementation of DSS in October 1998. However, in September 2000, we testified that DSS had not been fully utilized since its implementation, and noted that DSS was not being used for all the purposes intended.[23]

Last April, we testified that VHA had shown moderate progress in increasing usage of DSS among its veterans integrated service networks (VISN) and medical centers, and encouraged VA to continue providing top management support to ensure that the system is fully utilized and that financial and clinical benefits are realized. Our testimony noted several

[22] The current C&P payment system alone processes about 3.2 million payments each month. Altogether, the three benefits payment business lines process about 3.5 million payments monthly.

[23] GAO/T-AIMD-00-321.

efforts that VHA had undertaken to encourage greater use of DSS, including using DSS data to support the fiscal year 2002 resource allocation process and as a consideration in preparing VISN directors' year-end performance appraisals, requiring VISN directors to provide examples of their reports and processes that rely on DSS data, and ensuring that medical centers' processing of DSS data is current (no more than 60 days old).[24]

VHA's initiatives to encourage greater use of DSS have yielded results. The use of DSS data in the fiscal year 2002 allocation process has clearly raised VHA's awareness about the importance of this information. VHA's most recent DSS processing report, dated January 31, 2002, revealed that all 22 VISNs had completed processing fiscal year 2001 DSS data and that seven VISNs had begun processing fiscal year 2002 data. Further, every VISN has provided both clinical and financial examples of DSS usage, and this information is now being considered in the quarterly reviews of the VISN directors' performance. As a result, VHA's managers have grown more knowledgeable about and have begun to make more informed decisions regarding the cost of care being provided by their facilities.

Initiatives Are Being Taken to Improve the Accuracy, Timeliness, and Availability of DSS Data

VHA continues to explore other initiatives to improve the accuracy and completeness of DSS data. In response to a report issued by VA's inspector general in March 1999,[25] regarding the failure of some medical facilities to follow the DSS basic structure for capturing workload data and associated costs, VHA has taken several actions, including

- implementing a VHA decision support system standardization directive that requires annual standardization audits and the reporting of consecutive repeat occurrences of non-compliance to the assistant deputy under secretary for health;
- developing an audit tool for use in determining a facility's compliance with the DSS basic model for capturing workload data and associated costs; and
- performing a standardization audit in September 2001 to assess the extent to which each facility's DSS departments and products complied with national standards.[26]

[24] GAO-01-550T.

[25] Department of Veterans Affairs, Office of Inspector General, *Audit of Veterans Health Administration Decision Support System Standardization*, Report No. 9R4-A19-075 (Washington, D.C., March 31, 1999).

[26] The standardization audit revealed a 99.6 percent compliance rate with the National Department List, a 98.8 percent compliance rate with the National Product List, and a 99.5 percent match between facilities' cost centers and DSS departments.

Further, in response to managers' concerns that DSS data are not timely and easy to access, the DSS program office initiated several actions. These include establishing a working group last July to identify best practices and recommend actions for improving processing efficiency and the timeliness and availability of DSS data. To date, the working group has provided all DSS sites with an updated monthly guide detailing each step of the process, and has distributed a pharmacy rejects database and a step-by-step guide for processing these rejects. These products should help increase the efficiency of the monthly processing and facilitate more accurate and timely data. In addition, the program office has authorized two sites to pilot test an application aimed at providing the end user or manager with a user-friendly front end to display DSS information and allow patient inquiry.

In addition, several VISNs have independently begun exploring options for providing easier access to DSS data. For example, one is examining the feasibility of establishing a data warehouse where data extracted from DSS can be transformed into a format that will facilitate queries and reports that are simple to create and quick to run.[27] Another has begun building a data repository for use in creating an application to compile and deliver data requested by managers or clinicians.[28]

Even with these accomplishments, however, top management involvement and continued support will be critical to ensuring that VHA continues to make progress in improving the operational efficiency and effectiveness of DSS, and that it realizes the full clinical and financial benefits of this system. In March 2001, oversight for the DSS program was transferred from VHA's chief information officer to its chief financial officer. Since that time, VHA has also assigned three different acting directors to lead the program. However, VHA has not yet selected a permanent director to provide consistent management and oversight. In addition, of 56 personnel positions allotted to the DSS program office, 19 positions had not been filled at the end of January 2002. Without a permanent director to lead the DSS program or full staffing to support the system's operation, VHA runs the risk that continued increases in usage of DSS, along with its associated benefits, could be imperiled.

[27] Veterans integrated service network 16 (Jackson, Mississippi).

[28] Veterans integrated service network 13 (Minneapolis, Minnesota)

The Government Computer-based Patient Record Initiative Is Moving Away From Its Original Goal

Mr. Chairman, you also asked us to update you 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) project. Having readily accessible data to facilitate services to our nations' military personnel and others has proved particularly significant in light of recent terrorist actions and the associated responses that have been required.

The GCPR project developed out of VA and DOD discussions about ways to share data in their health information systems and from efforts to create electronic records for active duty personnel and veterans. As you know, the patients served by VA's and DOD's systems tend to be highly mobile, and consequently, their health records may be at multiple federal and nonfederal medical facilities, both in and outside of the United States. In November 1997, the president called for the two departments to develop a "comprehensive, life-long medical record for each service member," and in August 1998—8 months after the GCPR project was officially established—issued a directive requiring VA and DOD to develop a "computer-based patient record system that will accurately and efficiently exchange information."[29] IHS later became involved because of its expertise in population-based research and its longstanding relationship with VA in caring for the Indian veteran population.

As originally envisioned, GCPR was not intended to be a separate computerized health information system, nor was it meant to replace VA's, DOD's, and IHS's existing systems. Rather, it was intended to allow physicians and other authorized users at these agencies' 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.

In April 2001, we reported that expanding time frames and cost estimates, as well as inadequate accountability and poor planning, tracking and oversight, had raised doubts about GCPR's ability to provide the benefits expected.[30] In particular, we noted that the project's time frames had significantly expanded and that its costs had continued to increase. In

[29] National Science and Technology Council, *A National Obligation: Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families After Future Deployments,* Presidential Review Directive 5 (Washington, D.C., Executive Office of the President, Office of Science and Technology Policy, August 1998).

[30] 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., April 30, 2001).

addition, basic principles of sound IT project planning, development, and oversight had not been followed, creating barriers to progress. For example, clear goals and objectives had not been set; detailed plans for developing, testing, and implementing the new software had not been established; and critical decisions regarding goals, costs, and time frames were not binding on all parties. Further, data exchange and privacy and security issues critical to the project's success remained to be addressed.

As a result of these concerns, we recommended that the three agencies (1) designate a lead entity with final decisionmaking 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. In commenting on the report, VA, DOD, and IHS all concurred with our findings and recommendations.

Nonetheless, progress on the GCPR initiative continues to be disappointing. The scope of the project increasingly has been narrowed from its original objectives and it continues to proceed without a comprehensive strategy. For example, in responding to our report, VA, DOD, and IHS provided information on a new, near-term strategy for GCPR. However, this revised strategy is 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 phase of the revised strategy calls only for a one-way transfer of data from DOD's current health care information system to a separate database that VA hospitals can access. While even this degree of data sharing is a positive development, VA's clinicians, nonetheless, will only be allowed to read, but not perform any calculations on the data received. VA and DOD officials had initially planned to implement this near-term capability in November 2001, but recently stated that they now expect to do so by this July 2002. Further, the officials stated that they plan to change the name of the project to the Federal Health Information Exchange.

Subsequent phases of the effort that were to further expand GCPR's capabilities have also been revised. A second phase that would have enabled information exchange among all three agencies—VA, DOD, and IHS—is now expected to enable only a bilateral read-only exchange of data between VA and IHS.

Further, according to VA officials, plans for a third phase, which was to expand GCPR's capabilities to public and private national health information standards groups, are no longer being considered for the project. Instead, the third phase is now expected to focus only on expanding the data exchange between VA and IHS and allowing limited data calculations and some translation of terminology between the two agencies. Under the revised strategy, there are no plans for DOD to receive data from VA.

In addition, concerns expressed in our April 2001 report still need to be addressed. For example, the GCPR project continues to operate without clear lines of authority or a lead entity responsible for final decisionmaking. Last August, the VHA CIO informed us that a draft memorandum of agreement, designating VHA as the lead entity, was being considered within VA, DOD, and IHS. However, this memorandum had not been approved or implemented at the time that we concluded our review. The project also continues to move forward without comprehensive and coordinated plans, including an agreed-upon mission and clear goals, objectives, and performance measures. Without clearly defined lines of authority and a comprehensive and coordinated strategy, even the revised GCPR initiative is destined to continue on an uncertain course—one that is unlikely to deliver substantial results.

* * * * *

In summary, VA has made good progress toward addressing a number of important information technology concerns, but it still has much work to do. Its current leadership is to be commended for the dedication that it has demonstrated regarding VA's information technology problems. However, in totality, the steps taken to date have not been sufficient to overcome the wide range of deficiencies that threaten VA's operational effectiveness. Many of VA's problems are longstanding and pervasive, and can be attributed to fundamental weaknesses in management accountability—some of which can only be overcome through serious restructuring of current reporting relationships and lines of authority. Until VA makes a concerted effort to ensure that all necessary processes and controls exist to guide the management of its information technology program, it will continue to 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) 512-6257 or by e-mail at mcclured@gao.gov. Individuals making key contributions to this testimony included Nabajyoti Barkakati, Amanda C. Gill, David W. Irvin, Tonia L. Johnson, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, Rosanna Villa, and Charles M. Vrabel.

GAO Products Highlighting Concerns with VETSNET C&P Replacement

Issuance date Report/testimony	Summary of report findings and conclusions
April 4, 2001 GAO-01-550T	The project's viability was still a concern. It continued to lack an integrated project plan and schedule addressing all critical systems development areas, to be used as a means of determining what needs to be done and when. A pilot test of 10 original claims that did not require significant development work may not have been sufficient to demonstrate that the product was capable of working as intended in an organizationwide operational setting.
September 21, 2000 GAO/T-AIMD-00-321	VBA's software development capability remained ad hoc and chaotic. The VETSNET implementation approach lacked key elements, including a strategy for data conversion and an integrated project plan and schedule incorporating all critical systems development areas. Further, data exchange issues had not been fully addressed.
May 11, 2000 GAO/T-AIMD-00-74	$11 million had reportedly been spent on VETSNET C&P; both the May 1998 completion date and revised completion date of December 1998 were not met. Contributing factors included lack of an integrated architecture defining the business processes, information flows and relationships, business requirements, and data descriptions, and VBA's immature software development capability.
September 15, 1997 GAO/AIMD-97-154	VBA's software development capability remained ad hoc and chaotic, subjecting the agency to continuing risk of cost overruns, poor quality software, and schedule delays in software development.
May 30, 1997 GAO/AIMD-97-79	VETSNET experienced schedule delays and missed deadlines because (1) it employed a new software development language not previously used by the development team, one that was inconsistent with the agency's other systems development efforts; (2) the department's software development capability was immature and it had lost critical systems control and quality assurance personnel, and (3) VBA lacked a complete systems architecture; for example, neither a security architecture nor performance characteristics had been defined for the project.
June 19, 1996 GAO/T-AIMD-96-103	VETSNET had inherent risks in that (1) it did not follow sound systems development practices, such as validation and verification of systems requirements; (2) it employed a new systems development methodology and software development language not previously used; and (3) VBA did not develop the cost-benefit information necessary to track progress or assess return on investment (for example, total software to be developed and cost estimates).
June 19, 1996 GAO/AIMD-96-90	VBA's software development capability was immature and it could not reliably develop and maintain high-quality software on any major project within existing cost and schedule constraints, placing its software development projects at significant risk. VBA showed significant weaknesses in requirements management, software project planning, and software subcontract management, with no identifiable strengths.

(310419)

United States General Accounting Office

GAO

Report to Congressional Committees

April 2001

COMPUTER-BASED PATIENT RECORDS

Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing

GAO

Accountability * Integrity * Reliability

GAO-01-459

Contents

Abbreviations

CIO	Chief Information Officer
CPRS	Computer Patient Record System
DOD	Department of Defense
GCPR	Government Computer-Based Patient Record
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IHS	Indian Health Service
IT	information technology
MHS	Military Health System
MOA	memorandum of agreement
PACMEDNET	Pacific Medical Network
PDTS	Pharmacy Data Transaction System
TMIP	Theater Medical Information Program
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VISN	Veterans' Integrated Service Network
VISTA	Veterans Health Information Systems and Technology Architecture

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

April 30, 2001

The Honorable John Warner
Chairman
The Honorable Carl Levin
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Bob Stump
Chairman
The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

The Department of Veterans Affairs (VA) and the Department of Defense (DOD) combined provide health care services to approximately 12 million veterans, military personnel, and dependents at an annual cost of $34 billion. The Veterans Health Administration (VHA) and the Military Health System (MHS) collect and maintain patient health information in separate systems. The Gulf War exposed many deficiencies in these systems and highlighted the need for VA and DOD to be able to readily access and transfer accurate health data on their respective populations. In December 1992, the Congress asked us to report on how VA and DOD, along with the Indian Health Service (IHS), could share information technology (IT) and patient medical information to provide greater continuity of care, accelerate VA eligibility determinations, and save software development costs.[1] In November 1997, the President called for VA and DOD to create an interface that would allow the two agencies to share patient health information.

In 1998, the Government Computer-Based Patient Record (GCPR) project was initiated by VA, DOD, and IHS, which was included in the effort because of its population-based research expertise and its long-standing relationship with VA. Early project documents stated that, when completed, GCPR would allow health care professionals to "share clinical

[1] See *Federal Health Care: Increased Information System Sharing Could Improve Service, Reduce Costs* (GAO/IMTEC-93-33BR, June 1993).

information via a comprehensive, lifelong medical record." Given the inherent complexity of such an undertaking and the value of achieving this capability, the Congress directed us to report on the status of the GCPR effort. Specifically, we were asked to (1) describe GCPR's time frames, costs, and expected benefits; (2) determine whether barriers to the progress of the project exist; and (3) if barriers exist, describe agency actions to address them.[2]

Our review of the GCPR project was based on site visits to VA, DOD, and IHS facilities and on interviews with officials at these facilities and at the agencies' headquarters, GCPR management and contractors, and medical IT experts from the health care industry. We also reviewed relevant GCPR project documents as well as documents on the three agencies' health information systems. In addition, we conducted site visits to several private sector health care organizations that are also undertaking efforts to link disparate health information systems, and we interviewed representatives of these organizations about their experiences. We conducted this review from March 2000 through February 2001 in accordance with generally accepted government auditing standards. For more on our scope and methodology, see appendix I.

Results in Brief

Expanding time frames and cost estimates, as well as inadequate accountability and poor planning, have raised doubts about GCPR's ability to provide its expected benefits, prompting the agencies to refocus their approach to the project. Initial plans called for the agencies to begin worldwide deployment of GCPR on October 1, 2000, but intermediate target dates, such as those for testing, were not met, pushing project deployment out to an undefined date. GCPR cost estimates have also proven to be unreliable. In September 1999, GCPR was estimated to cost about $270 million over its 10-year life cycle, by August 2000, projections for GCPR stood at $360 million—estimates that GCPR project managers acknowledge are probably understated. By the end of 2000, it became evident that, in the near term, physicians and other health care professionals would not have access to comprehensive beneficiary health information across the three partner agencies, limiting the extent to which the effort will provide the benefits originally envisioned—including improved research and quality of care as well as clinical and administrative efficiencies.

[2] H.R. Rep. No. 106-616 at 383 (2000).

With accountability for GCPR blurred across several management entities, basic principles of sound IT project planning, development, and oversight have not been followed, creating barriers to progress. For example, clear goals and objectives have not been set; detailed plans for the design, implementation, and testing of the interface have not been developed; and critical decisions are not binding on all partners. In addition, GCPR plans have not resolved data incompatibilities and other differences that complicate the electronic exchange of health information among the three agencies' facilities. Finally, concerns related to developing a comprehensive strategy to guarantee the privacy and security of health information shared through GCPR have not been addressed.

In September 2000, we discussed these barriers with VHA's and MHS' Chief Information Officers (CIO). Soon after, they began to exercise much needed oversight, temporarily suspending further work on previously planned project activities and focusing on more immediate and less ambitious returns from GCPR. According to the CIOs, they are developing plans for an interim effort to allow VHA to view DOD health data and expect to have this capability by fall 2001. They plan to evaluate their existing IT products as well as commercial products that have a similar aim of sharing patient data to determine whether these technologies can be used for the interim effort, which may allow VA and DOD to reduce or eliminate redundancies. However, this interim effort, which does not include IHS as a partner, has several major limitations. For example, physicians at Military Treatment Facilities (MTF) will not be able to view VHA health information—or information from other MTFs. Moreover, the information's usefulness to health care providers and researchers will likely be limited, in part because the requested data could take as long as 48 hours to receive. Once DOD data are accessible to VA, project officials report that they plan to resume the broader, longer-term effort—establishing a link among multiple health information systems to provide comprehensive patient information to physicians and other health care professionals in the three agencies. However, to date, formal plans for the interim effort and the resumption of the broader GCPR project have not been developed. To help ensure that GCPR succeeds in exchanging patient health information, we are making recommendations for VA and DOD to continue to improve their oversight and planning of the project.

In commenting on our draft report, VA, DOD, and IHS concurred with the findings and recommendations. In their comments, the agencies also outline a new approach for GCPR.

Background

The GCPR effort developed out of VA and DOD discussions about ways to share data in their health information systems and from efforts to create electronic records for active duty personnel and veterans. The patients served by VA's and DOD's systems tend to be highly mobile. Consequently, their health records may be at multiple federal and nonfederal medical facilities both in and outside the United States. In December 1996, the Presidential Advisory Committee on Gulf War Veterans' Illnesses reported on many deficiencies in VA's and DOD's data capabilities for handling service members' health information. In November 1997, the President called for the two agencies to start developing a "comprehensive, life-long medical record for each service member." In August 1998, 8 months after the GCPR project was officially established, the President issued a directive requiring VA and DOD to develop a "computer-based patient record system that will accurately and efficiently exchange information." The directive further stated that VA and DOD should "define, acquire, and implement a fully integrated computer-based patient record available across the entire spectrum of health care delivery over the lifetime of the patient" and recognized VA and DOD's effort to "create additional interface mechanisms that will act as bridges between existing systems."[3] IHS became involved because of its expertise in population-based research and its long-standing relationship with VA in caring for the Indian veteran population as well as IHS' desire to improve the exchange of information among its facilities.

Each of the three agencies' health facilities is linked to their agency's regional database or an IT center: VA has about 750 facilities in 22 regions, DOD has about 600 MTFs in 14 domestic and overseas medical regions, and IHS has 550 facilities in 12 regions.[4] Currently, these facilities cannot electronically share patient health information across agency lines, and only VA facilities have the capability of sharing certain information across regions.

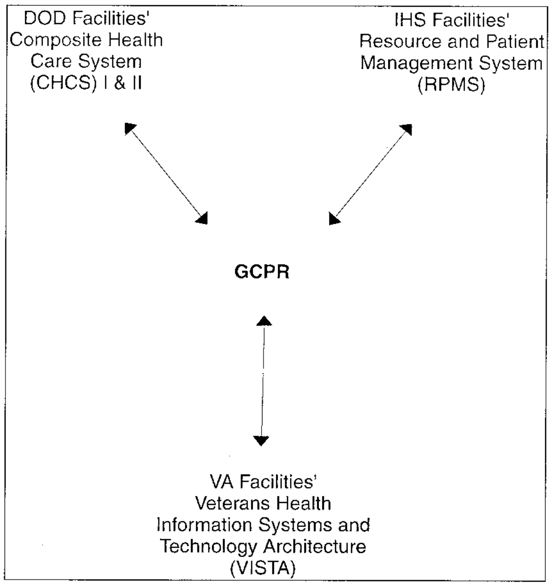
GCPR is not intended to be a separate computerized health information system, nor is it meant to replace VA's, DOD's, and IHS' existing systems.

[3] National Science and Technology Council, *A National Obligation: Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families After Future Deployments*, Presidential Review Directive 5 (Washington, D.C.: Executive Office of the President, Office of Science and Technology Policy, Aug. 1998).

[4] VA's regions are officially referred to as Veterans' Integrated Service Networks, or VISNs; IHS' regions are generally referred to as areas.

GCPR is intended to allow physicians and other authorized users at the agencies' health facilities to access data from any of the agencies' other health facilities by serving as an interface among their health information systems (see fig. 1). As envisioned, the interface would compile requested patient information in a temporary or virtual record while appearing on the computer screen in the format of the user's system. GCPR would divide health data into 24 categories, or "partitions," including pharmacy, laboratory results, adverse reactions, vital signs, patient demographics, and doctors' notes.

Figure 1: GCPR Interface With Agencies' Health Information Systems


DOD Facilities' Composite Health Care System (CHCS) I & II
IHS Facilities' Resource and Patient Management System (RPMS)
GCPR
VA Facilities' Veterans Health Information Systems and Technology Architecture (VISTA)

Source: GAO.

With this ability to exchange information, GCPR is expected to achieve several benefits, including improving quality of care; providing data for population-based research and public health-surveillance; advancing industrywide medical information standards; and generating administrative and clinical efficiencies, such as cost savings.

Several management entities share responsibility for GCPR:

- *Military and Veterans Health Coordinating Board*: This entity was created to ensure coordination among VA, DOD, and the Department of Health and Human Services (HHS) on military and veteran health matters, particularly as they relate to deployed settings, such as the Persian Gulf. The board also oversees implementation of the President's August 1998 directive. The board consists of the Secretaries of VA, DOD, and HHS.
- *DOD and VA Executive Council*: The council was created to identify and implement interagency initiatives that are national in scope. One initiative is to ensure a smooth transfer of information between DOD's and VA's health care systems through efforts such as GCPR. The council comprises VA's Under Secretary for Health, DOD's Assistant Secretary for Health Affairs, their key deputies, and the Surgeon General of each military branch.
- *GCPR Board of Directors*: The board was established to set GCPR programmatic and strategic priorities and secure funding from VA, DOD, and IHS. The board consists of the VA Under Secretary for Health and CIOs for MHS and IHS.[5]
- *GCPR Executive Committee*: The Executive Committee sets tactical priorities, oversees project management activities, and ensures that adequate resources are available. The committee membership consists of senior managers from VA, DOD, and IHS.

GCPR is managed on a day-to-day basis by a program office staffed by personnel from VA, DOD, IHS, and the project's prime contractor, Litton/PRC of McLean, Virginia. Litton/PRC is responsible for building, shipping, installing, configuring, and operating the interface and administering site training. Battelle Memorial Institute of Columbus, Ohio, holds contracts for developing medical "reference models," which allow for the exchange of data among different systems without requiring

[5] The MHS CIO replaced the Deputy Surgeon General of the Navy as DOD's representative on the board. Previously, the MHS CIO was an ex-officio member and was recorded as a participant in board minutes.

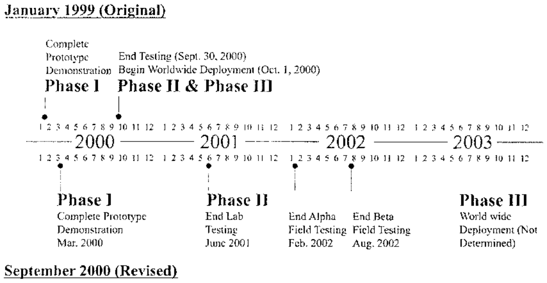
standardization.[6] Assisting in the project are government-led work groups, which consist of VA, DOD, and IHS employees and Litton/PRC staff. The work groups' key tasks include acquisition, finance, legal work, marketing, telecommunications, and documenting clinical practices.

Time Frames and Cost Estimates Have Expanded, and Expected Benefits Have Been Delayed

Throughout the course of the GCPR project, time frames and cost estimates have expanded, and GCPR's ability to deliver its expected benefits has become less certain. In 1999, initial plans called for GCPR to begin worldwide deployment October 1, 2000, but target dates for intermediate phases, such as testing, were not met, pushing project deployment out to an undefined date. For example, completion of testing was originally scheduled for September 2000 but was delayed until August 2002 (see fig. 2).

[6] Comprehensive industry standards for medical language and its context do not exist. Consequently, different health information systems or providers may use different terms to mean the same thing. For example, to indicate a patient is suffering from a rhinovirus, some may use "cold" while others may use "upper respiratory disorder" or "nasal congestion." In addition, without knowing the context in which a term such as "cold" is used, it is difficult to determine whether the patient has a rhinovirus or feels cold or has chronic obstructed lung disease. According to GCPR project documents, reference models would allow translation among the different medical languages and terminologies used by VA, DOD, and IHS.

Figure 2: GCPR Time Frames as of January 1999 and September 2000


January 1999 (Original)
Complete Prototype Demonstration
Phase I
End Testing (Sept. 30, 2000)
Begin Worldwide Deployment (Oct. 1, 2000)
Phase II & Phase III
1 2 3 4 5 6 7 8 9 10 11 12
2000
2001
2002
2003
Phase I
Complete Prototype Demonstration Mar. 2000
Phase II
End Lab Testing June 2001
End Alpha Field Testing Feb. 2002
End Beta Field Testing Aug. 2002
Phase III
World wide Deployment (Not Determined)
September 2000 (Revised)

Source: GCPR project documents.

GCPR cost estimates also increased. GCPR was estimated in September 1999 to cost about $270 million over its 10-year life cycle; by August 2000, projections for GCPR stood at $360 million (see table 1). However, GCPR project officials told us that the cost estimates were unreliable and probably understated, in part because some costs—such as computer hardware needed by the project's contractors—were not included. Other cost estimates, such as those for deployment, could not be verified. In the case of deployment, final decisions affecting costs were not made.

Table 1: Changes in GCPR's Estimated Project Cost

(Dollars in millions)

Phase	Estimates as of Sept. 1999	Estimates as of Aug. 2000
Preliminary	$12.5	$1.8
Phase I (prototype and proof of concept)	42.0	17.7
Phase II (pilot, alpha-, and beta-field testing)	23.3	98.2
Phase III (phased deployment)	92.8	133.5
Ongoing operations	99.0	108.7
Total	**$269.6**	**$359.9**

Source: GCPR project documents.

By the end of 2000, it became apparent that the benefits described in GCPR project documents and brochures and on its website—including access to comprehensive, life-long patient information—would not be realized in the near future. According to Litton/PRC, preliminary testing of data transfer among selected VA facilities is demonstrating that the GCPR technology works. However, significant issues in sharing comprehensive patient data have not been adequately addressed. For example, while GCPR managers planned to field test 6[7] of the 24 data partitions, they had no plans for when other partitions would be tested. Moreover, access was to be limited to patient information in VA's, DOD's, and IHS' health information systems; information in other major data sources, such as TRICARE—DOD's managed care program—and other third-party providers would not be accessible. Access to patient information would be further limited because full deployment of CHCS II—DOD's new, more comprehensive health information system, currently under development—has been delayed until 2004 as the result of complications such as limited system capacity and slow response time. With CHCS II, GCPR would provide access to information on immunizations; allergies; and outpatient encounters, such as diagnostic and treatment codes; as well as to information in CHCS I, DOD's current system, which primarily includes information on patient hospital admission and discharge, patient medications, laboratory results, and radiology. Providing other anticipated benefits—such as improved quality of patient health records—will also be difficult because GCPR plans do not include steps for correcting long-standing data problems, such as inaccurate data entries.

[7] Demographics, security, laboratory results, problem lists, medication profiles, and adverse reactions.

Inadequate Accountability and Planning Compromised GCPR's Progress

The lack of accountability and sound IT project planning—critical to any project, particularly an interagency effort of this magnitude and complexity—put GCPR at risk of failing. The relationships among GCPR's management entities were not clearly established, and no one entity had the authority to make final project decisions binding on the other entities. As a result, plans for the development of GCPR have not included a clear vision for the project and have not given sufficient attention to technological and privacy and security issues as the effort has moved forward.[8]

Lack of Accountability Undermined Agencies' Commitment to the Project

From the outset, decision-making and oversight were blurred across several management entities, compromising GCPR's progress. The roles and responsibilities of these entities and the relationships among them are not spelled out in the VA-DOD-IHS memorandum of agreement (MOA), and no one entity exercised final authority over the project. The Board of Directors and the Executive Committee did not follow sound IT business practices—such as ensuring agency commitment, securing stable funding, and monitoring the project's progress—as dictated by federal requirements.[9] For example, GCPR documents show that VA, DOD, and IHS should provide consistent project funding of 40 percent, 40 percent, and 20 percent, respectively, but DOD has never provided this level of funding and, at times, temporarily withheld funding it had promised. Moreover, the Board of Directors and the Executive Committee did not exercise sufficient oversight, including monitoring, to ensure that the project would be adequately funded.

Without agency commitment and sufficient oversight, the project team has been limited in its ability to manage GCPR effectively or efficiently. Unstable funding forced GCPR project managers to develop and issue multiple short-term contracts for work that could have been covered by a single longer-term contract. At one point during our review, project managers told us that the project would end after field-testing because of a lack of adequate funding and a lack of a clear mandate to proceed with full

[8] An earlier independent risk assessment by Northpoint Software Ventures, Inc., found similar weaknesses in GCPR's business practices.

[9] Six laws largely lay out the IT management responsibilities of federal agencies: the Federal Records Act of 1950, the Privacy Act of 1974, the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Government Paperwork Elimination Act of 1998.

deployment, even though plans called for the project to continue through deployment.

Inadequate Planning Hindered Progress

The three partner agencies never reached consensus on GCPR's mission and how it would relate to the individual agencies' missions. In addition, key project documents, such as the MOA establishing GCPR, have not adequately spelled out the project's goals and objectives. For example, some DOD officials thought GCPR's mission paralleled the goals and objectives of Presidential Review Directive 5; however, GCPR project managers did not share this understanding and the directive was never adopted as GCPR's mission. Without an agreed upon mission with clear goals and objectives, it remained unclear what problem GCPR was trying to solve. This lack of consensus on the project's mission, goals, and objectives affected the agencies' dedication of resources. Expecting GCPR to enhance its ability to carry out its mission to provide health care to veterans, VA was providing the most funding to the project. In contrast, DOD elected to place priority on funding CHCS II, which is estimated to cost several billion dollars because officials believe it will more specifically address the Department's health mission.

GCPR plans have also not sufficiently addressed other critical issues that need to be resolved, such as decisions about key data elements. For example, DOD and IHS use different identifiers to match health records to patients—DOD facilities use Social Security numbers, while IHS facilities use facility-specific health record numbers. Differences such as these complicate the electronic exchange of health information. Further, in the absence of common medical terminology, project personnel, assisted by Battelle, are developing reference models they believe will interpret VA, DOD, and IHS data and present the data in a format understandable to the user—without requiring cross-agency standards. However, GCPR plans have not specified the key tasks for developing these models, their relation to one another, and who should carry them out. As a result, work progressed slowly and rework has been necessary. For example, coordination between the Battelle team and Litton/PRC was, initially, not adequate to ensure that the reference models developed by Battelle would meet Litton/PRC's technical requirements for developing the interface. Therefore, the models had to be revised.

In addition, the MOA and other key project documents did not lay out the specific roles and responsibilities of VA, DOD, and IHS in developing, testing, and deploying the interface. GCPR plans also did not describe how the project would use the agencies' existing technologies for sharing patient health information and to avoid duplication of effort. For example, GCPR plans do not discuss VA's "remote view" capability—which will allow users of VA's Computer Patient Record System (CPRS)[10] to simultaneously view health data across multiple facilities—or three of DOD's health information systems: Theater Medical Information Program (TMIP), Pacific Medical Network (PACMEDNET), and Pharmacy Data Transaction System (PDTS).[11]

Finally, a comprehensive strategy to guarantee the privacy and security of electronic information shared through GCPR was not developed. GCPR's draft privacy and security plan delegates primary responsibility for ensuring privacy and security to more than 1,000 VA, DOD, and IHS local facilities, with few additional resources and little guidance. However, there have been long-standing privacy and security problems within VA's, and DOD's information systems. For example, weak access controls put sensitive information—including health information—at risk of deliberate or inadvertent misuse, improper disclosure, or destruction.[12] By providing broader access to more users, GCPR may exacerbate these risks. DOD is required by the Floyd D. Spence National Defense Authorization Act for 2001 (P.L. 106-398) to submit to the Congress a comprehensive plan consistent with HHS medical privacy regulations to improve privacy. [13] The act also requires DOD to promulgate interim regulations that allow for use of medical records as necessary for certain purposes, including patient treatment and public health reporting, thus providing DOD the flexibility to share patient health information through a mechanism such as GCPR. The HHS privacy regulations went into effect on April 14, 2001, and contain provisions that require consent to disclose health information

[10] CPRS is a component system of VISTA.

[11] DOD's TMIP, currently under development, is intended to capture medical information for deployed personnel; PACMEDNET is a joint DOD/VA effort to link medical records in the Pacific region; and PDTS is DOD's new patient drug transaction and safety database. Program costs are $14.8 million for PDTS and $19.5 million for PACMEDNET; program costs for TMIP have not been determined.

[12] See *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, Sept. 6, 2000).

[13] The Health Insurance and Portability Act (HIPAA) requires the development of comprehensive privacy standards that would establish rights for patients with respect to their medical records and define the conditions for using and disclosing identifiable health information. (P.L. 104-191, 264, 110 Stat. 1936, 2033.) The final regulations require that patient consent must be secured before disclosing information in individual medical records.

before engaging in treatment, payment, or health care operations (45 C.F.R. parts 160-164).[14]

CIOs Change Immediate Focus, but Serious Concerns Remain

Over the past several months, we have provided briefings on our findings to agency and project officials, including the CIOs of VHA and MHS whom we initially briefed in September 2000. Concerned about the lack of progress and the significant weaknesses that we found, the CIOs have begun to exert much needed oversight. They told us that they are now focusing on "early deliverables" for VA and DOD. To ensure more immediate applicability of GCPR to their missions, VA and DOD's current priority is to allow VA health care providers to view DOD health data by the end of September 2001. Once this interim effort is completed, the CIOs told us that they plan to resume the broader GCPR project—establishing a link among all three partner agencies' health information systems.

Under the interim effort, as described by the CIOs, certain trigger events, such as a new veteran enrolling for VA medical treatment, will prompt VISTA to contact a central server, which would search the hundreds of CHCS I sites and collect any data on that patient. To help ensure efficient development of the interim effort, VA and DOD now plan to evaluate their existing IT products—such as VA's remote view capability, which could have the potential to facilitate the retrieval of DOD health data—as well as commercial products to determine if these technologies can be used to electronically transmit data among the agencies' systems. While we did not conduct an in-depth review of these initiatives, we agree that such an evaluation may allow VA and DOD to reduce or eliminate redundancies because these products have a common aim of sharing patient data. However, it is unclear to what extent the interim effort will be using the GCPR technology—which, according to Litton/PRC, has demonstrated that data can be moved among VA facilities.

However, our concerns regarding the usefulness of the information—and the implications for GCPR's expected benefits—still remain. For example, under the interim effort, the requested information is expected to take as long as 48 hours to be received. In addition, only authorized VHA personnel will have the ability to see CHCS I data from MTFs; health care

[14] The Secretary of HHS has stated that there will be guidelines and modifications made to the consent provisions to make it clear that doctors and hospitals will have access to necessary medical information about patients whom they are treating.

providers at MTFs will not be able to view health information from VHA—or information from other MTFs. It is also unclear whether all or only selected VA and DOD facilities will have the interim capability now being proposed. IHS will not be included in the interim effort. Moreover, the interim effort will rely on DOD's aging system, CHCS I, which historically has not been adequate to meet physicians' needs. CHCS I is primarily limited to administrative information and some patient medical information, such as pharmacy and laboratory results. CHCS I does not include patient information on the health status of personnel when they enter military service, on reservists who receive medical care while not on active duty status, or on military personnel who receive care from TRICARE providers. CHCS I also does not include physician notes made during examinations. In addition, information captured by CHCS I can vary from MTF to MTF. Some facilities, such as Tripler Army Medical Center in Hawaii, have significantly enhanced their CHCS software to respond to the needs of physicians and other system users and to collect patient health information not collected by other facilities.

Further, the interim effort will need to address many of the same problems that confronted the broader GCPR effort:

- Transmitted information will be viewable only as sent; therefore, it will not be computable—that is, it will not be possible to organize or manipulate data for quick review or research.
- Electronic connectivity among MTFs is limited, and the interim effort does not propose to establish facility-to-facility links. Currently, only MTFs within the same region and using the same DOD IT hardware can access one another's data using CHCS I.
- The requested data will not be meaningful to the VA user unless CHCS' language is translated into VISTA's. For example, without interpretation, a VA physician's VISTA query for a patient's sodium level would not recognize "NA" (used by DOD) as equivalent to "sodium" (used by VA). Until terms and their context are standardized or the variations are identified, or "mapped," across all VA and DOD facilities, much of the information could be meaningless to VA physicians.

According to VHA's and MHS' CIOs, detailed plans and time frames are being prepared for the short-term, interim effort to allow VA to receive available electronic health information in CHCS I. However, as of the end of February 2001, no agreement on the goals, time frames, costs, and oversight for the interim approach has been reached, and no formal plans for the interim project exist. Moreover, revised plans for the broader, long-term GCPR project—including how and when IHS will resume its role in the project—have not been developed.

While a draft of this report was being reviewed by the agencies, they developed a new near-term effort which they outlined in their comments. This effort, which revises their interim effort, is intended to address our concerns. However, many of our concerns remain and are addressed in our response to comments from the agencies.

Conclusions

GCPR's aim to allow health care providers to electronically share comprehensive patient information should provide VA, DOD, and IHS a valuable opportunity to improve the quality of care for their beneficiaries. But without a lead entity, a clear mission, and detailed planning to achieve that mission, it is difficult to monitor progress, identify project risks, and develop appropriate contingency plans to keep the project moving forward and on track. Critical project decisions were not made, and the agencies were not bound by those that were made. The VA and DOD CIOs' action to focus on short-term deliverables and to capitalize on existing technologies is warranted and a step in the right direction. However, until problems with the two agencies' existing systems and issues regarding planning, management, and accountability are resolved, projected costs are likely to continue to increase, and implementation of the larger GCPR effort—along with its expected benefits—will continue to be delayed.

Recommendations for Executive Action

To help strengthen management and oversight of GCPR, we recommend that the Secretaries of VA and DOD and the Director of IHS reassess decisions about the broader, long-term GCPR project, based on the results of the interim effort. If the Secretaries of VA and DOD and the Director of IHS decide to continue with the broader effort, they should direct their health CIOs to apply the principles of sound project management delineated in our following recommendations for the interim effort.

For the interim effort, we recommend that the Secretaries of VA and DOD and the Director of IHS direct their health CIOs to take the following actions:

- Designate a lead entity with final decision-making authority and establish a clear line of authority.
- Create comprehensive and coordinated plans to ensure that the agencies' can share comprehensive, meaningful, accurate, and secure patient health data. These plans include an agreed-upon mission and clear goals,

objectives, and performance measures, and they should capitalize on existing medical IT capabilities.

Agency Comments

VA, DOD, and IHS reviewed and separately commented on a draft of this report. Each concurred with the findings and recommendations. The agencies also provided comments that outline a new near-term effort for GCPR and that aim to clarify GCPR's purpose. Additionally, VA, DOD, and IHS provided written technical comments, which we have incorporated where appropriate. The full texts of their comments are reprinted as appendixes II, III, and IV.

Regarding our recommendation to establish a clear line of authority, the Secretary of VA committed to meeting with the Secretary of Defense and the Director of IHS to designate a lead entity that will have decision-making authority for the three organizations. He said that once established, that entity will have a clear line of authority over all GCPR development activities. With regard to our recommendation to create comprehensive and coordinated plans for sharing patient health data, the Secretary of VA said he would direct the VHA CIO, in collaboration with VA's departmentwide CIO to prepare such plans under the oversight of the lead entity. In response to our recommendation that longer-term GCPR decisions be reassessed based on the results of the interim effort, the Secretary of VA responded that GCPR will be reassessed based on the results of their near-term effort. Additionally, he said that the longer-term strategy will depend to some extent on advances in medical informatics, standards development, and the ability to bring in additional partners.

DOD provided similar comments on our recommendation concerning longer-term GCPR decisions and also mentioned that it plans to include the Military Health System Information Management Committee in GCPR oversight. While IHS provided no information on the steps it plans to take to implement our recommendations, it commented, along with VA and DOD, that collaboration is essential to the future of GCPR. Overall, the agencies' statements, in our view, represent a commitment to oversight and management of GCPR. However, it is much too soon to know whether their commitment will result in a successful project.

VA, DOD, and IHS also provided information that, according to the organizations, is intended to serve as a foundation for assessing GCPR and its progress. The agencies emphasized that GCPR is not intended to carry the whole weight for the service members' health records and the related health information systems, but instead consists of the agencies' core health information systems with GCPR handling the transfer and mediation of data. Our report does not suggest that GCPR is a replacement for the agencies' information systems or that it should carry the weight of the agencies' patient health information. Rather, our report states that GCPR is intended to create an electronic link that will enable the agencies to share patient data from their separate health information systems.

The agencies also provided a clarification of GCPR's purpose, stating that it will provide a longitudinal record covering service members from the start of their service through their care with VA. VA acknowledges that the realities of the challenges the project has presented have led to a scaling back of the initial version of GCPR as described in early project documents, such as budget submissions, contractors' statements of work, and project plans. These documents indicated that in addition to including IHS, GCPR would permit health care professionals to share clinical information via a comprehensive lifelong, medical record—one that would include information from all sources of care. GCPR was similarly described on GCPR's home page and during briefings to the Congress and others, such as the National Committee on Vital and Health Statistics. Some documents, such as VA's Fiscal Year 2001 Performance Plan, have described GCPR as including dependents of service members. To the extent that the agencies agree on the scaled-back description of GCPR, project documents and communications need to reflect this new understanding. This is, in part, why we recommended that the agencies develop and document a clear, agreed upon project mission, along with specific goals, objectives, and performance measures.

The agencies' also provided information on a new near-term effort for GCPR, which they developed while reviewing our draft report. According to the agencies, this revised near-term effort that they have developed uses the GCPR framework and will provide VA clinicians with DOD data on all active duty members, retirees, and separated personnel. VA and DOD recognize that this one-way flow of information is not perfect but should be a substantial improvement for physicians making medical decisions and enhance the continuity of care for veterans. According to the agencies, the near-term effort is funded through year 2001 and they expect to have initial operating capability by fall 2001. We agree that, if successful, this effort should provide useful information to VA clinicians. In our view, their outline of the new near-term approach indicates that it is only in the concept stage and detailed planning and actual work are just beginning. For example, the agencies note that current data will be sent in "near real-time transmission," and historical data will be "extracted and transmitted on a predetermined schedule." But they do not define "near real-time" and "predetermined schedule."

Additionally, the agencies assert that the new near-term effort addresses many of the concerns we raised in the report. However, several of these issues remain and, as we recommended, need to be reassessed at the conclusion of the near-term effort because of their implications for the long-term effort:

- GCPR—both the near-term and larger efforts—will not provide a longitudinal record because plans call for GCPR to use DOD's CHCS I for the foreseeable future. CHCS I, as DOD acknowledges in its comments, was not designed to include patient information on the health status of personnel when they enter military service, on reservists who receive medical care while not on active duty status, or on military personnel who receive care outside MTFs.
- The meaningfulness of the transmitted data remains in question because the agencies do not plan to standardize or map the differing terminology in their health information systems. As we note in the report, without standardized terminology or mapping, the meaning of certain terms used in medical records may not be apparent to the VA provider requesting the information. For example, unless the context is clear, the meaning of the term "cold" in a medical record may be interpreted as meaning a rhinovirus, a feeling of being cold, or having chronic obstructed lung disease.
- The agencies also need to more fully address data-specific matters, such as GCPR's reference modeling, before developing additional hardware and software. Once they reach consensus on these issues, their agreement must be clearly stated in a formalized document—one that is binding on all three partners. Finally, for the project to be successfully deployed, detailed plans on GCPR's system components and tasks with clear project parameters need to be developed. Until such plans are developed, the agencies' GCPR efforts cannot be fully assessed.
- Privacy and security issues are also continuing concerns. DOD states in its comments that it does not intend to delegate responsibility for complying with DOD and federal privacy and security requirements to its local facilities. However, DOD does not describe how it plans to ensure compliance, raising concerns such as how unintended or unauthorized disclosure or access of information would be prevented when the near-term effort provides selected "data feeds from CHCS I [into] a database to be accessed by VA." Similarly, VA generally describes how authorized VA staff will access DOD medical records. However, we have concerns about how the two Departments will ensure the privacy and security of patient information given the security weaknesses in their computer systems, which we have repeatedly reported on. In March 2001, we reported that DOD continues to face significant personnel, technical, and operational

challenges in implementing a departmentwide information security program, and DOD management has not carried out sufficient program oversight.[15] We included VA's computer security in our January 2001 High-Risk Series and, in an accompanying report, pointed out persistent computer security weaknesses that placed critical VA operations, including health care delivery, at risk of misuse, fraud, improper disclosure, or destruction.[16] For example, we found that VA has not adequately limited access granted to authorized users, managed user identification and passwords, or monitored access activity—weaknesses that VA's Inspector General recently testified on.[17]

- Funding is also a concern. VA states that GCPR's "success and rate of progression will depend to some extent on the ability to add partners and available funding." Similarly, DOD states that GCPR program requirements will be funded in accordance with overarching DOD mission priorities. IHS also noted that it faces competing demands for scarce resources. We recognize that each agency has multiple priorities. However, securing adequate and stable funding and determining whether additional partners are needed depends on reliable cost estimates—which can only be determined with well-defined goals and detailed plans for achieving those goals. As DOD points out in its comments, the 10-year cost estimates for GCPR will continue to be considered unreliable until clear mid- and long-term goals and objectives have been established and agreed to by the three agencies.

Each of the three agencies also stated that GCPR may have been judged by the criteria used to assess a standard information system development effort and that doing so understates the complexity of their undertaking. While we believe that the technology exists to support GCPR—particularly the new near-term effort—we agree that GCPR presents unique and difficult administrative challenges. Yet it is this very complexity that calls for thorough planning, interagency coordination, and diligent oversight as well as consistent and regular communication of the project's status and progress to all stakeholders.

[15] *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, Mar. 30, 2001).

[16] *Major Management Challenges and Program Risks: Department of Veterans Affairs* (GAO-01-255, Jan. 2001).

[17] Testimony of Richard J. Griffin, Inspector General, Department of Veterans Affairs, before the House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, April 4, 2001.

Finally, VA noted that it would like to discuss with us certain details in our report with which it did not fully agree but yet did not disclose in its comments. Throughout the course of the project—and particularly over the past 6 months—we met frequently with the agencies to provide observations on our work and discuss any concerns that were brought to our attention. We are committed to continuing to meet with VA, DOD, and IHS to help in this important endeavor.

We are sending this report to the Honorable Anthony Principi, Secretary of Veterans Affairs; the Honorable Donald Rumsfeld, Secretary of Defense; the Honorable Tommy Thompson, Secretary of Health and Human Services; appropriate congressional committees; and other interested parties. We will also make copies available to others upon request. Should you have any questions on matters discussed in this report, please contact me at (202) 512-7101. Other contacts and key contributors to this report are listed in appendix V.

Stephen P. Backhus

Stephen P. Backhus
Director, Health Care—Veterans'
and Military Health Care Issues

Appendix I: Scope and Methodology

To determine the status of the GCPR project, we conducted site visits to VA, DOD, and IHS facilities; interviewed personnel at these locations, representatives of nonfederal health care organizations, and others knowledgeable about computerized linking of disparate health information systems; and reviewed documents relevant to the project. We also consulted with project officials at various times during our audit about the status of our review.

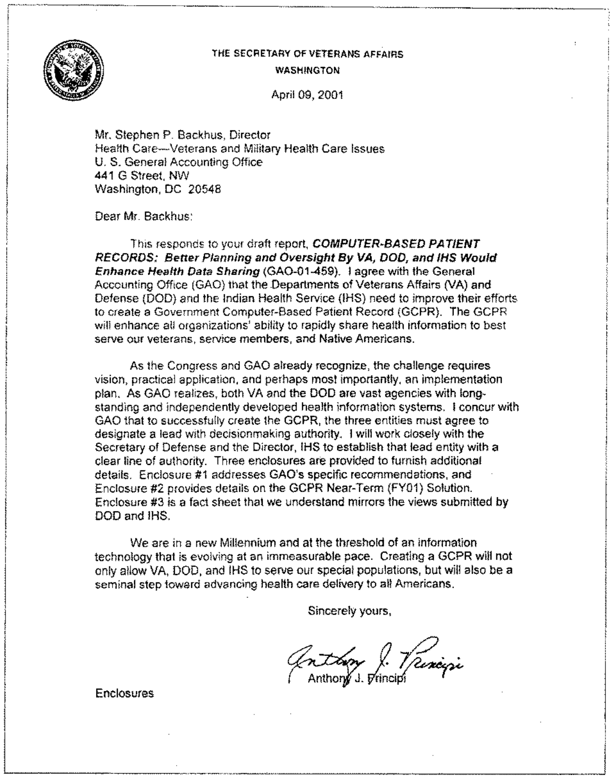
We went to a total of nine VA, DOD, and IHS health care facilities in California, Hawaii, Indiana, and Washington, D.C. These sites were judgmentally selected based on a variety of factors, including diversity of system capabilities and size and type of facility, such as major medical centers and small community-based clinics. Therefore, they are not necessarily representative of the agencies' facilities. During these site visits, we spoke with a variety of facility staff—ranging from a DOD regional medical commander and IHS facility managers to VA administrative personnel—about their experiences using the agencies' existing health information systems. We also asked them about what additional information and system features they consider to be important in treating patients and conducting population-based research. Further, we talked with facility IT technicians and administrators about their systems' capabilities and the technical requirements for developing the GCPR interface, and we discussed the potential effect the interface might have on current operations and systems.

We interviewed VA, DOD, and IHS officials, primarily from the agencies' headquarters, involved directly in the GCPR project to obtain specific information about the project's day-to-day operations and management, including timelines, costs, and technical matters. We also interviewed personnel from the two primary GCPR contractors—Litton/PRC in McLean, Virginia, and Battelle Memorial Institute of Columbus, Ohio—on the status of the interface development, particularly regarding the reference modeling. We also talked with agency representatives on the GCPR Board of Directors and Executive Committee about the oversight of the project.

To obtain additional perspectives about the development of computerized patient record systems, we talked with recognized leaders in the field and visited selected private sector facilities, including Kaiser Permanente, Aurora HealthCare of Wisconsin, and the Regenstrief Institute of the University of Indiana in Indianapolis. We also talked with officials from the National Committee on Vital and Health Statistics regarding privacy and security issues and the status of the development of HIPAA regulations.

Finally, we reviewed many GCPR project documents. These included technical plans, such as the project's draft privacy and security plan, deployment plans, and other planning documents; cost analyses; and Board of Directors and Executive Committee meeting minutes; and other relevant project documents. We conducted our review between March 2000 and April 2001 in accordance with generally accepted government auditing standards.

Appendix II: Comments From the Department of Veterans Affairs



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

April 09, 2001

Mr. Stephen P. Backhus, Director
Health Care—Veterans and Military Health Care Issues
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Backhus:

This responds to your draft report, ***COMPUTER-BASED PATIENT RECORDS: Better Planning and Oversight By VA, DOD, and IHS Would Enhance Health Data Sharing*** (GAO-01-459). I agree with the General Accounting Office (GAO) that the Departments of Veterans Affairs (VA) and Defense (DOD) and the Indian Health Service (IHS) need to improve their efforts to create a Government Computer-Based Patient Record (GCPR). The GCPR will enhance all organizations' ability to rapidly share health information to best serve our veterans, service members, and Native Americans.

As the Congress and GAO already recognize, the challenge requires vision, practical application, and perhaps most importantly, an implementation plan. As GAO realizes, both VA and the DOD are vast agencies with long-standing and independently developed health information systems. I concur with GAO that to successfully create the GCPR, the three entities must agree to designate a lead with decisionmaking authority. I will work closely with the Secretary of Defense and the Director, IHS to establish that lead entity with a clear line of authority. Three enclosures are provided to furnish additional details. Enclosure #1 addresses GAO's specific recommendations, and Enclosure #2 provides details on the GCPR Near-Term (FY01) Solution. Enclosure #3 is a fact sheet that we understand mirrors the views submitted by DOD and IHS.

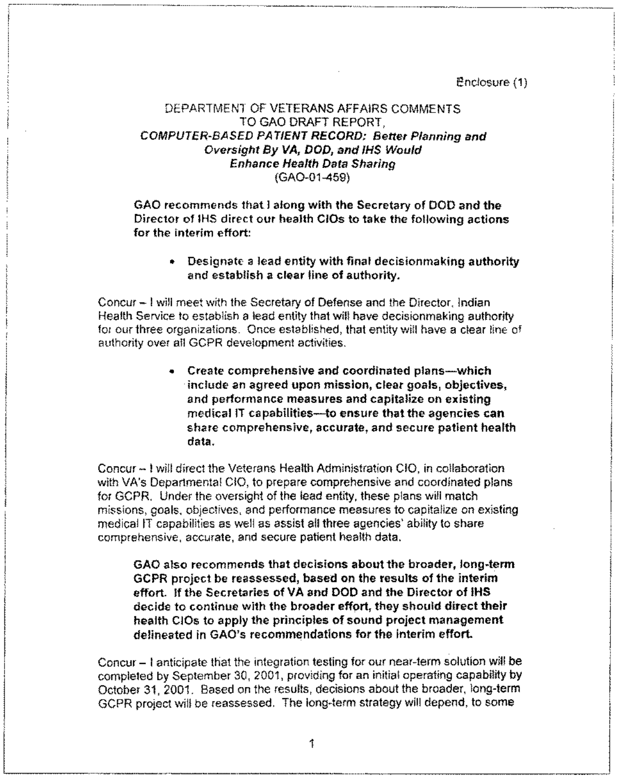
We are in a new Millennium and at the threshold of an information technology that is evolving at an immeasurable pace. Creating a GCPR will not only allow VA, DOD, and IHS to serve our special populations, but will also be a seminal step toward advancing health care delivery to all Americans.

Sincerely yours,

Anthony J. Principi

Anthony J. Principi

Enclosures



Enclosure (1)

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
COMPUTER-BASED PATIENT RECORD: Better Planning and Oversight By VA, DOD, and IHS Would Enhance Health Data Sharing
(GAO-01-459)

GAO recommends that I along with the Secretary of DOD and the Director of IHS direct our health CIOs to take the following actions for the interim effort:

- **Designate a lead entity with final decisionmaking authority and establish a clear line of authority.**

Concur – I will meet with the Secretary of Defense and the Director, Indian Health Service to establish a lead entity that will have decisionmaking authority for our three organizations. Once established, that entity will have a clear line of authority over all GCPR development activities.

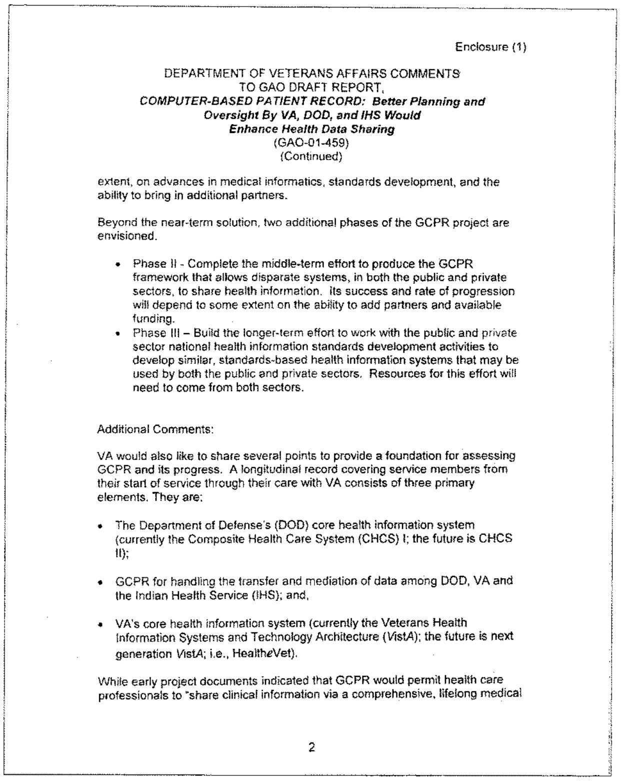
- **Create comprehensive and coordinated plans—which include an agreed upon mission, clear goals, objectives, and performance measures and capitalize on existing medical IT capabilities—to ensure that the agencies can share comprehensive, accurate, and secure patient health data.**

Concur – I will direct the Veterans Health Administration CIO, in collaboration with VA's Departmental CIO, to prepare comprehensive and coordinated plans for GCPR. Under the oversight of the lead entity, these plans will match missions, goals, objectives, and performance measures to capitalize on existing medical IT capabilities as well as assist all three agencies' ability to share comprehensive, accurate, and secure patient health data.

GAO also recommends that decisions about the broader, long-term GCPR project be reassessed, based on the results of the interim effort. If the Secretaries of VA and DOD and the Director of IHS decide to continue with the broader effort, they should direct their health CIOs to apply the principles of sound project management delineated in GAO's recommendations for the interim effort.

Concur – I anticipate that the integration testing for our near-term solution will be completed by September 30, 2001, providing for an initial operating capability by October 31, 2001. Based on the results, decisions about the broader, long-term GCPR project will be reassessed. The long-term strategy will depend, to some

1



Enclosure (1)

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
COMPUTER-BASED PATIENT RECORD: Better Planning and Oversight By VA, DOD, and IHS Would Enhance Health Data Sharing
(GAO-01-459)
(Continued)

extent, on advances in medical informatics, standards development, and the ability to bring in additional partners.

Beyond the near-term solution, two additional phases of the GCPR project are envisioned.

- Phase II - Complete the middle-term effort to produce the GCPR framework that allows disparate systems, in both the public and private sectors, to share health information. Its success and rate of progression will depend to some extent on the ability to add partners and available funding.
- Phase III – Build the longer-term effort to work with the public and private sector national health information standards development activities to develop similar, standards-based health information systems that may be used by both the public and private sectors. Resources for this effort will need to come from both sectors.

Additional Comments:

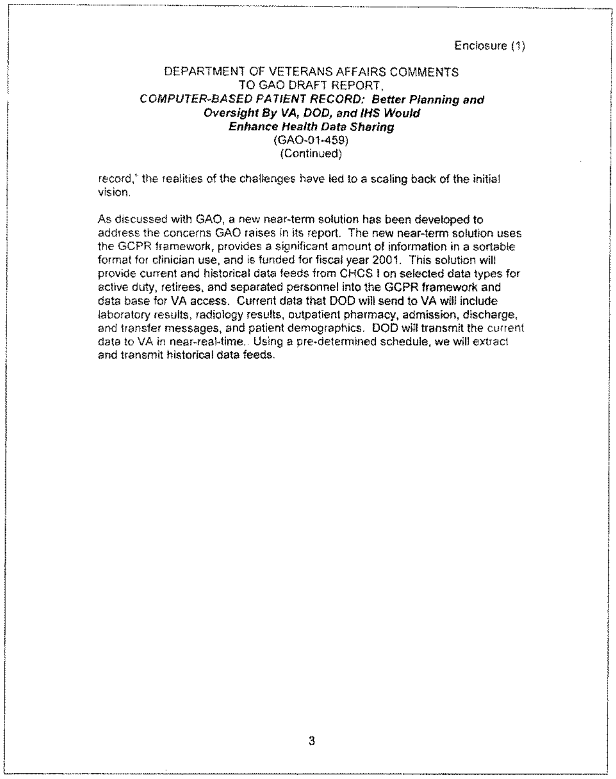
VA would also like to share several points to provide a foundation for assessing GCPR and its progress. A longitudinal record covering service members from their start of service through their care with VA consists of three primary elements. They are:

- The Department of Defense's (DOD) core health information system (currently the Composite Health Care System (CHCS) I; the future is CHCS II);

- GCPR for handling the transfer and mediation of data among DOD, VA and the Indian Health Service (IHS); and,

- VA's core health information system (currently the Veterans Health Information Systems and Technology Architecture (*VistA*); the future is next generation *VistA*; i.e., Health*e*Vet).

While early project documents indicated that GCPR would permit health care professionals to "share clinical information via a comprehensive, lifelong medical



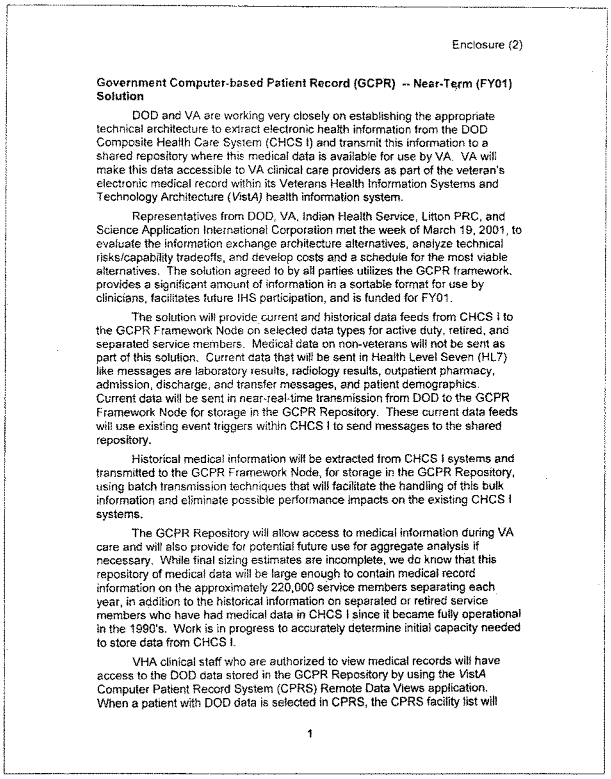
Enclosure (1)

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
***COMPUTER-BASED PATIENT RECORD:* Better Planning and**
Oversight By VA, DOD, and IHS Would
Enhance Health Data Sharing
(GAO-01-459)
(Continued)

record,' the realities of the challenges have led to a scaling back of the initial vision.

As discussed with GAO, a new near-term solution has been developed to address the concerns GAO raises in its report. The new near-term solution uses the GCPR framework, provides a significant amount of information in a sortable format for clinician use, and is funded for fiscal year 2001. This solution will provide current and historical data feeds from CHCS I on selected data types for active duty, retirees, and separated personnel into the GCPR framework and data base for VA access. Current data that DOD will send to VA will include laboratory results, radiology results, outpatient pharmacy, admission, discharge, and transfer messages, and patient demographics. DOD will transmit the current data to VA in near-real-time.. Using a pre-determined schedule, we will extract and transmit historical data feeds.

3



Enclosure (2)

Government Computer-based Patient Record (GCPR) -- Near-Term (FY01) Solution

DOD and VA are working very closely on establishing the appropriate technical architecture to extract electronic health information from the DOD Composite Health Care System (CHCS I) and transmit this information to a shared repository where this medical data is available for use by VA. VA will make this data accessible to VA clinical care providers as part of the veteran's electronic medical record within its Veterans Health Information Systems and Technology Architecture (*VistA)* health information system.

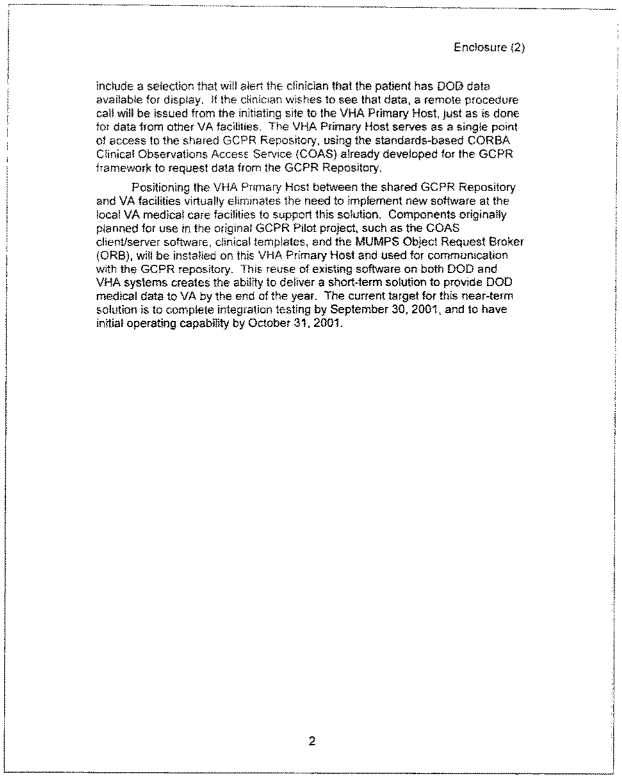
Representatives from DOD, VA, Indian Health Service, Litton PRC, and Science Application International Corporation met the week of March 19, 2001, to evaluate the information exchange architecture alternatives, analyze technical risks/capability tradeoffs, and develop costs and a schedule for the most viable alternatives. The solution agreed to by all parties utilizes the GCPR framework, provides a significant amount of information in a sortable format for use by clinicians, facilitates future IHS participation, and is funded for FY01.

The solution will provide current and historical data feeds from CHCS I to the GCPR Framework Node on selected data types for active duty, retired, and separated service members. Medical data on non-veterans will not be sent as part of this solution. Current data that will be sent in Health Level Seven (HL7) like messages are laboratory results, radiology results, outpatient pharmacy, admission, discharge, and transfer messages, and patient demographics. Current data will be sent in near-real-time transmission from DOD to the GCPR Framework Node for storage in the GCPR Repository. These current data feeds will use existing event triggers within CHCS I to send messages to the shared repository.

Historical medical information will be extracted from CHCS I systems and transmitted to the GCPR Framework Node, for storage in the GCPR Repository, using batch transmission techniques that will facilitate the handling of this bulk information and eliminate possible performance impacts on the existing CHCS I systems.

The GCPR Repository will allow access to medical information during VA care and will also provide for potential future use for aggregate analysis if necessary. While final sizing estimates are incomplete, we do know that this repository of medical data will be large enough to contain medical record information on the approximately 220,000 service members separating each year, in addition to the historical information on separated or retired service members who have had medical data in CHCS I since it became fully operational in the 1990's. Work is in progress to accurately determine initial capacity needed to store data from CHCS I.

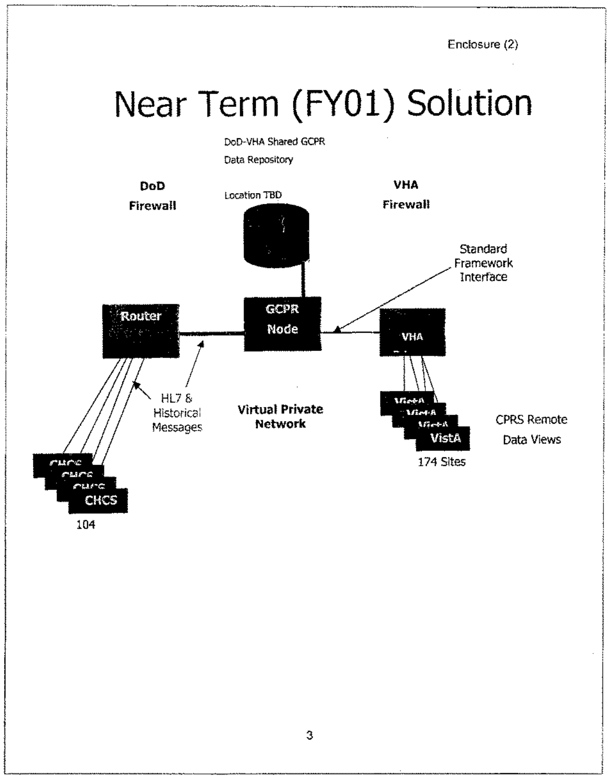
VHA clinical staff who are authorized to view medical records will have access to the DOD data stored in the GCPR Repository by using the *VistA* Computer Patient Record System (CPRS) Remote Data Views application. When a patient with DOD data is selected in CPRS, the CPRS facility list will



Enclosure (2)

include a selection that will alert the clinician that the patient has DOD data available for display. If the clinician wishes to see that data, a remote procedure call will be issued from the initiating site to the VHA Primary Host, just as is done for data from other VA facilities. The VHA Primary Host serves as a single point of access to the shared GCPR Repository, using the standards-based CORBA Clinical Observations Access Service (COAS) already developed for the GCPR framework to request data from the GCPR Repository.

Positioning the VHA Primary Host between the shared GCPR Repository and VA facilities virtually eliminates the need to implement new software at the local VA medical care facilities to support this solution. Components originally planned for use in the original GCPR Pilot project, such as the COAS client/server software, clinical templates, and the MUMPS Object Request Broker (ORB), will be installed on this VHA Primary Host and used for communication with the GCPR repository. This reuse of existing software on both DOD and VHA systems creates the ability to deliver a short-term solution to provide DOD medical data to VA by the end of the year. The current target for this near-term solution is to complete integration testing by September 30, 2001, and to have initial operating capability by October 31, 2001.



Enclosure (2)

Near Term (FY01) Solution

DoD-VHA Shared GCPR
Data Repository

Location TBD

DoD
Firewall

VHA
Firewall

Standard
Framework
Interface

Router

GCPR
Node

VHA

HL7 &
Historical
Messages

Virtual Private
Network

VistA

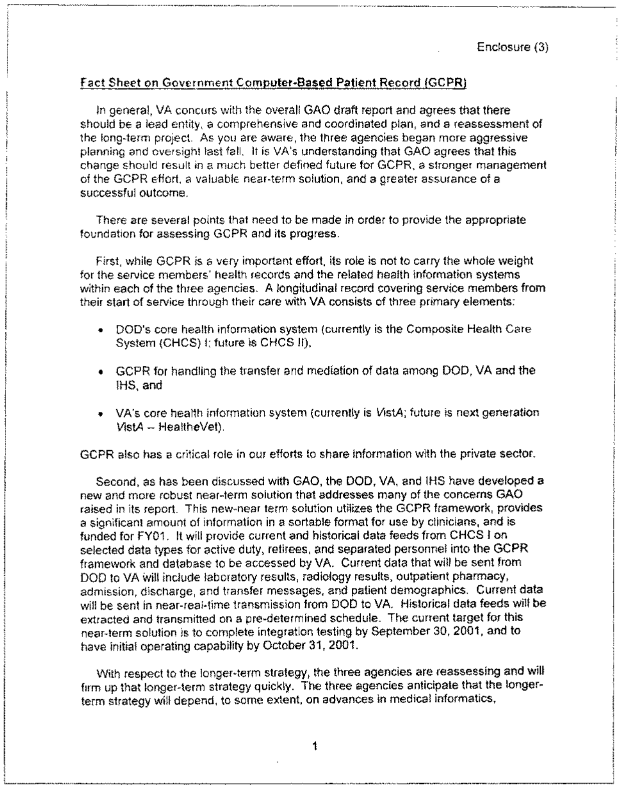
CPRS Remote
Data Views

174 Sites

CHCS

104

3



Enclosure (3)

Fact Sheet on Government Computer-Based Patient Record (GCPR)

In general, VA concurs with the overall GAO draft report and agrees that there should be a lead entity, a comprehensive and coordinated plan, and a reassessment of the long-term project. As you are aware, the three agencies began more aggressive planning and oversight last fall. It is VA's understanding that GAO agrees that this change should result in a much better defined future for GCPR, a stronger management of the GCPR effort, a valuable near-term solution, and a greater assurance of a successful outcome.

There are several points that need to be made in order to provide the appropriate foundation for assessing GCPR and its progress.

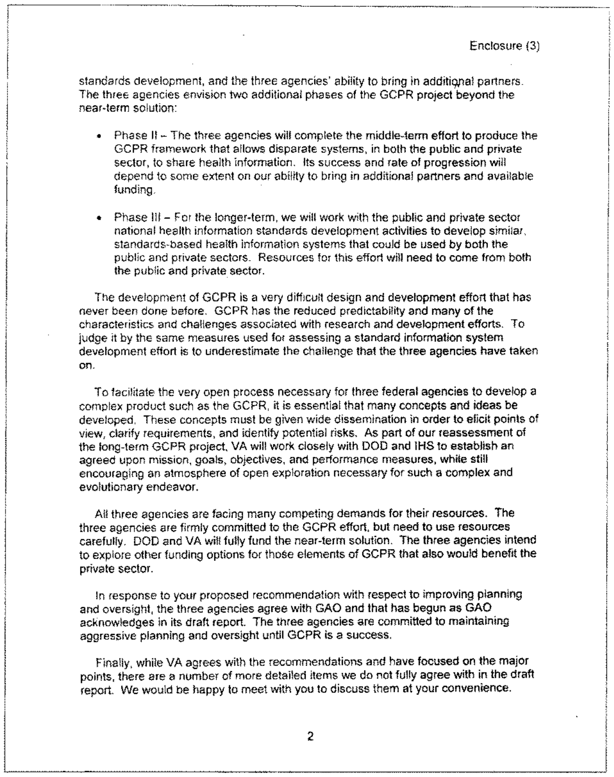
First, while GCPR is a very important effort, its role is not to carry the whole weight for the service members' health records and the related health information systems within each of the three agencies. A longitudinal record covering service members from their start of service through their care with VA consists of three primary elements:

- DOD's core health information system (currently is the Composite Health Care System (CHCS) I; future is CHCS II),
- GCPR for handling the transfer and mediation of data among DOD, VA and the IHS, and
- VA's core health information system (currently is *VistA*; future is next generation *VistA* – HealtheVet).

GCPR also has a critical role in our efforts to share information with the private sector.

Second, as has been discussed with GAO, the DOD, VA, and IHS have developed a new and more robust near-term solution that addresses many of the concerns GAO raised in its report. This new-near term solution utilizes the GCPR framework, provides a significant amount of information in a sortable format for use by clinicians, and is funded for FY01. It will provide current and historical data feeds from CHCS I on selected data types for active duty, retirees, and separated personnel into the GCPR framework and database to be accessed by VA. Current data that will be sent from DOD to VA will include laboratory results, radiology results, outpatient pharmacy, admission, discharge, and transfer messages, and patient demographics. Current data will be sent in near-real-time transmission from DOD to VA. Historical data feeds will be extracted and transmitted on a pre-determined schedule. The current target for this near-term solution is to complete integration testing by September 30, 2001, and to have initial operating capability by October 31, 2001.

With respect to the longer-term strategy, the three agencies are reassessing and will firm up that longer-term strategy quickly. The three agencies anticipate that the longer-term strategy will depend, to some extent, on advances in medical informatics,



Enclosure (3)

standards development, and the three agencies' ability to bring in additional partners. The three agencies envision two additional phases of the GCPR project beyond the near-term solution:

- Phase II – The three agencies will complete the middle-term effort to produce the GCPR framework that allows disparate systems, in both the public and private sector, to share health information. Its success and rate of progression will depend to some extent on our ability to bring in additional partners and available funding.

- Phase III – For the longer-term, we will work with the public and private sector national health information standards development activities to develop similar, standards-based health information systems that could be used by both the public and private sectors. Resources for this effort will need to come from both the public and private sector.

The development of GCPR is a very difficult design and development effort that has never been done before. GCPR has the reduced predictability and many of the characteristics and challenges associated with research and development efforts. To judge it by the same measures used for assessing a standard information system development effort is to underestimate the challenge that the three agencies have taken on.

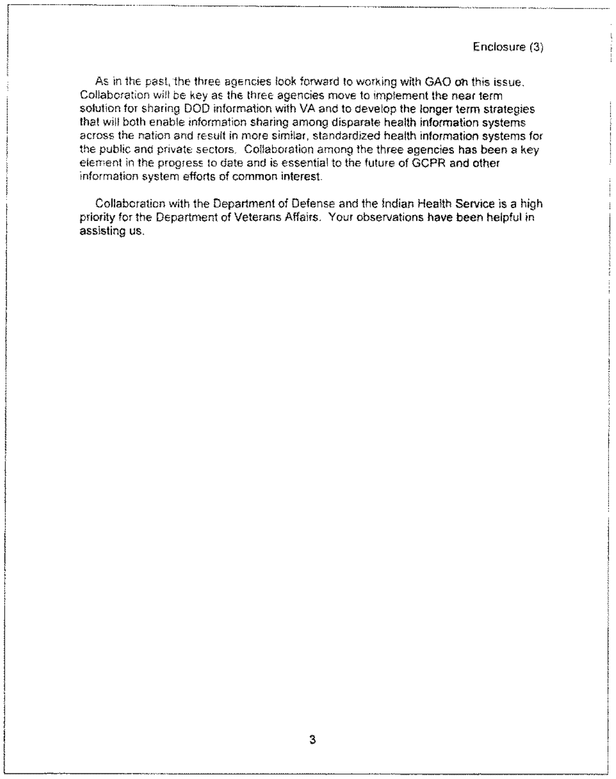
To facilitate the very open process necessary for three federal agencies to develop a complex product such as the GCPR, it is essential that many concepts and ideas be developed. These concepts must be given wide dissemination in order to elicit points of view, clarify requirements, and identify potential risks. As part of our reassessment of the long-term GCPR project, VA will work closely with DOD and IHS to establish an agreed upon mission, goals, objectives, and performance measures, while still encouraging an atmosphere of open exploration necessary for such a complex and evolutionary endeavor.

All three agencies are facing many competing demands for their resources. The three agencies are firmly committed to the GCPR effort, but need to use resources carefully. DOD and VA will fully fund the near-term solution. The three agencies intend to explore other funding options for those elements of GCPR that also would benefit the private sector.

In response to your proposed recommendation with respect to improving planning and oversight, the three agencies agree with GAO and that has begun as GAO acknowledges in its draft report. The three agencies are committed to maintaining aggressive planning and oversight until GCPR is a success.

Finally, while VA agrees with the recommendations and have focused on the major points, there are a number of more detailed items we do not fully agree with in the draft report. We would be happy to meet with you to discuss them at your convenience.

2



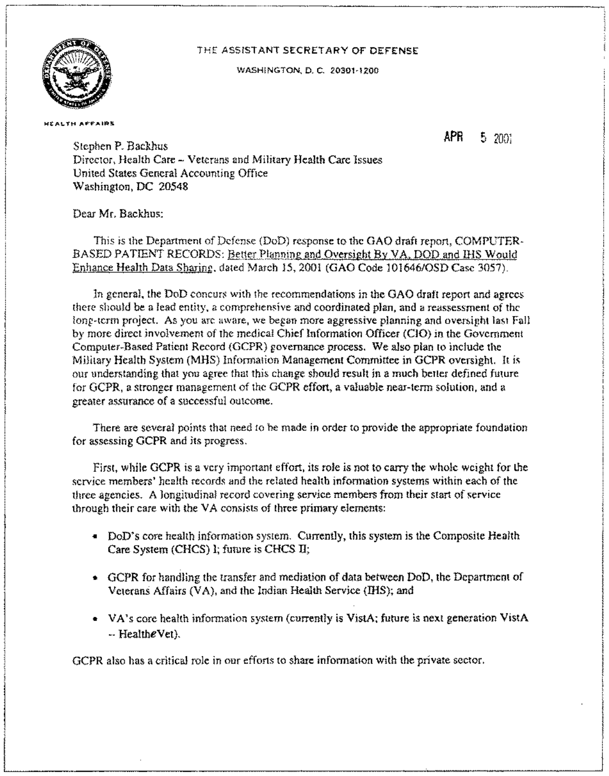
Enclosure (3)

As in the past, the three agencies look forward to working with GAO on this issue. Collaboration will be key as the three agencies move to implement the near term solution for sharing DOD information with VA and to develop the longer term strategies that will both enable information sharing among disparate health information systems across the nation and result in more simliar, standardized health information systems for the public and private sectors. Collaboration among the three agencies has been a key element in the progress to date and is essential to the future of GCPR and other information system efforts of common interest.

Collaboration with the Department of Defense and the Indian Health Service is a high priority for the Department of Veterans Affairs. Your observations have been helpful in assisting us.

3

Appendix III: Comments From the Department of Defense



THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D. C. 20301-1200

HEALTH AFFAIRS

APR 5 2001

Stephen P. Backhus
Director, Health Care – Veterans and Military Health Care Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. Backhus:

This is the Department of Defense (DoD) response to the GAO draft report, COMPUTER-BASED PATIENT RECORDS: Better Planning and Oversight By VA, DOD and IHS Would Enhance Health Data Sharing, dated March 15, 2001 (GAO Code 101646/OSD Case 3057).

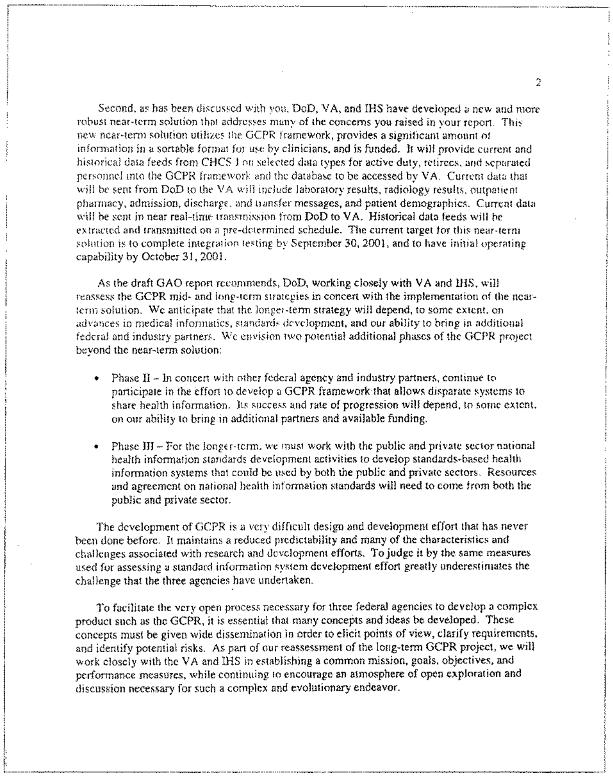
In general, the DoD concurs with the recommendations in the GAO draft report and agrees there should be a lead entity, a comprehensive and coordinated plan, and a reassessment of the long-term project. As you are aware, we began more aggressive planning and oversight last Fall by more direct involvement of the medical Chief Information Officer (CIO) in the Government Computer-Based Patient Record (GCPR) governance process. We also plan to include the Military Health System (MHS) Information Management Committee in GCPR oversight. It is our understanding that you agree that this change should result in a much better defined future for GCPR, a stronger management of the GCPR effort, a valuable near-term solution, and a greater assurance of a successful outcome.

There are several points that need to be made in order to provide the appropriate foundation for assessing GCPR and its progress.

First, while GCPR is a very important effort, its role is not to carry the whole weight for the service members' health records and the related health information systems within each of the three agencies. A longitudinal record covering service members from their start of service through their care with the VA consists of three primary elements:

- DoD's core health information system. Currently, this system is the Composite Health Care System (CHCS) I; future is CHCS II;
- GCPR for handling the transfer and mediation of data between DoD, the Department of Veterans Affairs (VA), and the Indian Health Service (IHS); and
- VA's core health information system (currently is VistA; future is next generation VistA -- Health*e*Vet).

GCPR also has a critical role in our efforts to share information with the private sector.



Second, as has been discussed with you, DoD, VA, and IHS have developed a new and more robust near-term solution that addresses many of the concerns you raised in your report. This new near-term solution utilizes the GCPR framework, provides a significant amount of information in a sortable format for use by clinicians, and is funded. It will provide current and historical data feeds from CHCS I on selected data types for active duty, retirees, and separated personnel into the GCPR framework and the database to be accessed by VA. Current data that will be sent from DoD to the VA will include laboratory results, radiology results, outpatient pharmacy, admission, discharge, and transfer messages, and patient demographics. Current data will be sent in near real-time transmission from DoD to VA. Historical data feeds will be extracted and transmitted on a pre-determined schedule. The current target for this near-term solution is to complete integration testing by September 30, 2001, and to have initial operating capability by October 31, 2001.

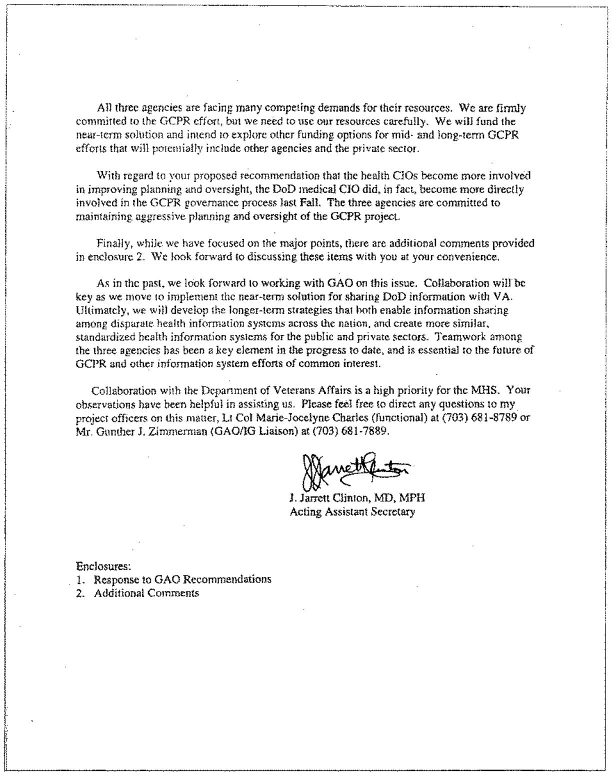
As the draft GAO report recommends, DoD, working closely with VA and IHS, will reassess the GCPR mid- and long-term strategies in concert with the implementation of the near-term solution. We anticipate that the longer-term strategy will depend, to some extent, on advances in medical informatics, standards development, and our ability to bring in additional federal and industry partners. We envision two potential additional phases of the GCPR project beyond the near-term solution:

- Phase II – In concert with other federal agency and industry partners, continue to participate in the effort to develop a GCPR framework that allows disparate systems to share health information. Its success and rate of progression will depend, to some extent, on our ability to bring in additional partners and available funding.

- Phase III – For the longer-term, we must work with the public and private sector national health information standards development activities to develop standards-based health information systems that could be used by both the public and private sectors. Resources and agreement on national health information standards will need to come from both the public and private sector.

The development of GCPR is a very difficult design and development effort that has never been done before. It maintains a reduced predictability and many of the characteristics and challenges associated with research and development efforts. To judge it by the same measures used for assessing a standard information system development effort greatly underestimates the challenge that the three agencies have undertaken.

To facilitate the very open process necessary for three federal agencies to develop a complex product such as the GCPR, it is essential that many concepts and ideas be developed. These concepts must be given wide dissemination in order to elicit points of view, clarify requirements, and identify potential risks. As part of our reassessment of the long-term GCPR project, we will work closely with the VA and IHS in establishing a common mission, goals, objectives, and performance measures, while continuing to encourage an atmosphere of open exploration and discussion necessary for such a complex and evolutionary endeavor.



All three agencies are facing many competing demands for their resources. We are firmly committed to the GCPR effort, but we need to use our resources carefully. We will fund the near-term solution and intend to explore other funding options for mid- and long-term GCPR efforts that will potentially include other agencies and the private sector.

With regard to your proposed recommendation that the health CIOs become more involved in improving planning and oversight, the DoD medical CIO did, in fact, become more directly involved in the GCPR governance process last Fall. The three agencies are committed to maintaining aggressive planning and oversight of the GCPR project.

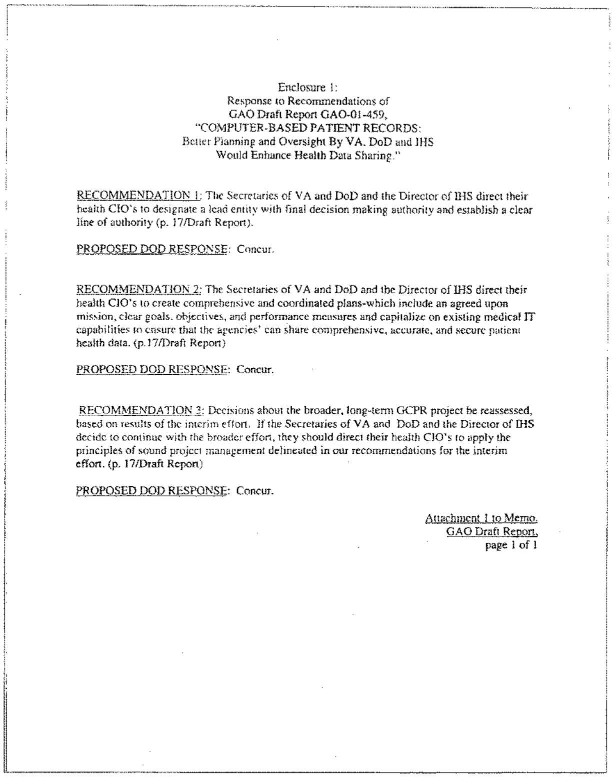
Finally, while we have focused on the major points, there are additional comments provided in enclosure 2. We look forward to discussing these items with you at your convenience.

As in the past, we look forward to working with GAO on this issue. Collaboration will be key as we move to implement the near-term solution for sharing DoD information with VA. Ultimately, we will develop the longer-term strategies that both enable information sharing among disparate health information systems across the nation, and create more similar, standardized health information systems for the public and private sectors. Teamwork among the three agencies has been a key element in the progress to date, and is essential to the future of GCPR and other information system efforts of common interest.

Collaboration with the Department of Veterans Affairs is a high priority for the MHS. Your observations have been helpful in assisting us. Please feel free to direct any questions to my project officers on this matter, Lt Col Marie-Jocelyne Charles (functional) at (703) 681-8789 or Mr. Gunther J. Zimmerman (GAO/IG Liaison) at (703) 681-7889.

J. Jarrett Clinton, MD, MPH
Acting Assistant Secretary

Enclosures:
1. Response to GAO Recommendations
2. Additional Comments



Enclosure 1:
Response to Recommendations of
GAO Draft Report GAO-01-459,
"COMPUTER-BASED PATIENT RECORDS:
Better Planning and Oversight By VA, DoD and IHS
Would Enhance Health Data Sharing."

RECOMMENDATION 1: The Secretaries of VA and DoD and the Director of IHS direct their health CIO's to designate a lead entity with final decision making authority and establish a clear line of authority (p. 17/Draft Report).

PROPOSED DOD RESPONSE: Concur.

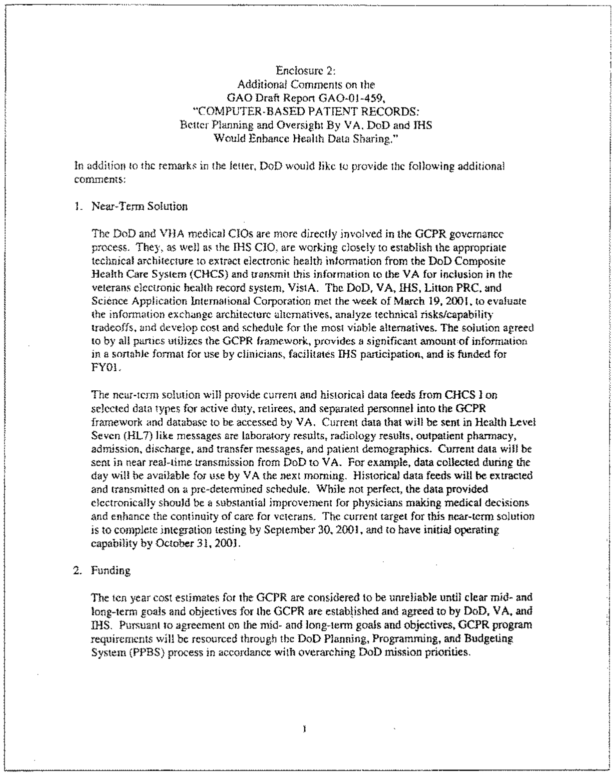
RECOMMENDATION 2: The Secretaries of VA and DoD and the Director of IHS direct their health CIO's to create comprehensive and coordinated plans-which include an agreed upon mission, clear goals, objectives, and performance measures and capitalize on existing medical IT capabilities to ensure that the agencies' can share comprehensive, accurate, and secure patient health data. (p.17/Draft Report)

PROPOSED DOD RESPONSE: Concur.

RECOMMENDATION 3: Decisions about the broader, long-term GCPR project be reassessed, based on results of the interim effort. If the Secretaries of VA and DoD and the Director of IHS decide to continue with the broader effort, they should direct their health CIO's to apply the principles of sound project management delineated in our recommendations for the interim effort. (p. 17/Draft Report)

PROPOSED DOD RESPONSE: Concur.

Attachment 1 to Memo,
GAO Draft Report,
page 1 of 1



Enclosure 2:
Additional Comments on the
GAO Draft Report GAO-01-459,
"COMPUTER-BASED PATIENT RECORDS:
Better Planning and Oversight By VA, DoD and IHS
Would Enhance Health Data Sharing."

In addition to the remarks in the letter, DoD would like to provide the following additional comments:

1. Near-Term Solution

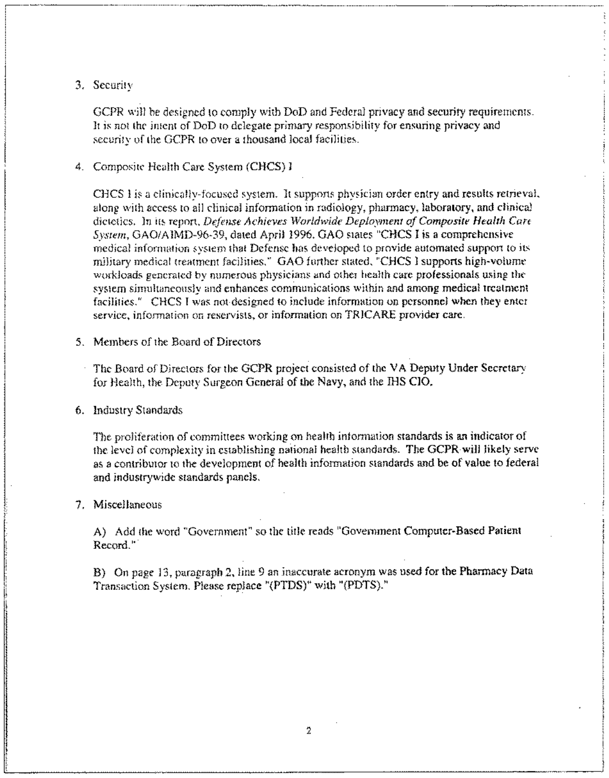
The DoD and VHA medical CIOs are more directly involved in the GCPR governance process. They, as well as the IHS CIO, are working closely to establish the appropriate technical architecture to extract electronic health information from the DoD Composite Health Care System (CHCS) and transmit this information to the VA for inclusion in the veterans electronic health record system, VistA. The DoD, VA, IHS, Litton PRC, and Science Application International Corporation met the week of March 19, 2001, to evaluate the information exchange architecture alternatives, analyze technical risks/capability tradeoffs, and develop cost and schedule for the most viable alternatives. The solution agreed to by all parties utilizes the GCPR framework, provides a significant amount of information in a sortable format for use by clinicians, facilitates IHS participation, and is funded for FY01.

The near-term solution will provide current and historical data feeds from CHCS I on selected data types for active duty, retirees, and separated personnel into the GCPR framework and database to be accessed by VA. Current data that will be sent in Health Level Seven (HL7) like messages are laboratory results, radiology results, outpatient pharmacy, admission, discharge, and transfer messages, and patient demographics. Current data will be sent in near real-time transmission from DoD to VA. For example, data collected during the day will be available for use by VA the next morning. Historical data feeds will be extracted and transmitted on a pre-determined schedule. While not perfect, the data provided electronically should be a substantial improvement for physicians making medical decisions and enhance the continuity of care for veterans. The current target for this near-term solution is to complete integration testing by September 30, 2001, and to have initial operating capability by October 31, 2001.

2. Funding

The ten year cost estimates for the GCPR are considered to be unreliable until clear mid- and long-term goals and objectives for the GCPR are established and agreed to by DoD, VA, and IHS. Pursuant to agreement on the mid- and long-term goals and objectives, GCPR program requirements will be resourced through the DoD Planning, Programming, and Budgeting System (PPBS) process in accordance with overarching DoD mission priorities.

1



3. Security

GCPR will be designed to comply with DoD and Federal privacy and security requirements. It is not the intent of DoD to delegate primary responsibility for ensuring privacy and security of the GCPR to over a thousand local facilities.

4. Composite Health Care System (CHCS) I

CHCS I is a clinically-focused system. It supports physician order entry and results retrieval, along with access to all clinical information in radiology, pharmacy, laboratory, and clinical dietetics. In its report, *Defense Achieves Worldwide Deployment of Composite Health Care System*, GAO/AIMD-96-39, dated April 1996. GAO states "CHCS I is a comprehensive medical information system that Defense has developed to provide automated support to its military medical treatment facilities." GAO further stated, "CHCS I supports high-volume workloads generated by numerous physicians and other health care professionals using the system simultaneously and enhances communications within and among medical treatment facilities." CHCS I was not designed to include information on personnel when they enter service, information on reservists, or information on TRICARE provider care.

5. Members of the Board of Directors

The Board of Directors for the GCPR project consisted of the VA Deputy Under Secretary for Health, the Deputy Surgeon General of the Navy, and the IHS CIO.

6. Industry Standards

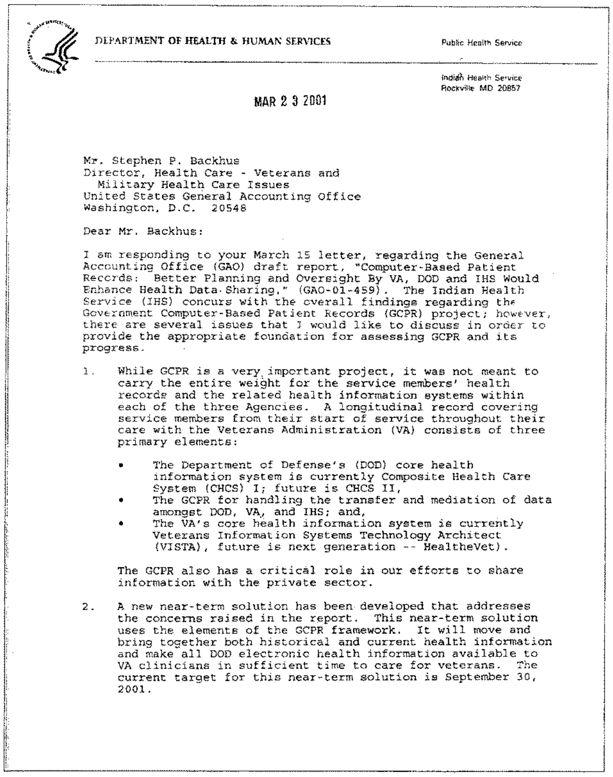
The proliferation of committees working on health information standards is an indicator of the level of complexity in establishing national health standards. The GCPR will likely serve as a contributor to the development of health information standards and be of value to federal and industrywide standards panels.

7. Miscellaneous

A) Add the word "Government" so the title reads "Government Computer-Based Patient Record."

B) On page 13, paragraph 2, line 9 an inaccurate acronym was used for the Pharmacy Data Transaction System. Please replace "(PTDS)" with "(PDTS)."

Appendix IV: Comments From the Indian Health Service



DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Indian Health Service
Rockville MD 20857

MAR 2 9 2001

Mr. Stephen P. Backhus
Director, Health Care - Veterans and
Military Health Care Issues
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Backhus:

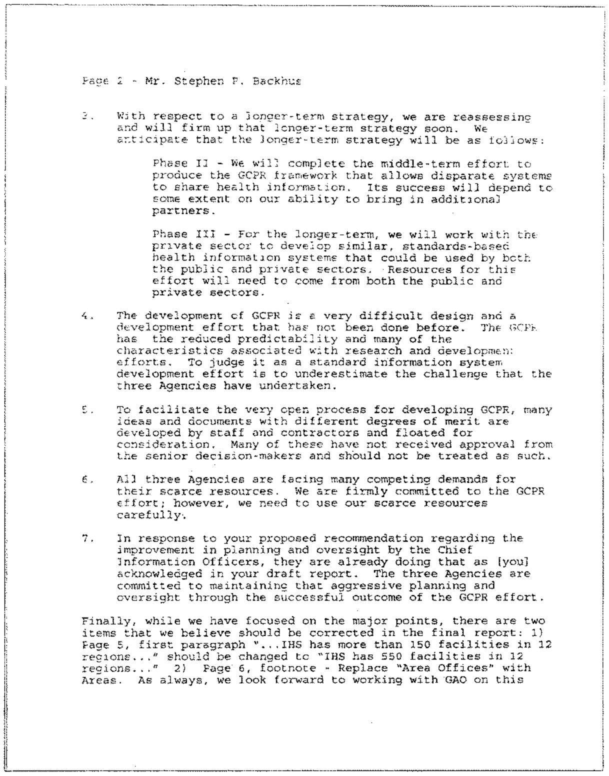
I am responding to your March 15 letter, regarding the General Accounting Office (GAO) draft report, "Computer-Based Patient Records: Better Planning and Oversight By VA, DOD and IHS Would Enhance Health Data Sharing," (GAO-01-459). The Indian Health Service (IHS) concurs with the overall findings regarding the Government Computer-Based Patient Records (GCPR) project; however, there are several issues that I would like to discuss in order to provide the appropriate foundation for assessing GCPR and its progress.

1. While GCPR is a very important project, it was not meant to carry the entire weight for the service members' health records and the related health information systems within each of the three Agencies. A longitudinal record covering service members from their start of service throughout their care with the Veterans Administration (VA) consists of three primary elements:

   - The Department of Defense's (DOD) core health information system is currently Composite Health Care System (CHCS) I; future is CHCS II,
   - The GCPR for handling the transfer and mediation of data amongst DOD, VA, and IHS; and,
   - The VA's core health information system is currently Veterans Information Systems Technology Architect (VISTA), future is next generation -- HealtheVet).

   The GCPR also has a critical role in our efforts to share information with the private sector.

2. A new near-term solution has been developed that addresses the concerns raised in the report. This near-term solution uses the elements of the GCPR framework. It will move and bring together both historical and current health information and make all DOD electronic health information available to VA clinicians in sufficient time to care for veterans. The current target for this near-term solution is September 30, 2001.



Page 2 - Mr. Stephen P. Backhus

3. With respect to a longer-term strategy, we are reassessing and will firm up that longer-term strategy soon. We anticipate that the longer-term strategy will be as follows:

   Phase II - We will complete the middle-term effort to produce the GCPR framework that allows disparate systems to share health information. Its success will depend to some extent on our ability to bring in additional partners.

   Phase III - For the longer-term, we will work with the private sector to develop similar, standards-based health information systems that could be used by both the public and private sectors. Resources for this effort will need to come from both the public and private sectors.

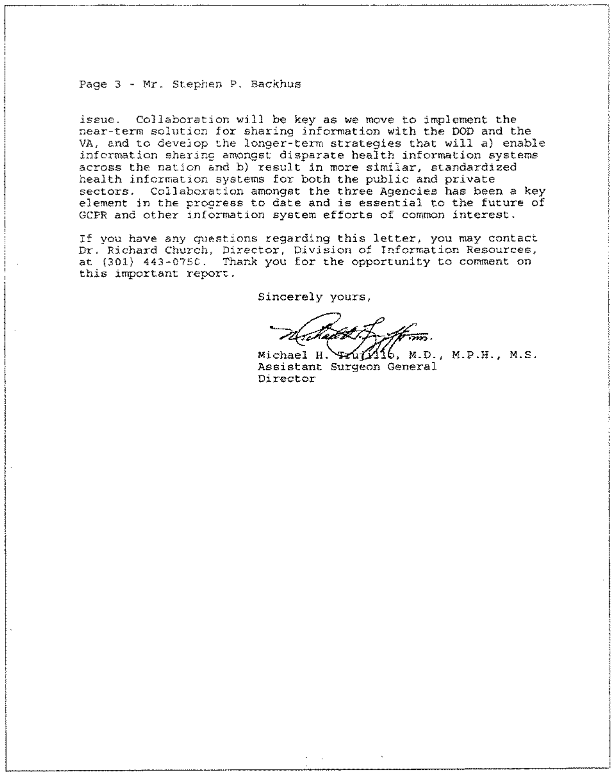
4. The development of GCPR is a very difficult design and a development effort that has not been done before. The GCPR has the reduced predictability and many of the characteristics associated with research and development efforts. To judge it as a standard information system development effort is to underestimate the challenge that the three Agencies have undertaken.

5. To facilitate the very open process for developing GCPR, many ideas and documents with different degrees of merit are developed by staff and contractors and floated for consideration. Many of these have not received approval from the senior decision-makers and should not be treated as such.

6. All three Agencies are facing many competing demands for their scarce resources. We are firmly committed to the GCPR effort; however, we need to use our scarce resources carefully.

7. In response to your proposed recommendation regarding the improvement in planning and oversight by the Chief Information Officers, they are already doing that as [you] acknowledged in your draft report. The three Agencies are committed to maintaining that aggressive planning and oversight through the successful outcome of the GCPR effort.

Finally, while we have focused on the major points, there are two items that we believe should be corrected in the final report: 1) Page 5, first paragraph "...IHS has more than 150 facilities in 12 regions..." should be changed to "IHS has 550 facilities in 12 regions..." 2) Page 6, footnote - Replace "Area Offices" with Areas. As always, we look forward to working with GAO on this



Page 3 - Mr. Stephen P. Backhus

issue. Collaboration will be key as we move to implement the near-term solution for sharing information with the DOD and the VA, and to develop the longer-term strategies that will a) enable information sharing amongst disparate health information systems across the nation and b) result in more similar, standardized health information systems for both the public and private sectors. Collaboration amongst the three Agencies has been a key element in the progress to date and is essential to the future of GCPR and other information system efforts of common interest.

If you have any questions regarding this letter, you may contact Dr. Richard Church, Director, Division of Information Resources, at (301) 443-0750. Thank you for the opportunity to comment on this important report.

Sincerely yours,

Michael H. Trujillo, M.D., M.P.H., M.S.
Assistant Surgeon General
Director

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Ann Calvaresi-Barr (202) 512-6986
Keith Steck (202) 512-9166

Staff Acknowledgments

In addition to those named above, the following staff made key contributions to this report: Tonia Johnson, Helen Lew, William Lew, Valerie Melvin, Karen Sloan, and Thomas Yatsco.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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

Info@www.gao.gov

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

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

PRINTED ON ♲ RECYCLED PAPER

VA'S INFORMATION 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

March 13, 2002

Mr. Chairman and Members of the Subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs (VA) Automated Information System (AIS) security program. Our work continues to identify serious Department-wide weaknesses in AIS security. As a result, we concluded in our audit of VA's Consolidated Financial Statements for Fiscal Years 2001 and 2000 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 April 4, 2001 testimony to this Subcommittee, we completed our first annual national audit of VA's information security program with a report issued on October 24, 2001. A second annual audit is currently in process. The audit has begun with a review of VBA's information security and in the weeks ahead will include the remainder of the Department. Our current audit work in VBA shows that significant information security vulnerabilities continue to place the Department at risk of:

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

In order to begin to effectively address its information security program weaknesses, we recommended in our October report that VA take the following actions:

- Establish centralized information security budgetary control for all information technology initiatives.
- Expedite actions to: (1) fill information security officer positions; (2) implement enterprise-wide intrusion detection, antivirus detection, and remediation plans; and (3) upgrade external electronic connections.

- Complete vulnerability assessments for all VA systems to address information security weaknesses exploited during our penetration testing.
- Direct Administration CIOs to: (1) address information system security vulnerabilities identified by the audit; (2) implement a VA-wide vulnerability assessment process; and, (3) enhance security awareness and highlight the need to assure compliance with existing VA information security policy, procedures, and controls.
- Assure that operation of all uncertified Independent Internet Gateways is discontinued.
- Establish minimum acceptable enterprise-wide security configuration standards involving desktop computers used in VA's automated systems, and require that Administration CIOs complete necessary upgrades/replacements.
- Centralize information security oversight and control over VA Central Office network operations.
- Eliminate physical security weaknesses identified by the audit at VA data centers and field facilities.
- Assure that VA's planned information security remediation actions address the areas of non-compliance with GISRA and OMB Circular A-130, Appendix III.
- Update VA's Critical Infrastructure Protection Plan to reflect current planned milestone dates for completing security initiatives and include measures to implement the GISRA requirements.

Much work remains to be done to implement necessary security enhancements to properly secure VA's systems and sensitive data. The Department's CIO (Assistant Secretary for Information and Technology), the individual Administrations, and other VA elements have responded positively to the audit findings and agreed to take various corrective actions. However, our current audit found that the Veterans Benefits Administration (VBA) did not complete some agreed to corrective actions at its Data Centers and Regional Offices. Our audit found that many of the information system security weaknesses reported in our 2001 audit remain unresolved, and additional security weaknesses were identified. We have advised VBA top management that this situation requires immediate corrective action to assure protection of critical Department electronic infrastructure resources and continuity of operations and delivery of services to the nation's veterans.

Our current audit work also shows that additional action is needed to prioritize completion of key security initiatives, establish timelines for completion, and secure necessary budget resources.

Key Department Security Remediation Actions Need To Be Prioritized And Completed In The Next Year

Our review of the Department's planning documents found that completion of necessary remediation actions has not been prioritized with timeline start and completion dates. We believe that this is a necessary step in the planning process to help assure that those most serious security weakness areas are targeted for completion first, based on the level of risk to Department operations and assets. Prioritization of the Department's security remediation actions is important to assure that resource expenditures are properly focused and provide the maximum opportunity to strengthen the Department-wide security posture in the near term (next 12 months). This is also important because our discussion with officials in the Department's Office of Cyber Security (OCS) indicated concern that budget resources may not be available to complete all necessary remediation actions.

Based on our results and discussion with officials in the OCS, we identified the following key security weakness areas that should be considered for priority completion in the next year. Some of these weakness areas require enforcement of existing Department policy and Governmental regulations and others require new hardware, software, and or contractor support to correct.

- **Intrusion Detection Systems (IDS)**
- **Infrastructure Protection**
- **Data Center Contingency Planning**
- **Certification and Accreditation of Systems**
- **Upgrade/Terminate External Connections**
- **Configuration Management**
- **Application Program/Operating System Change Controls**
- **Physical Access Controls (access to computer rooms)**

We believe that correction of these key information security weakness areas will provide the Department with the opportunity to better strengthen its national security posture in the short term and reduce the vulnerability of the Department's programs and sensitive data to potential destruction, manipulation, and inappropriate disclosure. Completion of these actions will also help the Department address existing information security control weaknesses that contribute to the designation of information security as a Department material weakness area under FMFIA. In response to our findings, the Department has identified these key information security weakness areas in its GISRA remediation action plan for priority corrective action in the next 12 months.

Annual Department Security Expenditure Requirements Are Significant

Once these security initiatives are prioritized for completion, necessary budget resources will need to be secured. We recognize that the Department faces a significant challenge to implement necessary security remediation actions that are estimated to require $804 million (Fiscal Years 2002-2006). This represents substantial budget resource expenditures above those levels funded in past years. In Fiscal Year (FY) 2001, about $17 million was expended for cyber security program initiatives in support of OCS efforts to strengthen the Department's national security posture. During FY 2002, about $21.4 million is budgeted for OCS directed security program initiatives. This level of funding support is significantly below the $93.2 million budget requirements identified in the Department's Cyber Security Capital Investment Proposal. In FY 2003, the level of projected security funding requirements increases to over $132 million. In addition to OCS directed security program expenditures, each of the Department Administration's budgets also includes security program expenditures that address various security initiatives. For FY 2002, these planned expenditures are significant and total an estimated $34.4 million.

During our current audit, we will be reviewing individual Administration security expenditures to assess the value of those expenditures in light of VA's national security priorities.

Conclusion

VA has been slow to implement a risk management framework to proactively identify information security related risks and implement corrective action. We evaluated VA compliance with requirements of GISRA and OMB Circular A-130, Appendix III. We found that VA has complied with provisions relating to organization, planning, and risk assessment, but additional effort is needed to effectively implement required agency wide security controls, monitoring, and assessment.

The Department has established a VA-wide security plan, policies, procedures, and guidelines as required by the Act. In addition, the Department has established performance measures for executive level managers in all Administrations. The establishment of performance measures for other managers is in process and may require changes to the management/labor agreements before completion.

VA has not effectively implemented planned security measures and has not assured compliance with established policies, procedures, and control requirements. Based on the audit work completed and in process, VA is not in compliance with the GISRA requirements. To attain compliance with the Act, VA needs to:

- Improve information security awareness training for all VA employees.
- Fully implement the Critical Incident Response Capability.
- Assure that the Critical Infrastructure Protection Program is implemented and addresses GISRA requirements.

- Complete risk assessments of all VA systems.

The Department should also identify information security best practices both within and outside of VA that can be used to help implement the requirements of the Act. As an example, we found that one of VBA's data centers had established a hardened security screening process for all electronic information entering the facility. This process, which should be implemented system wide, limits access to VA systems, examines e-mail for malicious code, and prohibits access by unauthorized persons.

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

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

March 13, 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;
- Cyber Security program;
- VBA's VETSNET program;
- VHA's Decision Support System; and,
- VHA's Government Computer-Based Patient Records Program.

On April 4, 2001, the Secretary appeared before this committee and gave you his personal commitment to reform the way VA uses information technology. He committed to:

- Developing a comprehensive integrated Enterprise Architecture that would end "stove-pipe" system design and incompatible system development;
- Ensuring that networks and systems we depend upon are secure and available;
- Conducting an independent audit of VETSNET to enable us to chart the proper course for future modernization of our Compensation & Pensions System; and,
- Standardizing the use of the Decision Support System (DSS) in VHA to support day-to-day business and management decision processes.

I am pleased to report to you today that it is no longer "business as usual" in VA's information technology program. With respect to Enterprise Architecture (EA), the Department has selected a methodology known as the Zachman Framework to develop and maintain its One-VA EA. This methodology requires us to define all aspects of the VA Enterprise from a business process, data, technical, location, personnel, and requirements perspective. This has been accomplished. The next step in implementing the Zachman methodology is to define all functions related to each business process and identify associated data elements. Once identified, duplication of function and inconsistency in data definition can be identified. The hard job then follows to de-conflict the data definitions and resolve duplicative implementations of the same business function. This work is underway. Concurrent with reconciling business functions and data definitions, we have developed a technical implementation model for the future VA Information Technology (IT) Enterprise and are completing the development of a set of technical standards that will apply to all IT projects. Some of these standards will be based on open system commercial standards and some of these standards will be based on individual products for those cases where industry standards are immature or incomplete.

Companies in the private sector that have successfully modernized their IT enterprises have taken a two-pronged approach to their modernization. First they modernized their IT infrastructure to provide a network and computing environment capable of implementing re-engineered business processes. In parallel, they re-engineered their business processes, modernized the IT used to implement those processes, and finally implemented the IT on the modern, high performance, cost effective infrastructure. These commercial best practices are part of our overall strategy. Enterprise Architecture imposes a discipline on how we manage and implement our IT programs. Implementing these disciplines will be accomplished in the near term; however, completing the Zachman Framework for the entire VA enterprise will take several years and will require modernization of several of our major IT systems such as VistA.

Specific progress since the last hearing follows:

- The Department of Veterans Affairs "Enterprise Architecture: Strategy, Governance & Implementation" was approved in September 2001.
- The Information Technology Board (ITB), which is a critical element of the Enterprise Architecture Governance, was established in October 2001.
- VA's ITB has chartered an Enterprise Architecture Council (EAC), and an Enterprise Architecture Working Group has been established.
- An Acting Chief Architect has been appointed. We are in the process of establishing and recruiting for a VA Chief Architect (SES level); and a program-staffing plan has been developed.
- The top-level definition of the VA enterprise has been completed.
- A technical model for the implementation of new IT projects has been defined.
- A comprehensive change in how we oversee the management of our IT Projects has recently been approved. This new oversight process will

ensure that all new IT projects are developed in compliance with the Enterprise Architecture.

- A draft Enterprise Architecture Implementation Plan is under final review by my staff and will be approved by no later than 30 April 2002.

With respect to ensuring that the networks and systems we depend upon are secure and available, Cyber Security is another issue that has the Secretary's highest priority. In order to effectively secure our networked information, we must completely understand the topology of our data network. Our current 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. Further, our current network infrastructure will not support the modernization of our enterprise as previously discussed. 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 this project in concept. The detailed Business Case Analysis, Cost Benefit Analysis, Return on Investment Analysis, and Analysis of Alternatives are being developed. I anticipate these analyses will show 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;
- Remain within the current data network budget; and,
- Be accomplished within the scope of the existing FTS2001 telecommunications contract managed by GSA.

As Secretary Principi stated in his April 4, 2001 testimony, he takes the privacy and security of the information VA collects on our veterans very seriously. Since the last hearing, our Office of Cyber Security has conducted a review of the Department's security posture, paying particular attention to the findings of our Office of Inspector General (OIG) and the General Accounting Office (GAO). As a result of this review, we have established Department-wide priorities for securing VA's computing enterprise. Our first priority is securing VA's boundary against external attack. An Enterprise Cyber Security project, approved for project initiation by VA's Strategic Management Council in February, was the first step in meeting this priority.

This project will coincide with the previously discussed data network project. As we transition to a performance-based network, we will collapse the total number of gateways to external networks to a manageable number while providing significantly increased security protections at these gateways. Design and implementation of this standardized architecture and configuration will better protect VA's information systems and internal critical information repositories from external and internal attack. This and our data network project are key components of our approach to implementing a secure Enterprise Architecture and correcting Cyber Security deficiencies noted by our OIG and the GAO.

Other major improvements in our Cyber Security posture include:

- Deployment of anti-virus software across the entire Department;
- Implementation of a VA-wide firewall policy to protect the boundaries of our enterprise from external attack;
- Development of an acquisition strategy to enhance VA's existing central incident response capabilities, thereby ensuring immediate and effective action to counter such threats as the recent Code Red virus attack;
- Development of a comprehensive Certification and Accreditation policy to ensure that IT systems undergo a rigorous security review prior to being authorized to process sensitive information; and
- Deployment of several intrusion detection system pilot projects, which will serve as components of the Enterprise Cyber Security Infrastructure Project, to detect when external sources are attempting to intrude our networks so that proper defensive measures can be taken to protect the confidentiality of veteran data.

Since completing the GISRA self-assessment survey last August, the Department has aggressively pursued remediation of its reported information technology security deficiencies. Remediation of many of these deficiencies has increased our compliance with security requirements considered essential in ensuring data integrity, confidentiality, and sensitivity.

Concerning VETSNET, as you are aware, VBA embarked on a path to modernize and integrate IT used to support all of their business lines in the mid 1990s; however, they embarked on this path without the benefit of creating an Enterprise Architecture with its associated disciplines. When this "grand design" was found to be too hard to execute in the late 1990s, VETSNET became the name applied to the development and modernization of IT used to support the Compensation & Pension (C&P) program. VETSNET became a set of independently developed applications that, when fully fielded, would replace the Benefits Delivery Network (BDN). Many of these VETSNET applications have been fielded. Development activities remain on two applications required to replace BDN.

This past summer, Secretary Principi directed an independent audit of VETSNET to determine if the entire collection of VETSNET applications would be capable of operating under a full workload if deployed in all of VBA's Regional Offices (ROs). This audit examined the overall architecture of VETSNET and included a set of stress tests to determine if the system could perform as required. The results of this audit determined that the system would be capable of performing acceptably, in a fully loaded environment, once several changes are made to the system. This audit did not include a comprehensive set of functional tests to determine if each function performed as designed.

As a result of this audit, I directed VBA's CIO to develop a comprehensive plan to bring VETSNET into compliance with the Enterprise Architecture to include completing the two remaining VETSNET, or C&P Replacement, applications; implementing the changes recommended from the independent audit; performing detailed functional testing of all VETSNET applications; and conducting a comprehensive stress test to ensure all changes are implemented correctly. FY2003 and FY2004 funding will be used to complete this effort. I anticipate these actions will be completed in April 2004. Actual deployment of VETSNET (C&P Replacement) will be determined as a function of when VBA can afford to insert a new system into the ROs, with the companion learning curve, such that the impact on working off backlogged claims can be effectively managed.

I know this is a very sensitive issue and I will personally oversee progress to ensure VETSNET meets the projected time line. Should this effort proceed with the same problems of its past, I will recommend to the Secretary that the effort be terminated.

With respect to the Decision Support System (DSS), we have made significant strides to improve data quality and access. Combining clinical and financial information from existing data systems into an integrated database to support informed decision-making, DSS serves all VA Medical Centers and about 800 Outpatient Clinics. Not only does the system continue to provide critical data for making informed decisions for planning, programming and budgeting, DSS also aids in patient care process improvement and quality control.

A DSS Steering Committee, comprised of field representatives and chaired by a Veterans Integrated Service Network (VISN) Director, serves as VHA's advisory body to ensure field requirements are identified and considered as functional upgrades. Further, this steering committee works to achieve standard operation of DSS across all of VHA.

Much progress has been made in achieving VHA-wide standardization in the way DSS is utilized; however, this is still work in progress that is being addressed through improved staff training. We have identified numerous Centers of Excellence for DSS application that will impart best practices across all of VHA.

I recently conducted a post implementation review of DSS. During that review, I directed VHA's CIO to develop a proposal for modernizing DSS to address several noted deficiencies for consideration in the FY2004 budget submission. DSS was developed in late 1980s technology and is therefore very expensive to operate, maintain and implement new functions identified by the DSS Steering Committee. Further, since DSS was developed prior to the definition of today's cyber security requirements, DSS was not designed with the proper level of cyber security protection. Considering all of these factors, it is worth developing a Business Case, performing an Analysis of Alternatives and determining the possible return on investment for a potential FY2004 modernization project.

With respect to the Government Computer Patient Records (GCPR) program, we have re-baselined and re-scoped the program to address issues identified in a 2001 GAO report. The re-baselined GCPR program uses a VA application called the Computer Patient Record System (CPRS) as a fundamental building block. CPRS enables a clinician to access clinical data from any VA health facility. GCPR is a database that receives DoD clinical data (but not physician notes). CPRS is the application that will enable VA to import clinical data from the GCPR database in addition to clinical data available within VA as previously described. GCPR is in the final stages of field-testing. As part of the test program, DoD has completed transmitting health information on approximately 3.7 million records on separated service members to GCPR (note: a separated service member may have more than one record if treated at more than one military heath facility). Within the next few weeks, I will chair a review of the test results to determine whether or not the first phase of GCPR is ready for deployment. Future investment in GCPR will enhance functionality based on clinician feedback once operational.

This implementation of GCPR addresses only part of the ultimate solution of medical information sharing with DoD. We are currently working closely with DoD to determine the correct path for the future. We need to address matters of data standardization, technology sharing, and the establishment of interoperable data interfaces.

Mr. Chairman, I am very concerned about two other areas in addition to what I have presented to you today.

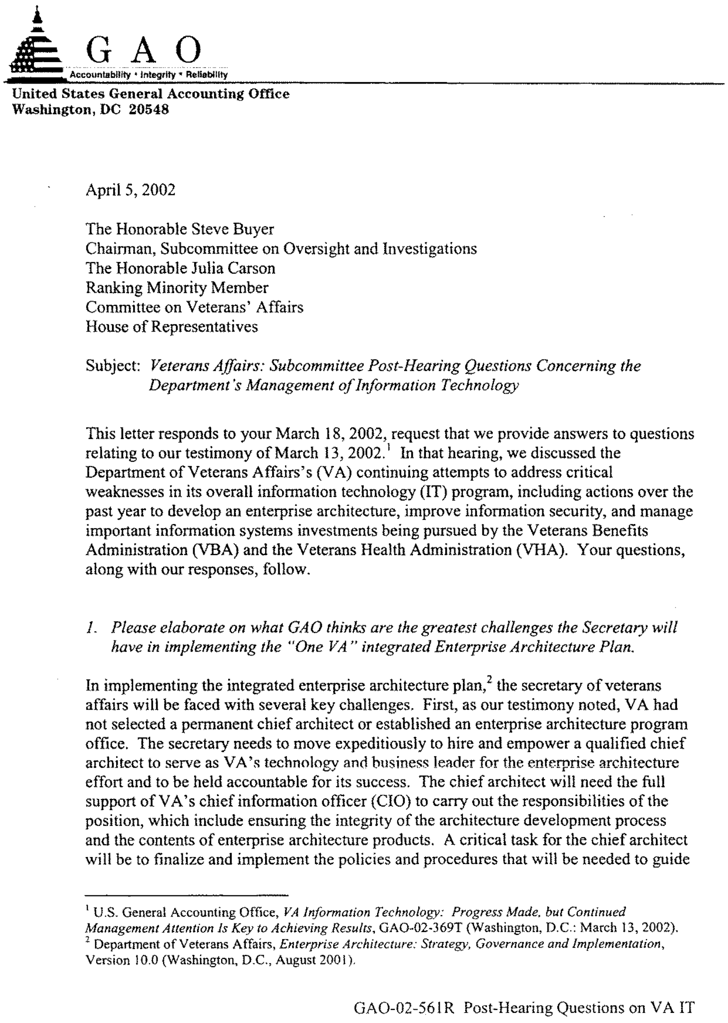
- First, we need to reverse the trend in IT spending in two different areas. Our overall IT budget continues to grow. Even more troubling is the sustainment costs to operate and maintain in-service IT systems as a percentage of the overall budget. For example, 62% of our current FY 2002 budget is earmarked for sustainment. As the current systems continue to age, we can expect the percentage of our IT dollars that we spend for maintaining the current state to increase dramatically. As we formulate the IT budget for FY2004, we will develop a five-year strategy to reverse these two trends of IT spending.
- Second, just like other agencies, our IT workforce is aging, with a large percentage nearing retirement. To address this issue, I have launched an aggressive IT Workforce Initiative to develop and implement a plan for evolving the workforce, recruiting new people, training current employees with modern skills, and managing workforce sustainment and succession. In addition to the business and technical elements of the Enterprise Architecture, this workforce initiative will complete the last critical element of the Enterprise Architecture.

I hope I have provided some insight as to why it is no longer "business as usual" at VA. I believe these efforts demonstrate our very strong commitment, at all levels, to building an effective information technology program for the long-term. I also hope to establish confidence that we will be successful in implementing a comprehensive, coordinated, and efficient IT program within the Department. 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.

WRITTEN COMMITTEE QUESTIONS AND THEIR RESPONSES

CHAIRMAN BUYER TO GENERAL ACCOUNTING OFFICE



GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

April 5, 2002

The Honorable Steve Buyer
Chairman, Subcommittee on Oversight and Investigations
The Honorable Julia Carson
Ranking Minority Member
Committee on Veterans' Affairs
House of Representatives

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

This letter responds to your March 18, 2002, request that we provide answers to questions relating to our testimony of March 13, 2002.[1] In that hearing, we discussed the Department of Veterans Affairs's (VA) continuing attempts to address critical weaknesses in its overall information technology (IT) program, including actions over the past year to develop an enterprise architecture, improve information security, and manage important information systems investments being pursued by the Veterans Benefits Administration (VBA) and the Veterans Health Administration (VHA). Your questions, along with our responses, follow.

1. *Please elaborate on what GAO thinks are the greatest challenges the Secretary will have in implementing the "One VA" integrated Enterprise Architecture Plan.*

In implementing the integrated enterprise architecture plan,[2] the secretary of veterans affairs will be faced with several key challenges. First, as our testimony noted, VA had not selected a permanent chief architect or established an enterprise architecture program office. The secretary needs to move expeditiously to hire and empower a qualified chief architect to serve as VA's technology and business leader for the enterprise architecture effort and to be held accountable for its success. The chief architect will need the full support of VA's chief information officer (CIO) to carry out the responsibilities of the position, which include ensuring the integrity of the architecture development process and the contents of enterprise architecture products. A critical task for the chief architect will be to finalize and implement the policies and procedures that will be needed to guide

[1] U.S. General Accounting Office, *VA Information Technology: Progress Made, but Continued Management Attention Is Key to Achieving Results*, GAO-02-369T (Washington, D.C.: March 13, 2002).
[2] Department of Veterans Affairs, *Enterprise Architecture: Strategy, Governance and Implementation*, Version 10.0 (Washington, D.C., August 2001).

the department in establishing its enterprise architecture. Further, VA must establish an enterprise architecture program management office to support the chief architect in managing, monitoring, and controlling the development, implementation, and maintenance of the enterprise architecture.

A second major challenge will be successfully translating the contents of the integrated enterprise architecture plan into an effective enterprise architecture program. VA's enterprise architecture plan spells out how the department intends to define, implement, and maintain its enterprise architecture to support program and business processes. Successful implementation of the enterprise architecture process is an agencywide endeavor requiring effective management, allocation of resources, continuity, and coordination. Agency business line executives must work closely with the architecture team to produce a description of the agency's operations, a vision for the future, and an investment and technology strategy for accomplishing defined goals.

Third, to effectively plan and implement its enterprise architecture program, the secretary needs the continued commitment and involvement of VA's senior business and technical executives. For large, complex agencies such as VA, developing, implementing, and managing enterprise architectures can be multiyear efforts. As such, clear and continual communications about architecture plans, actions, and progress are essential for keeping relevant senior executives, business units, and stakeholders informed and supportive of the initiative. To this end, the secretary must have an effective marketing strategy and communications plan to provide information and direction about its enterprise architecture activities to its internal and external stakeholders.

Finally, the secretary must make certain that VA successfully integrates enterprise architecture with enterprise engineering and program management, and with VA's capital planning and investment cycle. This integration can provide VA with the proactive management necessary to focus on ensuring that investment management and systems development and acquisition are closely linked with the enterprise architecture processes. It can also help VA effectively and efficiently change the enterprise over time by incorporating new business processes, new technology, and new capabilities, as well as maintaining and disposing of existing elements of its enterprise. Properly synchronizing these processes should enable VA to migrate systems efficiently from legacy technology environments through evolutionary and incremental developments, and help it demonstrate a clear return on investment. This, in turn, should help VA more effectively manage information technology as a strategic resource and business-process enabler.

2. *In your testimony, you stated that VHA has begun steps to further improve the accuracy and timeliness of its decision support system (DSS) data. This has been a documented problem for years. Can you tell us what specific steps VHA has taken?*

Over the past year, VHA has taken several actions that have helped improve the accuracy and timeliness of its DSS data. These actions have been facilitated by a work group established last July to identify best practices and recommend actions for improving the timeliness and availability of DSS data.

Among the steps VHA has taken, it developed and issued a directive and a tool for conducting standardization audits, in response to a VA inspector general report regarding the failure of some medical facilities to follow the DSS basic structure for capturing workload data and associated costs.[3] The directive requires annual audits and the reporting of repeated noncompliance with the DSS basic structure to the assistant deputy under secretary for health. Under the direction of VHA's DSS steering committee, the audit tool was developed for use in determining a facility's compliance with the basic DSS model for capturing workload data and associated costs. Last September, every VHA medical facility participated in an audit to assess the extent to which its DSS department and products complied with national standards. The audit revealed a 99.6 percent compliance rate with the national department list, a 98.8 percent compliance rate with the national product list, and a 99.5 percent match between facilities' cost centers and DSS departments.[4]

As another step, this past February the DSS best practices work group distributed a database, along with step-by-step instructions, to help manage the process of identifying and clearing incorrectly coded pharmacy products identified during the monthly processing of DSS data. According to DSS officials, this database is expected to save time and increase data accuracy by automatically (rather than manually) comparing incorrect data against the national products list and assigning correct product numbers to matched records.

DSS officials have also indicated that the use of DSS data in VHA's fiscal year 2002 resource allocation process has helped improve both data accuracy and timeliness. As part of the allocation process, the assistant director of resource management compared DSS fiscal year 2000 cost data with that maintained in the department's financial management system (FMS)—a feeder system to DSS. Variances were found in the DSS and FMS cost data, indicating that audits that should have been performed during the processing of the DSS data either were not performed or were not followed by actions to resolve the discrepancies. Results from the comparison were provided to all pertinent VHA personnel, including veterans integrated service network (VISN) directors and chief financial officers (CFO) and DSS site managers. According to VHA officials, the results were also instrumental in improving collaboration among the medical center and VISN

[3] Department of Veterans Affairs, Office of Inspector General, *Audit of Veterans Health Administration Decision Support System Standardization,* Report No. 9R4-A19-075 (Washington, D.C., March 31, 1999).

[4] A DSS department is defined as a discrete labor pool using specific supplies and/or equipment to produce a similar set of products. For example, the DSS hematology department would include the technicians' labor and the equipment and reagents needed to complete a group of tests, such as a hemoglobin test. The DSS national department list has a standard set of numbers for identifying the various departments. The DSS national product list has a standard set of unique product identifiers, such as for hemoglobin tests.

CFOs and DSS staff during the process to reconcile fiscal year 2001 DSS and FMS cost data.

In addition, the decision to use fiscal year 2000 DSS data for the fiscal year 2002 resource allocation process facilitated the timeliness of DSS data processing. For example, to ensure that fiscal year 2000 clinical and financial data would be available for the allocation process, every DSS site had completed its processing of this data by April 30, 2001. In comparison, at the end of May 2000, seven sites had not yet completed fiscal year 1999 data processing.

Since fiscal year 2001, VHA has required VISN directors to ensure that their medical centers' processing of DSS data is current (that is, no more than 60 days old). This requirement appears to be yielding results. According to a November 30, 2001, DSS processing report, 127 of the 133 DSS sites were current in processing fiscal year 2001 data. A subsequent report dated January 31, 2002, showed that all DSS sites had completed this data processing. Moreover, the reports revealed that the processing of the fiscal year 2001 data had been completed a full 3 months sooner than the processing of the fiscal year 2000 data. In addition, the February 28, 2002, report indicated that all but 16 of the DSS sites had already begun processing their fiscal year 2002 DSS data.

To improve the timeliness of data even further, this past January the best practices work group provided all DSS sites with an updated guide detailing each step involved in the monthly processing of data. The guide was developed using best practices information gathered from the various DSS sites. The work group has now begun gathering best practices data to be considered for improving the fiscal year conversion process.[5]

3. *How would you characterize the success of the VETSNET project? Should VETSNET be terminated?*

VBA has not been very successful in developing and implementing the VETSNET compensation and pension replacement system. Moreover, until VBA performs a complete analysis of the VETSNET initiative, it is questionable whether additional resources should be expended on continued systems development activities.

Since its inception in 1996, VBA has faced a number of problems in carrying out the VETSNET compensation and pension replacement initiative, and we have repeatedly stressed the need for VBA to complete certain tasks that are fundamental to the system's successful development and implementation. These include (1) developing detailed,

[5] The conversion process entails closing out the financial and medical records for the fiscal year and establishing the structure for the new fiscal year. For fiscal year 2000, the process included a new national method to capture vendor-provided home/community health care workloads and a new veterans health information systems and technology architecture extract that records mental health psychological testing workload. Because of problems experienced during the fiscal year 2000 conversion process, clinical processing information did not begin until February 29, 2000.

integrated plans with milestones and costs for use in determining what project activities need to be accomplished and by which organizational components, and to measure the progress of the initiative; and (2) ensuring that the project is carried out with necessary support from the compensation and pension business line. However, VBA has not yet fully addressed these concerns, and after 6 years and at least $35 million expended on the VETSNET project, has not made substantial progress toward fully implementing the replacement system.

Overall, the project is taking considerably longer to implement than was originally anticipated, and its implementation schedule continues to encounter delays. For example, although last year VBA indicated that it had implemented its rating board automation tool and had completed developing and testing its four other software products,[6] the administration stated during our most recent review that two of the software products that will support its award processing and finance and accounting systems still needed more development. Further, VBA's current estimates do not call for completely implementing the system until sometime in 2005.

Because VA's consistent and effective delivery of benefits payments is vital to fulfilling its service delivery obligations to our nation's veterans, successfully implementing a system to replace the existing, aging benefits delivery network is essential. Moreover, responsibility for project success is not limited to VBA, but also depends on VA management oversight to ensure that the project meets milestones, does not exceed costs, and is consistent with the "One VA" information technology environment that the department envisions.

Regarding its termination, a complete assessment of the compensation and pension replacement initiative is needed to determine whether VBA should proceed with the VETSNET project. In fully assessing VETSNET, it will be imperative that VBA determine whether the project is capable of producing an acceptable return on investment. Such a determination will depend on a number of factors, including the outcomes of user acceptance and functional testing to assess whether the system being developed satisfies users' requirements, and detailed planning and analysis to determine how the system can be implemented without significant errors or downtime. This information is particularly relevant given the department's emphasis on reducing the existing backlog of compensation and pension benefit claims.

4. *After years of joint efforts of the DOD and VA to create a government computer-based patient record, which has costs exceeding $40 million, what do they have to show for this decade-old initiative? Any suggestions?*

[6] The current C&P replacement strategy incorporates five software products: Search and Participant Profile, Rating Board Automation 2000, Modern Award Processing-Development, Award Processing, and Finance and Accounting System.

VA's and DOD's efforts toward implementing the government computer-based patient record (GCPR) initiative have not yielded the information-sharing capability and benefits that were originally anticipated. Specifically, in 1998, when the GCPR project was formally initiated, supporting documentation stated that when completed, GCPR would allow health care professionals to "share clinical information via a comprehensive, lifelong medical record." In particular, it was intended to allow physicians and other authorized users at VA, DOD, and Indian Health Service (IHS) facilities to access data from any of the other agencies' health facilities by serving as an interface among their existing health information systems. As a result of its data exchange capability, GCPR was expected to achieve several benefits, including improving quality of care; providing data for population-based research and public health surveillance; advancing industrywide medical information standards; and generating administrative and clinical efficiencies, such as cost savings.

However, as we noted in our testimony and in last April's report,[7] expanding time frames and cost estimates, coupled with inadequate accountability and poor planning, tracking, and oversight, have raised doubts about GCPR's ability to deliver its expected benefits. Since its inception, the scope of the project has been increasingly narrowed, and target dates for developing, testing, and deploying the GCPR interface have continually changed. Consequently, the intended interface capability has not been achieved, and GCPR is now proceeding under a revised strategy that is considerably less ambitious than the project was originally intended to be.

As our testimony noted, VA and DOD are just now testing the first phase of the revised strategy, which will result in a one-way transfer of patient medical information from DOD's system to a separate database that VA's clinicians can access. While this capability is expected to enable some degree of data sharing because VA's clinicians will be able to read and print information from DOD's system, the clinicians, nonetheless, will not be able to perform any calculations on the data retrieved. VA and DOD officials have indicated that they plan to implement this capability by July 2002. Plans for further expanding GCPR's capabilities in later phases are in their infancy, and currently do not include actions that would achieve the initial GCPR goal of a virtual comprehensive patient record.

If VA and DOD are to make significant progress beyond their current strategy of transferring patient medical information from DOD to VA, much work remains. Our April 2001 report noted that strategies for implementation have continued to be revised, and that the project has operated without clear lines of authority and comprehensive, coordinated plans. Before proceeding beyond the current strategy, therefore, it will be critical that VA, DOD, and IHS determine whether the original goals for GCPR remain valid today. If these agencies determine that project goals should be revised, then

[7] GAO-02-369T and 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., April 30, 2001).

attention must be given to establishing and firmly agreeing upon new goals and strategies for achieving real information sharing. Further, once this is accomplished, the agencies should implement the recommendations from our April 2001 report, which called for (1) designating a lead agency for the GCPR initiative and (2) developing detailed plans for the remainder of the endeavor. Beyond these actions, it will be essential that the agencies commit the financial and human resources and executive support necessary for adequately managing the project.

5. *Would it be more effective (quicker, better, cheaper) to implement and manage the enterprise architecture if the CIO had line authority over administration CIOs? Please explain.*

Based on the Clinger-Cohen Act of 1996 and Office of Management and Budget guidance,[8] lead responsibility for developing, maintaining, and facilitating implementation of VA's enterprise architecture should reside with the department CIO. Thus, this position should possess a strong level of governance for guiding and ensuring the success of the enterprise architecture program.

Moreover, ensuring that appropriate authority and reporting relationships exist to facilitate the enterprise architecture program is a key responsibility of each federal agency head. As a result, the department-level CIO's success in effectively implementing and managing the enterprise architecture will depend, in large part, on the secretary of veterans affairs's commitment to and continuation of agencywide support of the effort. Experience demonstrates that the CIO's authority alone is insufficient to make the enterprise architecture endeavor a success. A clear mandate from the agency head and involvement of other key agency executives is a prerequisite.

Therefore, VA's enterprise architecture success may be closely tied to how well the secretary sets expectations and holds administration officials accountable for working with the department-level CIO to institute the enterprise architecture. One mechanism by which the secretary can achieve such accountability is through mandating and enforcing the use of performance standards that are directly tied to senior management's involvement in the development, implementation, and management of the enterprise architecture, and that are controlled at the department level.

As reported in our recent testimony, over the past year, VA top management has demonstrated considerable support of and commitment to the enterprise architecture initiative. It is imperative that such support and commitment be sustained over the long term to ensure successful development, implementation, and use of the enterprise architecture.

[8] Office of Management and Budget, *Management of Federal Information Resources,* Circular A-130 (Washington, D.C.: November 30, 2000).

6. *What are the pros and cons regarding authorizing line authority for the chief of cyber security over the ISOs? Do you think that this would be a more effective method of managing security and remedying the numerous problems?*

Giving the chief of cyber security line authority over VA's many information security officers (ISO) has the potential for both positive and negative ramifications. It could positively affect its management of information security in several ways, including

- providing for departmentwide consistency in performing the security function,
- ensuring that the facility-level security function is adequately staffed,
- neutralizing administration and facility priorities relative to computer security issues that may be inconsistent with those of the department, and
- making the ISO accountable for implementing information security policies through performance oversight measures.

Creating line authority could also present unique challenges for VA. For example, such authorization could

- lessen opportunities for effective collaboration between facility directors and ISOs, thus reducing informal access to facility staff and information;
- enable the implementation of security actions that could be detrimental to the department's business goals, given that ISOs could be less accountable for facility business operations;
- confuse reporting relationships for ISOs departmentwide, given the wide variation in the extent to which VA's approximately 600 ISOs perform security functions as a full-time, primary duty, or in a part-time or secondary capacity;[9] and
- lessen attention to local security issues because priorities would be set at the department level.

These positive and negative factors must be balanced against VA's needs and considered within its organizational culture. Further, successful information security implementation will always depend on participation, ownership, and accountability being shared between security professionals and program managers. As our testimony pointed out, the department has recently mandated information security performance standards for members of the department's senior executive service. If effectively implemented, these standards could serve as a mechanism for enforcing compliance with security policies and procedures and for ensuring accountability for actions taken throughout the department. Employing information security performance standards will require the secretary and his top management to ensure that (1) the chief of cyber security is included during assessments of senior executives' compliance with the security performance standard, (2) a regular assessment of security at the facility level is performed to provide

[9] Currently, only 70 of VA's approximately 600 ISOs work full-time in this area; an additional 187 have security activities as their primary duties. About 370 of the ISOs operate in a part-time capacity, serving various other functions within their respective organizations.

a basis for assessing compliance with the performance standard, and (3) security performance standards are enforced.

As our testimony discussed, the department has not yet clearly defined the roles and responsibilities of facility security officers, or developed and established policies and procedures to ensure departmentwide coordination of security functions. Regardless of the reporting structure that it employs, until VA fully addresses such fundamental deficiencies in its computer security management program, it will continue to lack the framework needed to successfully manage departmentwide security activities.

-- -- -- -- --

We provided a draft of this letter to VA officials; their comments have been incorporated where appropriate.

We are sending copies of this letter to the secretary of veterans affairs and other interested parties. Should you or your offices have any questions on matters discussed in this letter, please contact me at (202) 512-6257. I can also be reached by e-mail at *mcclured@gao.gov*.

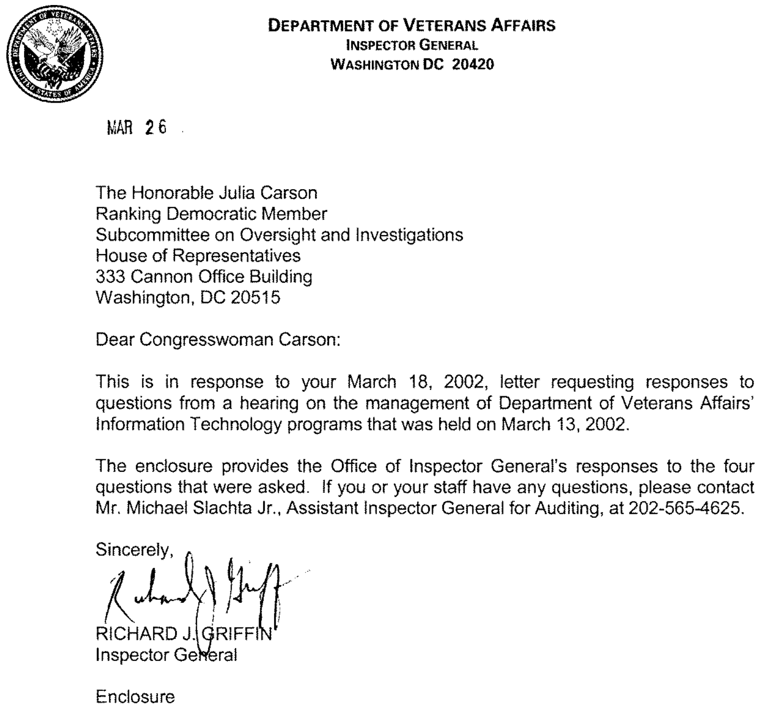
Sincerely yours,

David L. McClure

David L. McClure
Director, Information Technology
Management Issues

(310435)

Congresswoman Carson to Department of Veterans Affairs



Department of Veterans Affairs
Inspector General
Washington DC 20420

MAR 26

The Honorable Julia Carson
Ranking Democratic Member
Subcommittee on Oversight and Investigations
House of Representatives
333 Cannon Office Building
Washington, DC 20515

Dear Congresswoman Carson:

This is in response to your March 18, 2002, letter requesting responses to questions from a hearing on the management of Department of Veterans Affairs' Information Technology programs that was held on March 13, 2002.

The enclosure provides the Office of Inspector General's responses to the four questions that were asked. If you or your staff have any questions, please contact Mr. Michael Slachta Jr., Assistant Inspector General for Auditing, at 202-565-4625.

Sincerely,

RICHARD J. GRIFFIN
Inspector General

Enclosure

Enclosure
Page 1 of 2

1. Representative Tom Davis of Virginia recently introduced a bill that would, among other things, require agency inspectors general to perform independent assessments annually on the effectiveness of agencies' security programs, any deficiencies, and the progress of any corrective actions. How well would your office be able to contribute to the VA's overall cyber security under such a mandate? Please be specific.

We support the passage of this Act and the efforts to focus the Department's attention on this critical area. Currently we expend up to $ 1 million of in house and contracted resources in reviewing and reporting on IT Security as required in the Government Information Security Reform Act (GISRA). This level of effort has identified significant opportunities for VA to strengthen its IT security posture. Examples of some of the results of our IT reviews include recommendations to strengthen password requirements, implement intrusion detection systems, obtain adequate operating systems, and physically protect the department's information systems physical assets. We have also developed a positive working relationship with VA's Office of Cyber Security and the Administration Chief Information Officers. As a result, we believe that our contribution to the overall security of VA has been extensive and will continue under this proposed Act. Because the proposed Act includes similar review requirements now covered as part of GISRA, we believe it will require the same level of effort we have devoted to GISRA.

2. What computer security weaknesses have your Combined Assessment Programs Reviews identified in the VA since our April 2001 hearing?

Combined Assessment Program (CAP) reviews conducted since April 2001 continue to identify a wide range of vulnerabilities in VA systems that could lead to misuse of sensitive automated information and data. VA has established comprehensive information security policies, procedures, and guidelines, however CAP results found that implementation and compliance have been inconsistent. Recent CAP findings show a need to improve access controls, contingency planning, incident reporting, and security training. There is inadequate management oversight at all levels contributing to inefficient practices and to inadequate information security and physical security of assets. CAP results complement the results of our FY 2001 GISRA Audit that identified information security vulnerabilities that place the Department at risk of denial and/or disruption of service attacks on mission critical systems and unauthorized access to and disclosure of sensitive financial data and data subject to Privacy Act protection.

3. In your testimony, you recommend a number of measures to effectively address information security program weaknesses and refer to an OIG report on the subject. Your fourth recommendation states, "Direct Administration CIOs to …" and a number of reasonable action items are listed. Whose job is it to direct Administration CIOs to take these actions and to whom should they be held accountable?? What is a reasonable time to fix existing weaknesses?

Enclosure
Page 2 of 2

Under the current organization each Administration CIO is directly responsible and accountable to their respective Under Secretary to take corrective actions. However, based on a memorandum issued by the Secretary of Veterans Affairs on July 25, 2001, Administration CIOs are directed to "take their technology direction and guidance from the Assistant Secretary for Information and Technology, and the Department's Chief Information Officer." Officials responsible for evaluating the Administration CIO are also directed to "seek and include an evaluation of technical and managerial performance from the Assistant Secretary for Information and Technology." If sufficient resources, budget, and technical support are made available to the Administrations, we believe that these issues can be resolved within the next 2 years. VA has agreed to implement the 10 most imperative corrective actions, which constitute approximately 49 percent of the vulnerabilities, within the next year. We believe remaining vulnerabilities will require an additional year to correct.

4. You note in your testimony the gap between the $21.4 million budgeted FY 02 for cyber security and the $93.2 million in requirements identified in the Department's Cyber Security Capital Investment Proposal. Explain the impact of this gap on resolving weaknesses. Is the budget adequate to fix the problems or is the $21.4 million unrealistically low to solve the problems? Does the $93.2 million mitigate both internal and external threats?

We believe that the initiatives outlined in the Cyber Security Capital Investment Proposal are appropriate to address the weaknesses that currently exist. We have not audited the cost projections, but $21.4 million does not appear to be adequate funding to address weaknesses known to exist at this time. The Department's plan does address both internal and external threats.