VA IT INFRASTRUCTURE REORGANIZATION AND THE ROLE OF THE CIO

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SEPTEMBER 14, 2005

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-22

23-846.PDF

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2006

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

COMMITTEE ON VETERANS' AFFAIRS

STEVE BUYER, *Indiana, Chairman*

MICHAEL BILIRAKIS, *Florida*
TERRY EVERETT, *Alabama*
CLIFF STEARNS, *Florida*
DAN BURTON, *Indiana*
JERRY MORAN, KANSAS
RICHARD H. BAKER, *Louisiana*
HENRY E. BROWN, JR., *South Carolina*
JEFF MILLER, *Florida*
JOHN BOOZMAN, *Arkansas*
JEB BRADLEY, *New Hampshire*
GINNY BROWN-WAITE, *Florida*
MICHAEL R. TURNER, *Ohio*

LANE EVANS, *Illinois, Ranking*
BOB FILNER, *California*
LUIS V. GUTIERREZ, *Illinois*
CORRINE BROWN, *Florida*
VIC SNYDER, *Arkansas*
MICHAEL H. MICHAUD, *Maine*
STEPHANIE HERSETH, *South Dakota*
TED STRICKLAND, *Ohio*
DARLENE HOOLEY, *Oregon*
SILVESTRE REYES, *Texas*
SHELLEY BERKLEY, *Nevada*
TOM UDALL, *New Mexico*

JAMES M. LARIVIERE, *Staff Director*

CONTENTS

September 14, 2005

VA IT INFRASTRUCTURE REORGANIZATION AND THE ROLE OF THE CIO

WEDNESDAY, SEPTEMBER 14, 2005

U.S. House of Representatives,
Committee on Veterans' Affairs,
Washington, D.C.

The Committee met, pursuant to notice, at 10:08 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [Chairman of the Committee] presiding.

Present: Representatives Buyer, Bilirakis, Evans & Michaud.

The Chairman. The VA's Information Technology (IT) infrastructure reorganization hearing before the House Veterans' Affairs Full Committee will come to order September 14, 2005.

This hearing will provide the Committee with an update on the Department of Veterans' Affairs information technology infrastructure reorganization to learn more about the role of the chief information officer within that department.

VA's IT modernization efforts go back at least 29 years to 1985, when it was the policy of the Veterans Administration to "better serve the veteran through modern technology." Despite 20 years of "modernizing," this Committee has authorized, and Congress has appropriated roughly $10 billion over the last decade alone for VA IT spending.

This is probably a very conservative figure, as historically the VA has included funding for IT in general administration accounts of the Veterans Health Administration, the VA's Benefits Administration, and the National Cemetery Administration.

Since coming to Congress in 1993, I have witnessed this Committee struggle with VA's inability to adequately manage its IT funding and IT modernization efforts.

The Subcommittee on Oversight and Investigations has conducted six separate hearings on VA IT and related issues since 2000, when I chaired the Subcommittee.

Ms. Koontz, I see you so often, I feel like you're part of my family.

While there have been significant improvements in VA's IT modernization efforts, the improvements have come at a significant cost to our veterans and the system:

$600 million plus for a decade of VETSNET, the automated compensation and pension claims processing system that still has not been implemented in 10 years;

$342 million for CoreFLS -- the failed financial management system;

$300 million for HR Links, the failed automated personnel system;

$485 million annually to maintain VISTA, VA's 25-year-old medical information system.

In fiscal year 2004 and fiscal year 2005, VA received $1.4 and $1.6 billion respectively for IT funding. For the fiscal year 2006, VA's projected spending for IT will be approximately $2.2 billion.

This lack of accountability in VA IT spending, I believe must stop, and that's the reason why there was such a reduction in your budget requests for IT. Not only did I recommend it, it was supported then by the Budget Committee, by the Appropriations Committee, and also by the Senate.

So somewhere in here, we need to come to a meeting of the minds and to figure out how we're going to do this.

Last year, VA was able to testify before the Committee, that they were "well under way with an enterprise architecture that aims to align the business with the information technology plans, goals, and efforts." However, I am concerned that the structure in place lacks the authority to provide a better service to the veteran.

Today, we will hear testimony from Gartner Consulting, VA's own private IT consultant, on what the VA needs to do more effectively to reorganize itself, and at what cost would be of letting the bureaucracy maintain the status quo.

That's why myself, along with Ranking Member Lane Evans and other distinguished members of this Committee, we will soon be introducing legislation that will mandate the Department of Veterans' Affairs to empower the chief information officer with authority over resources, budget, and personnel related to the information technology of the Department.

I'm holding this hearing, Lane and I are, because our legislation is in draft form, we've not shared it with anyone.

We've come into a comfort zone where we are with the legislation, but we're going to ask a series of questions today, because we want to make sure that what we're about to do, we do correctly, because we also then want it to be leveraged into other departments of the federal government; so we want to walk cautiously and carefully as we do this correctly.

So I am really pleased that the GAO is here to testify. We have you

as the first panel for a reason, because you're experts in your field. Also, CRS, with all your vast knowledge and expertise. Ms. Koontz, the survey that you have done and also with an outside consultant of all the Chief Information Officers (CIOs) and how things are looking out there, you've spoken to so many, and so they've shared with you their successes and they've shared with you their challenges, and from that we want to create the model that can be leveraged.

With that, I'll yield to the Ranking Member for any comments that he may have.

MR. EVANS. Thank you. Thank you, Mr. Chairman.

I also want to praise the VA workers and the crisis response team for safely and swiftly evacuating so many veterans, staff, and their families out of the Gulf Coast.

I also commend VA workers for their current efforts to keep veterans out of the path of Ophelia.

I'm proud of the VA staff.

I have introduced three bills to help veterans and their families get their medical needs and their shelter after the storm. I hope we can mark up these three bills sometime in the near future.

As for information technology management, I think we see this issue in the same way. It is nice to be on the same sheet of music on this.

For years major IT projects at the VA have failed or suffered costly delays. This Committee and its Subcommittees have held a significant number of hearings on VA's mismanagement of IT. We've got to change that need.

Mr. Chairman, we both have consistently pushed for accountability and change. We now have an environment where any successes in the IT area are overshadowed by some well-publicized failure in IT someplace else.

Let us hear testimony about the current status of IT management and then facilitate any needed change.

Thank you, Mr. Chairman.

[The statement of Hon. Lane Evans appears on p. 44]

THE CHAIRMAN. Thank you, Mr. Evans.

I join you in your spirit and compliments to the VA in their rapid response. America doesn't get to hear about it, but Lane and I and members of this Committee are very proud of the VA employees and your direction, and how you responded to the crisis on the Gulf Coast, continue to respond, and help as part of our national response.

Here on Capitol Hill also there are different Committees that are examining Katrina, and so Secretary Mansfield, if you know of things that you need to do within your agencies, that you cannot do right presently within your executive authorities, let us know.

I'm not interested in doing theater or do something, that "do some-

thing" stuff that we get here in Washington, that really is duplicative or multiplicious.

So if it's outside that, please be in touch with Mr. Evans and I.

Mr. Bilirakis.

MR. BILIRAKIS. Mr. Chairman, thank you.

I really appreciate both you and Mr. Evans giving accolades where they're deserved.

The VA, certainly on this particular issue,is far from perfect. There's an awful lot of work that needs to be done and there are a lot of frustrations in the sense that we haven't been able to get IT to the point that it should be after all these many years.

But at the same time, they're probably heads over heels above most of the departments in the government in terms of IT, and they've proven that time and time again. They certainly proved it in New York City in 9/11. They proved it certainly in Katrina. And so they've done really good work.

And what we want to do is to help you to improve upon that, so the potential legislative solutions that the Chairman mentioned are very important.

So we want to be here to help you, but we're not going to be able to help you to really get this thing going the way it should be unless you're cooperative and unless you're being frankly very frank and blunt with us in terms of what needs to be done, in addition to money. It's always money, of course, and that's the unfortunate thing.

Thanks, Mr. Chairman.

THE CHAIRMAN. Mr. Bilirakis, we appreciate your leadership in the continued work on IT from your Subcommittee.

Mr. Michaud, opening statement?

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

I too want to thank you, Mr. Chairman, and Ranking Member Evans for having this hearing today.

Since this is our first hearing after Katrina, I, too, want to take this opportunity to praise the VA employees who kept our veterans, staff, and others safe during the storm.

I understand the staff did an amazing job in evacuating the very sick veterans after the storm and flooding. I applaud the VA frontline workers for reaching out to the veterans to make sure that the storm will not disrupt the delivery of needed medication and benefits.

Those employees and the others who have not yet been found, our thoughts and prayers are definitely with them, and I hope that they are safe.

I understand that the crisis response team is making sure that the VA IT system is working and the benefit files and medical data is secure, so I look forward to hearing your testimony here today.

So thank you very much, Mr. Chairman.

THE CHAIRMAN. Thank you, Mr. Michaud.

The first panel, I will now recognize Mr. Jeff Seifert, who is the Analyst in Information, Science, and Technology Policy Resources, Science, and Industry Division of the Congressional Research Service.

Next we'll hear from Ms. Linda Koontz. She is the Director, Information Management Issues, U.S. Government Accountability Office.

Then we'll hear from Mr. Michael Pedersen, Managing Vice President of Gartner Consulting.

Do each of you have a written statement?

All three have nodded their heads in the affirmative.

Your complete written statements will be made part of the official hearing record.

I will ask members to hold all their questions until the panel has testified. We will move under the five-minute rule.

And Mr. Seifert, you are now recognized.

STATEMENT OF MR. JEFFREY W. SEIFERT, ANALYST IN INFORMATION SCIENCE AND TECHNOLOGY POLICY, CONGRESSIONAL RESEARCH SERVICE

MR. SEIFERT. Thank you, Mr. Chairman and members of the Committee for the invitation to appear before you today to offer testimony on the background and role of chief information officers in the federal government.

While the specific topic of today's hearing is on the responsibilities and authority entrusted to the Office of the Chief Information Officer at the Department of Veterans' Affairs, my comments today will focus on the performance and challenges of federal CIOs more generally.

As you are aware, the Congressional Research Service does not take a position on issues or legislation.

The federal government spends more than $60 billion annually on information technology goods and services, reflecting how technology has become integrated into nearly all government processes.

Federal CIOs are on the front lines in implementing a wide range of e-government and homeland security initiatives. These include initiatives to develop a federal enterprise architecture, improve information security, and identify opportunities to facilitate information sharing.

While CIOs were once commonly thought of as "technocrats," they are now being called upon not only for their technological expertise, but also to provide strategic leadership in the areas of policy, budget, and contract oversight.

Federal CIOs serve as change agents for business modernization and transformation. They must possess strong management, leadership, and communication skills. The CIO's relationship with top-level department decisionmakers can also be critical to successfully

implementing IT and e-government initiatives.

Inherent to the nature of their responsibilities, CIOs need to look at the departments horizontally, across a department, rather than vertically, such as at a single program or function.

Likewise, there is a need to be able to exercise control over resources horizontally, in part to break down the so-called "stovepipes" and "islands of automation" that are created when resources and programs are developed individually.

However, this difference in perspectives can frequently put the CIO at odds with his/her counterparts, such as program managers, whose responsibilities may foster a more vertical view of the department and its assets.

For example, whereas CIOs may recommend adopting a standardized software platform for desktop computers, in order to facilitate interoperability and lower costs, program managers may oppose this approach on the basis that it reduces their decisionmaking authority to procure and develop assets used in the delivery of services.

This clash of perspectives exemplifies why the biggest challenges facing federal CIOs are not technical, but instead, organizational.

Decentralized organizations can be especially challenging for CIOs, whose primary role includes coordinating resources and personnel in an effort to effect transformation of the organization.

While having access to or direct participation in decisions regarding funding issues and allocation of resources is important, simply having a seat at the management table may not be sufficient if other parts of the department can act autonomously in areas that either undermine or mitigate attempts by the CIO to develop enterprise-wide standards.

Consolidating authority over IT resources and clarifying who is accountable for specific functions is one approach that some departments have begun using to address these challenges.

For example, earlier this year, the Federal Bureau of Investigation announced it was implementing a new strategic approach to information technology.

Specifically, the strategy includes centralizing management of FBI IT resources under the FBI's Office of the Chief Information Officer; creating several IT governance bonds; implementing an IT investment strategy and an enterprise architecture; and granting the CIO "budgetary authority over all FBI IT funds."

However, efforts to consolidate IT investment management decisions can be hindered at the outset by a lack of comprehensive accounting of a department's IT resources and responsibilities.

For example, in a March 2005 report, the inspector general at the Department of Transportation found that the consolidation of department-wide IT responsibilities, begun in fiscal year 2003, was not accompanied by a comparable level of budgetary and contract services

oversight.

Among the problems specifically identified in consolidating CIO control over systems originally maintained by the DOT's 11 individual operating administrations was an incommensurate transfer of project management and budget authority, as well as duplicative funding requests made by the CIO's office and the operating administrations.

In closing, information technology management has been a longstanding challenge for the federal government. The general problems facing the Department of Veterans' Affairs are not unlike those facing CIOs in other executive branch departments and agencies.

However, the challenges of harmonizing the acquisition, development, and maintenance of information resources across the department, including its three major subcomponents -- the Veterans Benefits Administration, the Veterans Health Administration, and the National Cemetery Administration -- are considerable.

By enhancing the authority of the department CIO, the Department of Veterans' Affairs may be able to better address some of its information technology management challenges in the future.

Thank you for your attention.

I welcome any questions.

[The statement of Jeffrey W. Seifert appears on p. 46]

THE CHAIRMAN. Thank you, Mr. Seifert.

Ms. Koontz.

STATEMENT OF MS. LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

MS. KOONTZ. Mr. Chairman and members of the Committee, I am pleased to be here at today's hearing on reorganization of VA's CIO office.

At your request, I will be discussing our previous work on the role of the CIOs in the federal government generally, and at VA in particular, to provide background and perspective for your consideration.

As you know, the CIO position was established by the Clinger-Cohen Act in 1996. Through this law and others, the Congress has expressed the view that the federal CIOs should play a central role in managing information and technology within federal agencies.

In this way, the CIO can help ensure that agencies manage their information functions in a coordinated and integrated fashion and thus improve the efficiency and effectiveness of government programs and operations.

CIOs have a wide range of responsibilities. For a review of federal CIOs that we reported on in 2004, we identified 13 major areas of CIO

responsibility that were either statutory requirements or critical to effective information and technology management.

Our review showed that CIOs were generally responsible for these key areas, although not all CIOs were completely responsible for all areas.

To give a few examples, all the CIOs were responsible for enterprise architecture and information security, and more than half were responsible for systems acquisition and major e-government initiatives.

In certain areas such as system acquisition and statistical policy, it was common for CIOs to share responsibilities with others.

We have also developed guidance on the effective use of CIOs in which we describe characteristics of organizations that contribute to CIO success.

First, successful CIOs work with supportive senior executives who embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decisionmaking.

Second, successful CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. Placement of the position at an executive management level in the organization is important, but in addition, CIOs earn credibility and produce results by establishing effective working relationships with business unit heads.

Third, successful CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with knowledge of business processes, market trends, internal legacy structures, and available IT skills, this understanding is necessary that the CIO's office is aligned to best serve agency needs.

To achieve this kind of success, CIOs face a number of challenges. In our 2004 review, CIOs most frequently cited two in particular:

First, implementing effective IT management practices.

A little over 80 percent of the CIOs reported that they face one or more challenges related to this area. This is not surprising, given the government's recognized difficulties in IT management.

We have issued numerous reports describing challenges in the specific management areas that the CIOs cited most frequently: information security, enterprise architecture, investment management, and e-government.

Second, obtaining sufficient and relevant resources.

Virtually all agency CIOs cited resources both in dollars and staff as major challenges.

Two other commonly cited challenges were communication and collaboration, both internal and external, and managing change.

CIOs cited the challenge of establishing effective communications with the business part of their organizations as well as sharing infor-

mation with partners and influencing OMB and the Congress.

And of course implementing major IT changes can involve not only technical risks but also risks associated with people and organizational culture.

At VA, the CIO position and IT management have received increasing attention in recent years.

The department went for two-and-a-half years after the passage of the Clinger-Cohen Act without a CIO.

For two years after that, the CIO role was held by an executive who also had other major responsibilities.

The department then had an acting CIO for a year, and in August 2001, it appointed a full-time permanent CIO.

Since then, the department proposed further strengthening the CIO position and centralizing IT management, recognizing that aspects of the VA computing environment were particularly challenging and required substantial management attention.

In particular, the department information systems and services were highly decentralized and a huge proportion of the department IT budget was controlled by the VA's administrations and staff office.

To address these challenges, the Secretary issued a memo in 2002 announcing that IT functions, programs, and funding would be centralized under the department-level CIO.

In our view, this alignment held promise for improving IT accountability and enabling the department to accomplish its mission. The additional oversight afforded by the CIO could have a significant impact on the department's ability to more effectively account for and manage the approximately $2.1 billion in planned IT spending.

Mr. Chairman, that completes my statement, and I would be happy to answer questions at the appropriate time.

[The statement of Linda Koontz appears on p. 54]

THE CHAIRMAN. Thank you, Ms. Koontz.

Mr. Pedersen.

STATEMENT OF MR. MICHAEL L. PEDERSEN, MANAGING VICE PRESIDENT, GARTNER CONSULTING

MR. PEDERSEN. Thank you, Mr. Chairman, and members of the Committee.

I appreciate the opportunity to participate in today's hearing regarding the Department of Veterans' Affairs IT reorganization.

My name is Michael Pedersen. I'm the managing vice president within the consulting division at Gartner, a provider of research and analysis on the global IT industry.

Unlike our competitors, we do not offer implementation services

that would compromise our independence and objectivity.

It is this objectivity that was the basis for us being selected to assess whether the VA's IT personnel assets are appropriately aligned to efficiently deliver world-class IT program management, operational support, and systems design and development services.

I was the lead consultant and subject matter expert on this assessment and directed activities.

When looking at the VA today, we documented several issues that must be addressed for the VA to achieve its objective of efficiently delivering world-class IT services in a veteran-centric model.

Our principal finding is there is excessive duplication of IT assets -- defined as people, process, and technologies -- across the VA It organizations. This approach leads to inefficiencies in IT delivery and creates significant barriers to improve performance at a VA-wide level.

Each IT group, and there are many, has its own unique, at times competing, at times complementary approach to delivering IT services.

Different approaches to work means working together on common objectives that much more difficult. It also costs more to operate such a fragmented IT organization and has the potential to leave unmanaged risk within its major programs.

There are few incentives or mechanisms in place for these multiple IT groups to work together.

In fact, the culture fosters a go-it-alone approach which forces the IT staff to engage their informal personal network when required to work across organizational boundaries.

To resolve these issues, we recommended changes at the VA. We recommended significant change in the underlying processes that make organizations work, as noted in my written testimony.

As organizational structure is the most visible aspect of organizations, it is worthy of additional discussion.

Several organizational structures were analyzed to resolve the issues uncovered within the VA. Two organizational structures had the greatest potential for application at the VA.

The first is an organizational structure where technology operations, such as data centers and networks, are controlled by a single group with all business applications developed and supported by each business line, whether medical care, pension, housing, or finance. We call this the federated model.

The second is an organizational structure where all VA IT is organized into a single entity reporting to a chief information officer. We call this the centralized model.

Each has its own risks and benefits.

The primary benefit of the federated model is it allows business leaders to develop the applications unique to their missions while

achieving economies of scale by managing the VA infrastructure through the centralized function.

While we did not undertake a cost analysis, our organization does extensive IT cost modeling regarding savings potential.

We estimate implementing the federated model will reduce the annual run rate by approximately $207 million within five years. However, this comes with risk to the VA.

The VA will struggle to obtain in a timely manner its One VA mission objectives, because of its culture, unaligned investment priorities between and within administrations, and differences in technology and process, which hinders efforts to create veteran-centric systems.

In contrast to this approach, the centralized organizational model provides the greatest opportunity to successfully execute One VA mission objectives in a timely manner.

Like the federated model, it achieves economies of scale, but will also allow for rapidly maturing the IT investment management process to better deliver its major IT programs.

We estimate potential savings from the centralized option to be approximately $345 million in annual run rate reduction within five years.

The potential risk from implementing the centralized option is significant. It is the big bang.

But both the centralized and federated potions are viable organizational structures to achieve One VA mission objectives.

However, it is our recommendation that the VA pursue the centralization option and aggressively manage the risk to maximize cost saving opportunity and reduce program risk.

Let me clearly state the organizational change is hard work. If not done properly, it places the entire organization at risk.

Many examples exist where change efforts were not conducted properly.

Whether a computerized position order entry system at Cedars Sinai or a financial management system at the VA itself, organizational change requires extensive planning, executive commitment, and a relentless focus on the details.

The whole organization must see the need for change, understand how change will occur, and participate in the change efforts.

If it embarks on any change effort, the VA must have:

One, its entire leadership team dedicated to the effort, visible in its executive, and held accountable for its results;

Two, fast-track budgeting and personnel change authority for its leaders to act quickly; and

Three, use outside experts to guide, track, and report on its performance against plan.

While it has risk, the payoff can be substantial improvement in IT performance at the VA.

Mr. Chairman, this concludes my statement.

Thank you again for the opportunity to discuss an important matter for our veterans.

I'll answer any questions at the appropriate time.

[The statement of Michael L. Pedersen appears on p. 77]

THE CHAIRMAN. Thank you very much, the three of you, for your testimony, your work, and that of your staffs, so please extend that to them.

Let me ask, Mr. Pedersen, the credibility that you bring to this, being one of the top companies in the world in what you do, are you aware of any organization in the private sector that's like how the VA is presently operating its IT? Is there anyone out there?

MR. PEDERSEN. There is no one out there, sir.

The profit motive of the commercial sector drives a natural cost reduction orientation and an investment oversight mentality, so I know of no other organizations like that.

THE CHAIRMAN. So as Congress has been asking the VA to act more like a business, this effort to bring -- streamline or bring a centralization to the CIO would place us in greater stead with modern business practices?

MR. PEDERSEN. Yes, sir.

If I could add, there are -- the organization as a whole, the agencies are well operating. I want to make that clear. And there is a tremendous desire for the staff to serve the veteran.

And is it our belief that there are efforts underway that have had small pockets of success.

The Austin Automation Center was a good example that we found, where they had defined how they work in a very detailed way. They talked about the costs of their services back through the franchise fund.

And we found that a very effective model. We applaud their efforts. It's the cost that they would -- the recovery or the price, if you will, that they charged the administration are comparable to the outside services.

So there are efforts underway throughout the organization to drive towards that more business, more commercial-oriented practice. It's just not on it as an organization as a whole.

THE CHAIRMAN. All right.

Ms. Koontz, in your written statement, you indicated that the Clinger-Cohen Act of 1996 mandated federal departments to establish the position of CIO. However, the VA did not appoint a permanent CIO position until August of 2001.

What other federal departments, if any, requested and received OMB waivers for appointing a permanent CIO?

MS. KOONTZ. I know of no department that has a waiver for estab-

lishing a CIO.

I don't know of any mechanism, either, that would allow an agency to go without a CIO.

The law requires that they have a CIO, and that the CIO report to the agency head.

THE CHAIRMAN. Also, in your written statement, you indicated that GAO conducted reviews of the relationships of CIOs and agency heads in 23 different agencies.

You further indicated the vast majority of these CIOs reported directly to the agency head.

Of the five largest federal agencies in terms of budget outlays, what is the reporting relationship for the CIO?

MS. KOONTZ. Of the five largest agencies that we looked at, based on discretionary spending -- and that would be Defense, Health and Human Services, Education, State, and VA -- four of the five, including VA, at the time we did our review in early 2004, the CIO reported directly to the agency head. Only HHS did not at that time.

THE CHAIRMAN. Also, in your written statement you indicated that virtually all agency CIOs cite resources, both in dollars and in staff, as a major challenge in effective IT management.

What specific challenges do you believe the VA's CIO must overcome in order for this position to effectively manage VA IT?

MS. KOONTZ. I think that the primary thing that the CIO needs -- there's two things that I think that are most important for the CIO to have in order to be successful.

And the first of that is, obviously, that the CIO has to have the support of the Secretary. Without management support, the CIO cannot be effective.

Secondly, I think that it's critical that the CIO have -- be a participant in an investment management process that's established and mature at the agency, that allows the senior management to come together and make decisions on proposed investments and then oversee those investments over time.

And as part of that process, it's absolutely critical that the CIO be able to veto any proposed investment that is not consistent, for example, with enterprise architecture, that's not consistent with standards, including network standards, or with other security requirements.

THE CHAIRMAN. Mr. Seifert and Mr. Pedersen, do you have an opinion based on Ms. Koontz' statement that she just made?

Do you concur or non-concur?

MR. PEDERSEN. I'd agree that investment management and that control is critical for future investment planning and success.

MR. SEIFERT. Well, as you know, CRS does not take a position on it or express an opinion.

THE CHAIRMAN. Do you have a personal opinion of what you just

heard Ms. Koontz say?

MR. SEIFERT. Well, I'm not allowed to express a personal opinion, but I would say that --

THE CHAIRMAN. Hypothetical?

MR. SEIFERT. -- evidence suggests that this is very important to the successful functioning of the department.

THE CHAIRMAN. That counts. That counts.

Mr. Evans and I and others on this Committee believe in line and budget authority for the CIO position.

So I'm going to go right to the heart of the question.

If we're to deliver line and budget authority to the CIO, give us your positives and negatives that you would foresee in that action being taken.

And then I'll yield to Mr. Evans.

All three of you can respond.

MR. SEIFERT. Well, some potential positives are that the CIO would gain control over all the IT resources within the department and be able to coordinate this in a better fashion, perhaps being able to execute an enterprise architecture plan.

A potential drawback is that, a department of the VA's size is fairly complex and it would be hard to imagine any one person being able to honestly understand every nuance that's required for every department or every function.

So it is possible that he or she may not be able to capture every little piece of that and may inadvertently overlook something.

THE CHAIRMAN. Ms. Koontz.

MS. KOONTZ. Similarly, I think that if you centralize the funding under the CIO, certainly the CIO gains control over the expenditure of those funds, and in that way can ensure that investments that are made are consistent with the enterprise architecture and standards and security requirements, et cetera, and that's an important thing.

My concern, in addition to the scope issue that I think that Mr. Seifert just mentioned, is that it removes the funds from the business areas, and its' very important, if not critical, that information systems arise from identified business needs, and that's critical to any successful systems development effort.

So removing that money from the business does run its own set of risks. It also puts the business in a position where they have -- they don't have the investment in the systems development effort anymore, because it's not their money.

MR. PEDERSEN. I'd agree with that.

The idea of bringing accountability is critical. What you want to guard against -- and you'll have that if you bring that to the single point in the CIO.

What you need to guard against is that budget flows for other purposes manifest themselves back into IT. You need to guard against

that. And you need those executives, those business leaders, back at the table to guide investment decisions.

It should not be the CIO deciding where investments go. All right. They should manage it, get the business to decide where the money should go, what the requirements are, and acceptance of those systems they build. That's where accountability lies on the business.

On the CIO side, it's build towards that spec, and that's where that -- the investment management process can be very effective.

THE CHAIRMAN. Mr. Pedersen, that's where we'd like to go.

Mr. Evans, you are recognized.

MR. EVANS. Mr. Pedersen, could you describe the safeguards necessary to prevent a so-called federated adoption from just becoming what you described as the status quo option, if there were a bureaucratic show of resistance? Can you tell us what those safeguards would have to be?

MR. PEDERSEN. There would be several that I could identify.

Clearly the idea of where money, people, and assets find themselves is going to be one element.

Policy alone won't protect that, because the complexity of the organization is so broad, the way money flows through the organization is so complex, IT spend is very difficult right now to control.

So for the federated model to be successful, there must be all three of those aspects, so the technology, the people, and the budget authority for those assets must move, and that will prevent itself from at least the broad, the very significant change back to the status quo.

But also, though, just good change management requires all members of the organization to be bought into it and lead that effort.

This is not a strike-of-a-pen activity. This is -- we've laid out that this is a long-term plan, it's hard work, it's hard work for the executive team. This is not something that's delegated. The executive team must be critically involved with this and be held accountable for what progress is being made.

Sir, does that help?

MR. EVANS. Yes, sir.

Thank you, Mr. Chairman.

THE CHAIRMAN. Mr. Bilirakis.

MR. BILIRAKIS. Thank you, Mr. Chairman.

Mr. Chairman, I recently returned from a two-day visit to Estonia.

Now, here is a country which just a few years ago was behind the Iron Curtain. Their IT is unbelievable.

Everybody in the country, I think, or virtually everybody in the country -- certainly there must be some exceptions, although I understand there probably aren't -- pay all their bills electronically. Everything is done electronically there.

Their cabinets, if I can call them that -- they took us into a room

where the cabinet sits, and they all have a computer right at their particular location. Everything is done electronically.

A smaller country, to be sure, but in no time at all, they're well past us when it comes to something like this.

You know, it seems to me what Ms. Koontz said in her testimony here, that certainly the VA did not take Clinger-Cohen seriously when they handled the CIO position the way they did, given the time that VA took to even put the position into place, and then it was a part-time job, and functions were divided. Then VA went one year with an acting CIO, and finally in August of 2001, VA appointed a full-time permanent CIO.

So we pass these laws up here, and maybe it's our fault that we don't follow through adequately and have the proper oversight.

In my time remaining, Ms. Koontz, you mentioned the challenges and you mentioned the lack, the implementing and practices -- I'm just paraphrasing. You mentioned obtaining relevant resources. I guess there's always that. And then the word "collaboration," et cetera, everything related to collaboration.

Why are these still challenges after so many years? When you research something like this, the GAO does such a great job, you must have details, specific instances which lead you to these conclusions.

Can you sort of expand upon that, go into these three challenges, particular the top two that you've mentioned, the implementing and the relevant resources, and sort of go into some details for us?

You know, we want to be able to picture this, I guess, is what I'm saying.

Ms. Koontz. I understand.

I will confess, we have lots of details, because we're GAO, but I'm not sure that I have all of them at my fingertips.

Mr. Bilirakis. Well, I don't want all of them.

Ms. Koontz. But I will -- I will provide what I can.

We have done an awful lot of work over the years about IT management practices, and in fact, that's one of the main -- you know, our main lines of work, and that's to look at things like, IT management practices, I mean having enterprise architectures in place, I mean having a robust investment management process in place that will again, like I said before, bring together the right people to make decisions about IT investments, and to not only make the right decisions but then continue to follow them over time.

And also, we've done a huge body of work on security. As you know from the annual reporting of agencies, there are many, many, continue to be many, many difficulties in these areas.

Many of our reports over the years point to the need to strengthen all these management areas and we, you know, continue to work on that.

VA specifically I think, one of the things that has been a threat in

the work that we have done, and I think you would find it's at those other agencies as well, it is not really the technology that is the big, insurmountable problem, it's putting the right management practices in place to make things successful.

MR. BILIRAKIS. It's not the resources, the mechanical resources, if you will, it's the --

MS. KOONTZ. Exactly. It's a matter of having the right institutional processes in place. It's a matter of having accountability. It's a matter of following disciplined processes in terms of building your systems.

And that does sound very simple, but yes, those are challenges. They have been challenges for a long time. This is very difficult. Much of what they're doing -- much of what's being done at the VA is very difficult. I think we can't --

MR. BILIRAKIS. So it's people.

MS. KOONTZ. -- we can't ignore that.

MR. BILIRAKIS. It comes down to people and personalities, and yeah, the thing -- the big problem in government, maybe in life in general, I guess, is what turf, jurisdiction, power, that sort of thing.

Is that what we're really talking about?

MS. KOONTZ. I think that may be an issue. I can't say as I've studied it for sure, but the reason that we support the idea of having these institutional processes in place is that if you have these strong institutional processes, they sort of transcend all those kinds of issues.

They transcend changes in personnel which happen all the time. They transcend personalities. They transcend turf. And that's why we continue to try to underscore the importance of having them.

MR. BILIRAKIS. Well, and it's critical, obviously, that we not do anything here in this legislation that's being talked about, and really heavily thought out, to hurt things.

MS. KOONTZ. Mm-hmm.

MR. BILIRAKIS. We don't want to make things worse.

And I'm not really sure, and I haven't even talked to the staff about it, what kind of cooperation they're getting from the VA, how much they've even gone to the VA for their inputs on it, and that sort of thing, and that's something, of course, that we should be concerned with here.

It's frustrating. We had a round robin in this room here a while back where we're trying to get the VA to cooperate with the DoD in terms of exchange of medical information, interoperability. And it's just frustrating.

The VA has gone, I think, a lot further, obviously, and they have already been commended by us, and well they should be, but if we can't get it done in the VA, which is just one department, I don't know where we're going to be thinking about transferring it over and working with DoD, which is so very, very -- well, particularly in a war such

as we're going through right now, where these people, you know, will -- you know, the transition, if you will, from DoD into the VA and the transfer of records that should take place adequately, and things of that nature.

It's frustrating. The bill was passed back in 1997, I believe, something like that, and here we are in 2005 and we're still not there.

I don't know. I know we change. You know, there's changes up here all the time, and so you have a lack of stability maybe, and then obviously in the departments and in the agencies they have big changes and whatnot, so you have a lack of stability, so it's a little more difficult, Mr. Pedersen, than it would be, I guess, in the private sector, mainly for those reasons.

But when it comes to the things like turf and whatnot, which stick their ugly, ugly head in the way, that upsets the hell out of me.

Thanks, Mr. Chairman.

THE CHAIRMAN. Thank you.

Mr. Michaud.

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

Many of the problems, when you look at the IT system at VHA, can be linked, I think, to the failure to involve front-line workers.

In some cases, I've been told about, for example, the CoreFLS system failed to adequately understand the needs to supply staff and others in ordering basic hospital resources, and as a result, you know, surgeries had to be postponed due to lack of surgical kits; and there are other situations, such as this.

My question is, under the different IT reorganization options, how can the VA best ensure that the end user, the front-line nurse, doctor, medical technician, and others, will have a meaningful involvement in identifying and selecting the IT system that will help them deliver the high quality care that they have to deliver.

It's one thing to sit in an office and see what might be good for a system, but it's another thing to actually be out there having to use that system and knowing what they need.

So what involvement is being done to ensure that end users have a say in this?

MR. PEDERSEN. Clearly, sir, defining the requirement, defining that need is the critical element for that whole investment process.

This is not a central -- you know, there's no effort or desire to say, "We will build it and they will come." It is clearly the role for the practitioners themselves, the consumer of those services to define what they need with the sufficient clarity that people can build it, but also be have to accept what comes back, and if it's not accepted, they have to say why it's not accepted, and that's how the business and the technology work well together to define that.

Where those problems emerge, they typically hadn't defined requirements sufficiently in detail. They hadn't set up the change pro-

cess of when it is a change, how will the new organization absorb that new system. The work, will they be doing things differently? How differently? And has the business leader helped lead that effort? If it comes from the technology group, these typically fail.

MR. MICHAUD. In what process do you envision that happening? Clearly, you know, you might go to one area and just ask one or two, or it might be different in different regions, you know, around the country.

I mean, how are you going to ensure that the end users will have, you know, adequate input into the process?

MR. PEDERSEN. As large organizations have defined it -- I go back to earlier when I said a principal challenge for the organization is defining how they work. They haven't sat down to say how those interactions should occur so that you can capture and manage that risk.

If there are differences for the health care system within each VISN, or within each hospital, we need to define that, or we need to understand it. That would be a cost to the system implementation and how the system will be built.

But if that isn't well established up front, how it gets delivered in the back, that will create a huge problem.

MR. MICHAUD. Thank you.

Thank you, Mr. Chairman.

THE CHAIRMAN. Mr. Pedersen, who are some of Gartner Consulting's private clients, if you're willing to tell me?

MR. PEDERSEN. We predominantly -- we have seven to ten thousand clients worldwide. Predominantly, it is the largest commercial organizations in the world, so names -- household names.

Bank of America, Abbott Laboratories, Office Depot, these are our clients, in addition to most states and large federal governments.

THE CHAIRMAN. So is it fair to say that you are the leader of your field?

MR. PEDERSEN. We are the leading provider of research services, yes, sir.

THE CHAIRMAN. Mr. Seifert, in your testimony when you mentioned Clinger-Cohen, and although the act is specifically -- strike the word "specifically" -- does not explicitly identify federal CIOs as having any form of budgetary control or authority over IT resources, do you know if any federal CIOs that have explicit control over that budget authority?

MR. SEIFERT. As I mentioned in the testimony, the FBI recently granted that authority, and also in the budget proposal for fiscal year 2006, it was proposed, although I don't believe it has been formally approved, that the Department of Justice CIO have budgetary authority over IT related just to information sharing, as compared to the whole department.

Otherwise, I would have to look at the different departments o see,

but so far, most do not appear to.

THE CHAIRMAN. Are you familiar with HHS and in particular NIH?

MR. SEIFERT. To some degree, yes.

THE CHAIRMAN. They're making strides, are they not, in the same fashion where we're going, they just haven't gotten there yet? Is that fair?

MR. SEIFERT. That would be a fair assessment.

THE CHAIRMAN. Ms. Koontz, I couldn't help but think that I could get this wrong, but it's probably pretty close.

I almost feel like I'm having a flashback here.

Five years ago, we sat just like this and at the time I believe it was Secretary Goss who had just testified. He testified after you, but I remember -- it was before you -- and I was asking him, "What kind of authority and powers do you need, you know, now that you've finally got this?"

And he said, "You know, I really don't -- I don't need any, because the Secretary is going to give me what I need to get this done" -- five years ago.

And then when I look at these systems that we have here, this Committee, has funded, that have failed, and that were even outside of his ability to control, it pains me. It -- I just want to say personally -- it pains me.

Because five years ago is where I came up with this, to give this line of budget authority, and I've been really patient, and you've been, too.

But we are -- I think the Committee is finally about there, we really are, to actually do this. But I want to make sure we do it smartly and correctly.

So I hate to be redundant, but I have to come back to this.

If we're to give the CIO budget and line authority and say, then, to the CIO that these are your CIOs that serve for the three under secretaries -- they don't work for the under secretary. They work for the CIO.

And then those regional CIOs report to each CIO, right? So we've got them in a control function?

At the same time, we want business practices to continue, okay?

So whatever system is being created, whether it's -- you know, we have in the works this competition going on with regard to our claims recovery. So we're going to find out which two pilots we'll do for a national rollout. But those are business practices.

But help me here, give me your counsel, give the Committee counsel on how we deliver line and budget authority to the CIO and how then we're going to have proper interface with the business office.

Tell me what your thoughts are.

MS. KOONTZ. I think that's precisely the question.

And one thing that I would like to emphasize developing about in-

vesting in and developing systems, the importance of collaboration between the CIO and the business units.

It's not necessarily that it's one or the other. It's really that it has to be a collaborative type of relationship.

The business is -- the business units are definitely the ones who have to identify the needs. They know what they want. And then the CIO has to be involved to make sure that this fits with the rest of the enterprise, make sure that -- advises them on different technological solutions, and sort of guides the implementation from an IT perspective.

I think that what is more important than who precisely controls the funds is that you have that investment process, that you have a strong institutionalized investment process that brings together the right people to the table to make these decisions, and of course that has to be supported by the head of the agency. The head of the agency has to be committed to making this process work.

The Chairman. All right.

Mr. Pedersen, in your counsel, now to me, take the private sector, how they control the enterprise architecture, interfaced with business, and your counsel is to say, this is how we can do it in the VA.

Mr. Pedersen. I agree heartily with the comments you just heard.

The idea of transparency of the budget, of the money, of how it's being spent, where it's being spent is critical for this. That's the first item that would come to mind.

The second is again, it is not -- well, the chain of command needs to clearly understand the change. They have to be very active in this. This is a very large, complex organization. I don't need to tell you all that.

But how IT currently is structured is very complex today. There isn't a well-defined chain of command. It reports to different people.

So bringing that together is itself an effort, so that all of those individuals need to be involved and have that ability to change.

So that quick change needs to be managed. That is a risk you'll have to manage as you go to that new operating model.

THE CHAIRMAN. All right.

Mr. Michaud, do you have anything?

MR. MICHAUD. No, sir.

THE CHAIRMAN. All right.

I'd like to thank all of you for your written testimony, and we may have follow-on, not today, but as we proceed, and if we can call on you, I'd appreciate that.

As I said earlier, we're trying to build a model that we want to leverage into the rest of the departments in the federal government, and more importantly, how do we do it first in the VA, and then others can examine what we do right and what we do wrong.

And I appreciate your counsel.

Thank you.

The first panel is now dismissed.

The second panel I would like to introduce is The Honorable Gordon H. Mansfield, Deputy Secretary of the Department of Veterans Affairs.

He is accompanied by the Honorable Daniel Cooper, the Under Secretary for Benefits, Veterans Benefits Administration; the Honorable Jonathan B. Perlin, Under Secretary for Health, Veterans Health Administration; and Richard A. Wannemacher, Jr., Acting Secretary for Memorial Affairs, National Cemetery Administration.

Also at the table is the Honorable Robert N. McFarland, the Assistant Secretary for Information Technology and Chief Information Officer, Department of Veterans Affairs.

We also have Pedro Cadenas, the Associate Deputy Assistant Secretary for Cyber and Information Security, Department of Veterans Affairs.

I have a name that a lot of people butcher, and I think I just butchered somebody else's name.

MR. CADENAS. Yes, sir. Cadenas.

THE CHAIRMAN. Cadenas? I apologize. You can call me Buyer.

Mr. Secretary, your complete written statement will be made part of the official record, and you are now recognized for an opening statement.

STATEMENT OF HON. GORDON H. MANSFIELD, DEPUTY SECRETARY, DEPARTMENT OF VETERANS AFFAIRS ACCOMPANIED BY HON. DANIEL L. COOPER, UNDER SECRETARY FOR BENEFITS, VETERANS BENEFITS ADMINISTRATION; HON. JONATHAN B. PERLIN, UNDER SECRETARY FOR HEALTH, VETERANS HEALTH ADMINISTRATION; HON. RICHARD A. WANNEMACHER, JR., ACTING UNDER SECRETARY FOR MEMORIAL AFFAIRS, NATIONAL CEMETERY ADMINISTRATION; HON. ROBERT N. MCFARLAND, ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY AND CHIEF INFORMATION OFFICER, DEPARTMENT OF VETERANS AFFAIRS; AND HON. PEDRO CADENAS, ASSOCIATE DEPUTY ASSISTANT SECRETARY FOR CYBER AND INFORMATION SECURITY, DEPARTMENT OF VETERANS AFFAIRS

MR. MANSFIELD. Mr. Chairman and members of the Committee, I'm pleased to be here this morning to discuss the Department of Veterans' Affairs' ongoing activities in the reorganization of our information technology programs.

I would request also, sir, that the articles noted in the full statement also be included in the record.

Mr. Chairman, I wish to acknowledge your continued interest in this area and thank you for your efforts --

THE CHAIRMAN. Hold just a second.

Which articles are you referring to? Which articles are you referring to that you're asking be incorporated in the record?

MR. MANSFIELD. The ones that are mentioned in my full statement, sir, that are summarized, I would ask that the full articles be included.

These are the ones that deal with our medical records, and they've been presented to the recorder, sir.

THE CHAIRMAN. All right. Hold on just a second right here.

MR. MANSFIELD. If that creates a problem, we will withdraw the request, sir.

THE CHAIRMAN. Well, let me just share this with you, Mr. Secretary.

What I'm going to try to get a control on here is the incorporation of so many outside journals and articles.

I just learned that one of our members on this Committee asked that the Independent Budget be made part of an official record, and we exploded the cost of the production of a record because of how large it is, and it really wasn't something that really was necessary.

So let me just --

MR. MANSFIELD. Sir, as a compromise, I would propose that I would withdraw that request and that, with your permission, copies of those articles will be sent to the members of the Committee.

THE CHAIRMAN. That sounds like a wonderful -- thank you -- request.

You may proceed.

MR. MANSFIELD. Yes, sir, and my apologies for the problem.

As I've said, sir, I wish to acknowledge your continued interest in this area and thank you for your efforts to aid our evolution in this important arena.

In fact, I would say that this truly has been a bipartisan effort by this Committee, and an effort to move us forward in the area of IT technology for the VA.

The size and scope of VA's mission demands a judicious use of all means at our disposal. Information technology has proven to be a valuable tool in a number of important aspects of our business and it holds great promise for increasing our capacity to perform for America's veterans.

I want to emphasize that IT is a tool to be utilized as an important aid to allow us to carry out the department's reason for existence, to deliver services and benefits to our nation's veterans.

Today, we are nearing the end of a fiscal year in which we will provide health care to 5.2 million veterans out of 7.1 million who are enrolled in our system.

We will provide monthly compensation and pension benefits to over 3.5 million veterans and beneficiaries.

Also, we will work with over 500,000 veterans or family members to provide education benefits and 95,000 service disabled veterans through our voc rehab programs.

We are also approaching 100,000 burials in our National Cemetery Administration facilities.

These large numbers are made up of individuals who have earned the benefits we are charged with delivering.

One of the first considerations I believe we have to these millions of veterans is to do no harm.

By that, I mean we must recognize that our current IT system is working and we are performing and providing those benefits.

One of the reasons we are performing is because over the past decades plus we have decentralized our system, as I explained in my submitted testimony.

One result of that decision was that we did gain an effectiveness. However, I recognize that that effectiveness has come with a loss of many efficiencies, and I agree that they must be regained.

As a part of the need to regain some efficiency, the VA must also recognize that we have reached the point in time where we must move, we must move towards standardization in these activities.

Dr. John Gauss, the first IT Assistant Secretary and CIO, started to move towards reorganization.

His efforts resulted in some progress towards a One-VA enterprise architecture, effective project review and approval process, modernization of the telecommunications infrastructure, implementation of an effective cyber-security program for the VA, and a move towards consolidating control over IT budgets, expenditures, and personnel.

When Mr. McFarland came to the VA in 2004, he recommended, and I approved, that we needed an outside consultant to review the VA IT organization and activities with a goal of giving us an "as is," that is an existing view of the organization, and some proposals on recommendations for change.

That activity was performed by Gartner Consulting, whose testimony has been presented by Mr. Michael Pedersen, the managing vice president.

This assessment was to help us enhance the effectiveness of VA's IT by first baselining how it operates today, then developing organizational models that increase VA's IT value in terms of greater efficiencies, economies of scale, and added business value, and finally, charting the path VA IT can follow to deploy its new organizational model to truly deliver value.

This assessment, as you noted, was completed in May of 2005. We are currently assessing alternative management structures and a recent organizational assessment has provided important input.

We understand that any changes must serve to increase our performance on behalf of veterans, in a way ensuring no interruption of services to them.

We are committed to organizing and managing our IT resources wisely and prudently, and look forward to this Committee's continued support.

Basically, Secretary Nicholson, after the briefing from Mr. Pedersen, asked me to review recommendations with the CIO and the under secretaries of the administrations, and come up with a recommended model for him to make the final decision.

I believe that the federated model is the best answer for VA at this point, in that it will produce the quickest return on investment.

VA's size and the scale of its mission make it unique. While centralization of IT application and system development should be the long-term goal, it is not a prudent near-term solution based on the current culture and the ability to manage significant change.

The federated approach includes high-level management, budget control, and comprehensive oversight of application and systems development within the CIOs's office. This will significantly strengthen the VA's ability to deliver high-risk, high-value application development projects.

This is the first step, and will start breaking down the stovepipes, moving us closer towards One-VA.

And finally, I have directed each administration to realign and reorganize the methods by which they do application and systems development and reorient those activities based on industry standard best practices.

This will ensure proper planning, design, integration and standardization requirements are followed throughout the department as we build our next generation systems and applications as One-VA systems to better serve our veterans.

I might note in closing that the CIO will have management oversight and budget decision authority.

Two issues I would like to address include, number one, resources. That issue has been brought up.

But I would say that this Congress and the administration have been generous with the VA for funding IT projects, and I believe that it's not an issue of dollar resources as much as it is qualified personnel that we need to be able to get into this organization and help us design, manage, and run these programs.

We also recognize that right now we cannot do it from inside, and as we move forward towards a change, we're going to need outside help, and we're planning on that. And the last point I would make is one that's mentioned in the Gartner report. And that is that we do have a highly motivated workforce in the administrations that want to deliver services to veterans and will get in line with a proper plan

that's properly explained and that they have a part in designing and moving forward.

Thank you very much for this opportunity, Mr. Chairman, and I look forward to answering your questions.

[The statement of Hon. Gordon H. Mansfield appears on p. 90]

THE CHAIRMAN. Thank you, Mr. Secretary.

I can choose one word to describe the mission when I took over this job as Chairman of the Committee: accountability -- accountability, accountability, accountability.

People will demand it on this Committee, will demand it equally of the administration or any of the advocates on behalf of veterans.

Why did you hire Gartner Consulting?

MR. MANSFIELD. At the point in time we made the decision to hire them, we decided that, with Mr. McFarland as a brand new assistant secretary for information technology, and I as a brand new deputy secretary, looking at the situation we had in hand and in discussions with the then Secretary, acknowledged that we needed to look at this total IT structure, what it was doing, what it was not doing, and make decisions to make changes in its operations.

We wanted to bring in somebody from the outside that could take an outside view of it, and give us some information on where they saw the "as is" picture, and also make some recommendations where they thought we might want to go.

And Mr. McFarland is the person that was put in charge of that, and followed up on that mission.

THE CHAIRMAN. And why that specific consulting firm?

MR. MANSFIELD. I'll turn that over to Mr. McFarland, since he's the expert in this area.

MR. MCFARLAND. Well, sir, Gartner and the firm which they acquired, which was META, is known throughout the industry as having a unique set of qualifications.

Primarily, I was interested in someone that didn't have a vested interest in what we did and how we organized ourselves and what the outcome was.

Gartner nor META had any businesses that are related to integration of products or selection of products and tools, so I was interested in an independent attitude.

I also wanted a fresh set of eyes. Everybody in the VA has an opinion about IT. I wanted a fresh set of eyes, and that was the best fresh set of eyes I could find at the time, and I --

THE CHAIRMAN. What was the cost of the contract?

MR. MCFARLAND. The contract was, I believe, sir, somewhere between $4.5 and $5 million, I believe, to the best of my recollection.

THE CHAIRMAN. Secretary Mansfield, what makes an effective CIO?

MR. MANSFIELD. Someone that, number one, is knowledgeable and

understands information technology, understands what it can do as a tool, somebody who is able to look to the future, and in this fast-changing arena, be able to anticipate some of the changes or be able to move with the changes, and then somebody who is dedicated to ensuring that these activities go forward in the best way possible.

THE CHAIRMAN. You would concur with this statement, that this is the 101, that IT is an enabler for you to accomplish your mission in an effective manner, correct?

MR. MANSFIELD. Yes.

THE CHAIRMAN. In order to have a good enabler, you have to have one architecture; would you concur with that?

MR. MANSFIELD. Yes.

THE CHAIRMAN. So it is extremely important, whether you choose a centralized approach or a federated approach, that we maintain one architecture, correct?

MR. MANSFIELD. Yes, sir.

THE CHAIRMAN. Okay.

Let me -- Mr. Secretary, may I turn to your three under secretaries for a moment?

MR. MANSFIELD. Pardon me, sir?

THE CHAIRMAN. May I turn to your three under secretaries for a moment for questions?

MR. MANSFIELD. Yes, sir. That's what they're here for.

THE CHAIRMAN. What would be the concern of the three of you of a centralized approach, whereby we give a line of budget authority to the CIO?

What are the positives of that approach, and what are the negatives of that approach with regard to centralized, let me just say this, recognizing that testimony we just had before you took to this table, the testimony was what you presently do is not mirrored anywhere, not anywhere.

So give me your counsel. Whoever wants to go first.

MR. MANSFIELD. Dr. Perlin, do you want to go first?

DR. PERLIN. Thank you, Mr. Chairman for the opportunity to comment on that.

First, let me acknowledge the positives of either centralization or a federated approach.

We are One-VA. We should have seamless interoperability between benefits and health and commemoration of veterans, period. We should have an architecture that supports and facilitates that.

Some might actually agree that the control of funds within the Office of Information Technology will allow us to coordinate our projects and realize an enterprise architecture that delivers that.

My concern about centralization really relates to our history, as well as the experience of health information technology in the United States.

Health information technology is not pervasive. Less than 20 percent of health care providers, certainly hospitals, have health information systems, and certainly VA has been hailed for its exceptional performance in delivery of high-quality health care facilitated by health information technologies.

In fact, this month's issue of Healthcare Papers in Canada, (an entire issue) was dedicated to understanding the improvement and the transformation of VA. It recognized the health information technology as a supporting technology, and it recognized further the performance measurement and the accountability.

Sir, you asked about accountability. Our performance is our accountability. Our performance is the fulfillment of our mission of high-quality health care services.

We've had a history of a centralized health information before. In fact, before this very Committee, the Inspector General testified he did a "flyoff" between one centralized and one decentralized program. Ultimately it was the centralized one that had failed.

It failed because it had characteristics that were similar to some of the shortcomings of CoreFLS. It didn't engage the end user.

So with all due respect to what I've just heard in terms of testimony and with absolute cognizance of health information in the United States and the experience of health care executives and chief information officers in health care, I support the consolidation of the infrastructure, the generic architecture, the enterprise architecture, but the attachment of development to the clinicians, to the end users is the defining characteristic and has been reported in Healthcare Papers, among other journals, as the key feature of the success of the health information system in VA.

So in the federated model, I think we gain the efficiencies but preserve that unique aspect of the information system that allows and has demonstrated VA's ability to deliver high-quality care to veterans.

THE CHAIRMAN. Admiral Cooper.

ADMIRAL COOPER. Essentially, I would say that the devil is in the details.

In my organization, VBA, we essentially have a centralized process. In my opinion, I could acclimate to whatever decision is made.

The whole execution of the IT reorganization is dependent upon the agreements that we have and how we execute them. My concern is that because such a large portion of VBA's budget goes to paying people, if at times I have to use money, I do not having full control of the budget. However, that is something that can be worked out.

THE CHAIRMAN. Mr. Wannemacher.

MR. WANNEMACHER. The National Cemetery Administration supports the VA CIO by working within federated model. This insures we adapt and adhere to Department goals which promote synergy

and efficiency of business processes.

With the smallest of the three VA administrations IT budget, NCA has operated with an internalized centralized system for the past 10 years in order to enhance memorial benefits and service delivery to our Nation's veterans and their families.

MR. MANSFIELD. Mr. Chairman, Dr. Perlin would like to add another point, if he may.

DR. PERLIN. I think you asked for the pros and cons of the two models, so I was very taken by the testimony where it supported the thesis that I just offered.

It was said that one of the risks is a lack of intellectual investment in the activity.

That singularly has been the disconnect in the clinical community in terms of getting health information technologies to work. Maintaining that connectivity with clinicians, is one of the key features. That is why I recommend the federated model.

THE CHAIRMAN. Secretary McFarland, if we were to give you line and budget authority, how do you place at ease the three under secretaries that you're not going to stymie innovation, and their ideas?

There's a budget. There's only so many dollars. But you're part of a team, and when we're now going to heed counsel that you paid a lot of money for, and he talked about the importance of collaboration between the business and the CIO, how do we achieve a central model?

MR. MCFARLAND. Well, I believe in no matter which model you choose, a key factor has to take place, and that is a customer orientation.

I've spent 33 years in the information technology sector, and I am a full believer and have seen this environment be successful, where you have a customer mentality.

IT is a tool. It's a business enabler. It serves its customers. It should first serve the veteran in this organization and it should second serve the employees, and the employees of the administrations.

If the users are not served, then IT fails.

So any IT organization that I've ever headed up or will ever head up will have a customer mentality that says that the people we serve every day and supply power to, supply technology to, are the customers. They are the people that we have to deliver services and technology that make their business applications work.

We have to take input from them on what's required. They are the experts.

IT itself is not a business application. IT is a tool. And it can only be enabled if you're able to serve the customer.

Candidly, I haven't always seen a customer mentality in VA in the 18 months I've been here, and I believe we have to first and foremost take 6,000 IT people out there, no matter what they're doing or

where they're serving, and get them to understand that IT and their participation is about serving the customers -- the veterans and the employees.

THE CHAIRMAN. All right. That was pretty hard.

We're well aware of, as we roll out in more areas the patient medical records issues, that those words are all meant to be customer friendly and help deliver and improve quality care.

So as Dr. Perlin would come up with an idea, all right, or roll out into another VISN, your job would be to make sure that it fits the architecture, right, and hardware and software, right?

So you got to put a check in the box for that, under a centralized approach?

MR. MCFARLAND. Yes, sir.

THE CHAIRMAN. All right? Not that you're the guy that's to tell him, "No, it cannot be done," or if you say it can't be done, then it's a real issue that's got to be resolved then between Secretary Mansfield and the Secretary, right?

MR. MCFARLAND. Well, under either model you have to be able to do this.

Under either model, you have to be able to agree that anything the user wants you to build or wants you to run has to be able to meet the enterprise architecture. It has to be able to fit within the One-VA approach to delivering services.

Our job, in either model, is to advise the administrations and their constituents exactly what will fit and what won't fit --

THE CHAIRMAN. Okay.

MR. MCFARLAND. -- and then sit down and negotiate how we change a specification, how do we move a design to make it fit. That's a collaborative effort. It has to be done that way.

THE CHAIRMAN. All right.

Mr. Michaud,.

MR. MICHAUD. Thank you, Mr. Chairman.

I have one question for Mr. Mansfield.

I realize that the VA is still in the process of securing IT assets and restoring information systems and communication in the Katrina-affected area, and this may be too early for the question.

But do you have any preliminary lessons learned on improving the IT system at VA, and how would IT reorganization have improved or hindered efforts during this disaster?

MR. MANSFIELD. Thank you for that question, sir.

I would make a couple of introductory comments, and then turn it over to the experts here.

But I do know the one lesson -- and we do have a lessons learned group out of our readiness operations center that is currently in the process of coming up with a total lessons learned for everything in this operation, as we do every time we go through one of these exer-

cises.

One lesson learned is that our backup communications systems were not able to do the job, and we need to go forward and find something better than we had and get that on site and be able to use that so we can maintain communications.

One of the aspects of our system, though, is fortunately, because of our planning, because of our training, we have folks out there that have been through this, and were able to operate on their own even if communications was interrupted from a certain point.

The other part of it is dealing with records, and I'll turn that over to Dr. Perlin, is that in general, we were able to make the move in time to be sure that any of the veterans in that affected area, no matter where they moved to, the practitioners were able to get access to those records.

However, it does raise one issue that is a problem in our system, and that is that it oftentimes, again in these, as I say, decentralized operations, each one doesn't fit across the whole system, and that's where we need to go, where instead of having to work a special fix each time, we can ensure that across the total system, those records are interoperable.

And I would ask Dr. Perlin to comment on that, and then Mr. McFarland.

DR. PERLIN. Thank you, Secretary Mansfield.

Congressman Michaud, thank you for the question.

I actually have in front of me two articles from today.

One: "Katrina Shows Need to Computerize Records," Orlando Sentinel, talking about how effective having electronic health records were.

And a similar article from Government Computer notes, "Agency IT Provides Relief After Katrina."

Both comment on VA's effectiveness in meeting the mission: That's serving veterans - ultimately our mission, not an IT mission - a mission of patient care, because those records could be made available to the entire system, being hosted at another facility, even after New Orleans came off-line.

The deputy had mentioned one important improvement, that backup communications henceforth will have satellite uplinks, and we appreciate the collaboration with the Office of Information Technology in establishing those at Biloxi and Jackson in the middle of the crisis to provide broadband communications.

The second is that --

THE CHAIRMAN. Can I interrupt a second?

I want you to correct me if I'm wrong.

There's no single data repository for all of these records. Would that not be correct? That's correct, is it not?

DR. PERLIN. That is correct.

THE CHAIRMAN. Okay. So when a patient was transferred directly from, whether it's New Orleans to Houston, or Biloxi to Jackson, somebody had to back up a tape.

So when that patient was taken directly to Houston, Houston couldn't come on line, show a doctor, "Here's what the medical record is," that it had to be backed up and inserted?

DR. PERLIN. No, that record would have been, Sir, available had there been connectivity between New Orleans and Houston.

Under the circumstance, the latest footprint, the most recent data was acquired in fact, during the storm. In fact, that's one of the take-home lessons: that the facility could continue to operate independently!

Let me turn to Mr. McFarland in terms of our corporate repository.

MR. MCFARLAND. It is true that, in order to get the records from New Orleans to Houston, we did have to take a tape from New Orleans bring it to Houston, install a configuration that was equal to the New Orleans configuration, and then bring it up.

One of the initiatives that Dr. Perlin's people and myself have been working on some two months now, two-and-a-half, three months now, is the concept of regional data processing centers, so that we can get to a point where these records will not have to be moved by tape, that they would be accessible anywhere within a region that a veteran would be able to go.

But, yes, currently today, they are different instances, different configurations based on medical centers, but there is a process in place to change that.

THE CHAIRMAN. All right.

Mr. Michaud, I want to thank you for yielding to me, because that's a fine example of why I'm hesitant on a federated approach, because we think that this is all out there, but it's really not if you don't have the word, "connectivity."

I yield back to the gentleman.

MR. MICHAUD. That's a good point, Mr. Chairman.

Actually, that was going to be my follow-up question. Is there a central place where there is a backup, and if so, where is that, or do you envision that being so?

DR. PERLIN. Sir, there is backup of corporate data nationally. It doesn't integrate as one seamless record at this moment.

The project Mr. McFarland described, the health data repository, will allow it to operate as one seamless health record.

The reason it does not is not because we willfully wanted to have different instances of VISTA. The reason it is as it is now is entirely an artifact of history.

Even ten years ago, let alone 20 years ago, one didn't think in terabytes of data or national data files. It was really quite miraculous to

stand up one hospital on one system.

In fact, as they evolved over time, there was differentiation.

The task before us, and Mr. McFarland and I are absolutely in lockstep agreement on this, is that there be one consistent instance of the system of the electronic health record, and it's that which allows in this really imminent next generation of the health data repository one seamless record across the United States.

MR. MANSFIELD. Sir, if I may add a follow-up to that, to the Chairman's point, it's my belief in the federated model that we're talking about and recommending to go forward with, that the issue you brought up would be solved because there would be one operational system that would be under the control of the CIO, across the whole VA, and that would take care of not only the problem with VHA, but it would, when we get to the final point, also give us One-VA where the veterans' records would be accessible across the system.

So in the model that I'm looking at and proposing, we would have that solution, sir.

MR. MICHAUD. I want to follow up on that question.

So what would happen if we had a terrorist attack and it took out that system? What would happen as far as the records?

THE CHAIRMAN. The national system or the local system?

MR. MICHAUD. Yes, the national system.

MR. MCFARLAND. Well, first off, sir, we would never have a single instance of any system.

I believe we will be able to put those records, that national system in multiple locations, and have a mirror image of those at all times, so that no matter whether we lose any specific site, we will be able to recover immediately from the backup site, and that's a mirroring effect. You don't want it to be anything except a mirrored image.

MR. MICHAUD. Thank you very much.

And Mr. Chairman, Dr. Perlin had mentioned a couple of articles. We do not need them for the record, but if he could provide the Committee with those articles, I'd appreciate it.

The material was provided to the Committee, and is maintained in the Committee files.]

THE CHAIRMAN. Thank you, Mr. Michaud.

MR. MICHAUD. Thank you.

THE CHAIRMAN. Mr. Bilirakis.

MR. BILIRAKIS. This is not, I guess, considered a very sexy subject, high-profile, et cetera, and yet we've got a room full of people here.

I mean, to me that's very meaningful. There's concern in this area. There's a lot of interest in this area. And I'd like to say there's a lot of frustration in this area.

Mr. McFarland, Mr. Secretary McFarland -- I guess you're Secretary, right?

MR. MCFARLAND. Assistant Secretary.

MR. BILIRAKIS. Under the federated model that Mr. Mansfield and others have talked about putting that into effect, you would be in charge, I guess.

Would you have the adequate authority to be able to do what is necessary to be done, referring now again -- I don't know whether Ms. Koontz is still in the room -- referring again to the challenges that she mentioned, the implementation practices, the obtaining relevant resources, the collaboration.

Would you have the adequate authority?

Now, I know you guys work next to each other and you probably go to lunch together and you're friends, as well you should be.

But can you be honest with us?

MR. MCFARLAND. As long as I have what I would consider, and this may not be the right government word, but I'll use it anyway, as long as I have veto power over the way money is spent on IT infrastructure and IT projects --

MR. BILIRAKIS. How about if money is spent for -- money which may be allocated to IT, but is not being proposed to be spent for IT, is being used for any other purposes?

MR. MCFARLAND. Well, then, would that be the case, then I would not have the control, no.

But I don't believe that is the intent of either model, If I understand what we're working --

MR. BILIRAKIS. I'm sure it's not the intent, officially the intent.

What happens now? You have money allocated to IT, and is all of it being spent on IT?

MR. MCFARLAND. I daresay, according to what staff tells me, it is not.

I do not have visibility into all of the money being spent today, and as to whether it is completely spent on IT --

MR. BILIRAKIS. Should you not have that authority?

MR. MCFARLAND. I definitely should have.

MR. BILIRAKIS. You should have that authority, and you would not have under the model that is proposed by the VA, would you?

MR. MCFARLAND. No, I believe I could have it under either model. I don't have it today, but I could have it under either of the models that are proposed here.

MR. BILIRAKIS. Well, I should think that it's not a matter of could have. I think it should be a matter of should have or will have based on the way legislation is crafted.

The VA has spent, what is it, half a billion dollars, whatever, what the figure was for the consultant that we talked about earlier.

They disagree, the VA disagrees with the consultant's recommendations. As I understand it the piece of legislation which the Committee is crafting is consistent with the consultant's recommendations.

How do you feel about that?

MR. MANSFIELD. Sir, I would say that --

MR. BILIRAKIS. I was asking Mr. McFarland, but I would like to hear from you, too, Gordon.

MR. MANSFIELD. Sir, I would say that we have agreed with one of the options, and the consultant, as requested, came up with a number of options, and we believe that, based on his input plus other input, that the one that we've chosen is the best one for the organization.

MR. BILIRAKIS. Are you saying the consultant --

MR. MANSFIELD. We didn't say that "You have complete control and you'll run this." We said, "We want you to make recommendations."

We've taken those recommendations inside the Department, and as I mentioned, at the Secretary's direction, we've had numerous discussions with the CIO and the administrations and come up with what we have --

MR. BILIRAKIS. So the consultant suggested a number of options and the centralized model which is going into the legislation is one of them, but the federalist -- the federated model --

MR. MANSFIELD. Yes, sir. And I believe his testimony that he presented here indicates that those two are the preferred -- those two are the preferred models.

MR. BILIRAKIS. Mr. McFarland, what say you?

MR. MCFARLAND. I believe that I can support a federated model based on the concept that the very first thing we need to do is get our arms around the infrastructure.

The reason we have stovepipes today is because the infrastructure is divided among the administrations. There is no collaboration. There is no joint use. There is none of that today. And that is the primary reason for the stovepipes. And I also --

MR. BILIRAKIS. Would the federated model be consistent with that particular status quo?

MR. MCFARLAND. The federated model would solve that. Both the centralized and the federated model would solve that issue.

The other thing, candidly, that I have to look at as a political appointee is, I have a limited amount of time to pour what I call concrete with good rebar, and that is that what can I do quickly in my three years left here that I can do to make sure that we make change that stays here; and certainly, the infrastructure is the quickest return on investment.

MR. BILIRAKIS. Which model would you prefer, sir? You, our political appointee?

THE CHAIRMAN. In your personal opinion.

MR. MCFARLAND. In my professional opinion --

MR. BILIRAKIS. Personal, professional, any kind of opinion.

MR. MCFARLAND. -- I support what the consultant said.

That being said, it is the big bang, and the big bang has a great

amount of risk to it.

And at the direction of the Secretary and the deputy --

MR. BILIRAKIS. Are you a lawyer, Mr. McFarland?

MR. MCFARLAND. Pardon me, sir?

MR. BILIRAKIS. Are you a lawyer?

MR. MCFARLAND. No, sir, I am not a lawyer.

MR. BILIRAKIS. Well, you know how to dance around these questions.

MR. MCFARLAND. I'm not trying to dance, sir.

I'll be honest and tell you, in my professional opinion and my personal opinion, the centralized option is the best thing in the long run for the VA.

MR. BILIRAKIS. Okay.

MR. MCFARLAND. I'm also a realist and know that we have to take this thing a step at a time. There are no --

MR. BILIRAKIS. Okay, and that's good. I really appreciate your adding those additional words. We have to take it a step at a time and what not.

And I think it's important that the Committee understand, I know that the Chairman understands, that we don't want to do any harm here. We don't want to cause more problems.

And we understand also, or we should understand, hopefully we understand correctly that you're on the line and you know this stuff better than we do.

But, you know, we have concerns. The major VA IT investments that have failed in the past, who was -- you know, the questions, who was in charge of the following programs: VETSNET, CoreFLS, VISTA, two billion dollars down the drain, that could have gone to health care, Mr. Secretary.

I understand the CIO was not in charge. Who was in charge? Who is currently in charge of management of these programs?

We can get answers from you, but these things have happened.

Now, there's a level. We've already said great things about the VA. We've commended you. Frankly, I felt like standing up and applauding you on the work that you have done on Katrina and your help with 9/11 back in 2001, et cetera.

But there are a lot of failures here, and so there's a lack of credibility, I would say.

And Dr. Perlin -- you know, you want to put up your hand -- you're a doctor, and you care about health care, and you don't mind my concern. I've chaired the Health Subcommittee on the Energy and Commerce Committee for 10 years on health care, and I'm very much concerned with it all.

By God, the question that Mr. Michaud asked, about why the Houston computers had to be reconfigured in order to be able to use that tape? What's wrong? Something is wrong with that scenario.

And I'm going to ask, on behalf of -- I'm vice Chairman of the Committee. I've already cosponsored the legislation.

But I'm going to ask that we sit down with you all and that you'll be yielding, that you'll be yielding, that you're not going to be stubborn and say, "Hey, our model is the model that we want to go to and we don't want to cooperate as far as a centralized model is concerned."

But Mr. McFarland, who I think can see the forest for the trees hopefully, has said that the centralized model is clearly the preferred one. He said he can work with both of them, I think, as I understand his paraphrasing his statements, but that's the better model.

Now, should that model be twisted a little bit and whatnot to make sure that no harm is done? I suppose so. But we've all got to be open minded.

I've taken a lot of time, Mr. Chairman. I apologize for it. But I've sat in these meetings all through the years. We had our roundtable the other day. I just can't get over how little Estonia can do what they've done and how we can't even do it within one of our departments.

Thanks, Mr. Chairman.

THE CHAIRMAN. Mr. Michaud.

MR. MICHAUD. Thank you, Mr. Chairman.

I'm reading the GAO Report, and I have one question, Mr. Chairman.

According to a memorandum dated back in August of 2002 from Secretary Principi, in that memorandum, he talked about realigning to a central IT system. That was back in 2002.

The GAO reported in September of 2002 that it would build credibility, it would achieve a One-VA, it was bold, it was innovative, and that memorandum was signed in 2002.

My question is, why hasn't it happened? That was for a centralized system.

MR. MCFARLAND. I've only been here 18 months, so I didn't have the benefit of being here at that time, but I've done my best to look into the history.

I believe the intent was there. With all due respect to my predecessor, I do not believe it was executed on. It's as simple as that.

MR. MICHAUD. I guess from the VA side this was signed by the former Secretary.

What has been done to move it to a centralized system?

And I realize, Mr. Mansfield, you've only been there for a short time, as well. I don't know if Dr. Perlin or --

MR. MANSFIELD. Sir, the effect of that memo was carried out with a change, I believe, of 97 personnel being in effect dual-lined, reporting both to the CIO and to the administration head, and then further down the line.

And as I mentioned in my oral statement, there was work done on

a One-VA enterprise architecture. There was a move towards project review that got the Office of the CIO the ability to sign off before money could be authorized.

There was a modernization of the telecommunications infrastructure that Mr. McFarland finished, which is saving us millions of dollars, the implementation of an effective cyber security program -- for the first time in history, VA has completed that and is certified -- and a move towards, only a move towards, consolidating control over IT budgets, expenditures, and personnel.

And as I indicated, what Mr. McFarland and I were looking for when we asked for the outside consultant to come in was to look at, based on that change, where we were and what did we need to do to go forward so that we would have a plan, and then we could, inside the Department, make a decision or make a recommendation to the Secretary, based on his final decision then, as you said, sir, assume the responsibility and move forward.

MR. MICHAUD. If I might, Mr. Chairman, just follow up.

Mr. McFarland, you said you've only been there 18 months. That's a year-and-a-half.

Did you make any attempt to try to move forward on this memorandum?

MR. MCFARLAND. Well, as soon as I got my hands on the memorandums and the history is when I sat down with the new deputy and said, "We are not where this says we were supposed to go. I think we need to get an understanding of where we are and then figure out how we get to go where we're supposed to go." And that's what generated the Gartner study.

And, you know, it took me some time to get that contract awarded. We have our share of issues in the area of getting contracts, so it took some matter of months before I could actually get a contract out.

So I apologize for having been here 18 months and not getting it done sooner, but I moved about as fast as I was able to, sir, candidly.

MR. MICHAUD. Okay. Thank you very much.

Thank you, Mr. Chairman.

THE CHAIRMAN. You know, Mr. Michaud, when you talked about what's been done in moving toward that direction of centralization, I couldn't help but think there's also been a trip, a stumble, and a fall.

And I recall the trip, the stumble, and the fall: CoreFLS, VETSNET, and VISTA, and some of that was outside of control and responsibility.

And so what I'm hopeful, I think, as we move toward this centralization, that there's not going to be a lot of fingerpointing. We're going to know how we're going to make the system accountable.

At this moment, I want to pause, and I think we need to get some input here from the chief information security officer.

We've heard from the other three under secretaries, and you work

directly for McFarland. Now, we know that the Federal Information Systems Management Act gave an F on the report with regard to cyber security, and so we've got some pretty strong concerns here.

And so if Congress were to move toward a centralized approach and follow the counsel of Gartner Consulting, as opposed to a federated approach -- so take federated approach and flush it out of your mind at the moment -- how do we improve the cyber security under a centralized approach?

MR. CADENAS. Thank you for the opportunity to be here, sir.

Tremendous opportunities in regards to a centralized approach, as you've been talking about, sir.

With me working for Mr. McFarland, it allows me to go out there with my teams, established a more formalized process, applying hardening systems to ensure configuration baseline, change control boards, everything, and bringing in what I would call good systems engineering from a security point of view, to out there and do that to the systems out there, to ensure hardening -- perimeter in depth, defense in depth approach.

THE CHAIRMAN. So if we're under the centralized approach, the CIO, your boss, now owns the people for the three under secretaries, and then owns those CIOs that go down regionally, right, and it continues to go down.

Do you believe that the centralized approach will regain control, or could take this control away from these autonomous networks?

MR. CADENAS. Well, sir, I've been there -- I'm a newbie, as well. I will have my third anniversary here in November.

Yes, it will help in those areas, but what we have been doing is, we have developed a tremendous collaboration effort with the community in working with us. The result of worms that we've experienced in the past have only applied or reinforced the need for that strong collaboration.

The control that you're talking about, sir, that it will allow us to have, will allow us to act much quicker. A great deal of our success has been on KOOMBAYA's, shared accountability working groups with the various communities out there. Versus having that control, I can immediately engage and move out.

THE CHAIRMAN. Well, if the Federal Information Systems Management Act Report gave you an F --

MR. CADENAS. Yes, sir.

THE CHAIRMAN. -- I mean, come on. We need to move out swiftly here.

MR. MANSFIELD. Sir, if I may, I believe that the federated model that I'm proposing would give him exactly the same capability. He would be able to do it.

THE CHAIRMAN. Well, I asked my particular question because I think we're about to follow the centralized approach that you paid $5 mil-

lion to a consultant that's giving us counsel here.

And I know, Mr. Secretary, you're under tremendous pressures. You have three under secretaries that you also have to work with, and you've developed relationships with.

And to be very frank with you, I don't have much patience, because I've been doing this for six years -- six years -- and I've watched the system, and all along, it's been, "Steve, let this mature, let it massage, we'll move in that direction, incremental approaches." I'm pretty exhausted, Mr. Secretary.

MR. BILIRAKIS. Well, Mr. Chairman, sorry to hitchhiked upon your comments.

This trying to set up an IT system that will be able to accomplish all of these things the way it should in today's high-powered electronic and mechanical world is significant, but it's even more so now because of the threat of terrorism, because of natural disasters, and everything of that nature.

So, boy, we should all have lost our patience, not knowing what may happen tomorrow.

But you seem to be intent on the federated model. The Committee seems to be intent on the centralized model. Hopefully, there will be something in between or at least some of your ideas certainly should be used to be part of any legislation that comes up.

But what I'm wondering, Mr. Chairman, is if they're working towards a federated model with their full speed ahead on the federated model, and we in the meantime are thinking another way, and the time that it takes, of course, to get through the process, through this very unwieldy republic system of ours, it becomes legislation, are they going to be expending dollars on a system that will not -- that will be moot, basically, once we finally have --

THE CHAIRMAN. That's a good question, and I think that's one that we can also entertain off line, but just playing this out, my counsel to the Secretary would be to be cautious, in how you proceed.

Because there is such strong bipartisan support on this Committee for a centralized approach, we will immediately go to conference with the Senate, where we also know that House Appropriations staff along the Senate Appropriations staff is also embracing, I believe, a centralized approach.

So there is time between now and when we leave, potentially, on November 18th, that we could actually send this to the President.

So, Mr. Bilirakis, your point is well made, and I think Mr. Mansfield has heard the response.

I yield back to Mr. Bilirakis.

MR. BILIRAKIS. Well, thank you, sir.

I would just hope, Mr. Mansfield, that you would -- you know, let's be logical and reasonable and all this, knowing that this may be coming down the pike, with hopefully suggestions from you all, which

might sort of squirm it a little bit, you know and change it a little bit and that sort of thing.

I don't know where it might be needed and acceptable that in the process of what you're doing with your federated model, you take all that into consideration.

As I understand the federated model, it probably would be right on the same path as the centralized model, anyhow, so hopefully, we're not talking about any waste of dollars or waste of effort that would then have to be undone later on.

MR. MANSFIELD. Yes, sir. In fact, the Gartner report makes the point for the centralized model that it cannot be done in one step, that it will require multiple steps, and the federated model is a part of that process, I would believe, or can be made so.

MR. BILIRAKIS. Okay. That's good. Thank you, sir.

THE CHAIRMAN. Thank you.

Mr. Michaud.

MR. MICHAUD. Just a comment, Mr. Chairman.

My question to Mr. McFarland wasn't to point fingers. It was more or less to find out why they have not moved in that direction, because having been involved for a number of years at the state level, if sometimes individuals who are running programs, if they do not like the particular program, they'll do everything they can to make sure that it doesn't happen, so that was my questioning.

And I agree with you 100 percent on the accountability, and we definitely have to have accountability and make sure that the end users are involved in doing it, because they're the ones that are going to have to use the system.

And I know that you will hold them accountable, and actually, in Maine, Mr. Chairman, we have a saying, and hopefully you don't take it disrespectfully, but knowing you just the short time I have known you, you're like a pit bull. When you get something, you hold onto it, and you hold that accountability.

And I think we definitely will get that accountability. Looking forward to working with you, making sure that we have a system that everyone can live with and will be accountable not only to the taxpayers but also to members of Congress.

Thank you, Mr. Chairman.

THE CHAIRMAN. Thank you, Mr. Michaud.

I appreciated the candor of the gentleman from Gartner Consulting in that it's almost like, well, of course, this isn't going to be out in the private sector, because there it is for profit. Right? And if you're a government enterprise, you don't have to worry about it. You do budget submissions. Who wants to be against spending in the veterans' arena? Right?

And so trying to bring efficiencies to these processes, I mean, it is our responsibility.

You know, there are a couple of really large procurement contracts with regard to IT that are sitting out there -- PAIRS and PCHS. PCHS and PAIRS.

So if we're about to move into this, tell me where we are on these two larger procurement contracts that could involve billions of dollars. What are we doing?

MR. MCFARLAND. Well, sir, we are currently operating under what's called PCHS II, which is a common hardware and software procurement vehicle that we use to buy all of our hardware and software throughout the VA. It's based on a set of standards.

It has served us reasonably well, but it's due to be redone, because it's about to hit its cap, and we'll have to implement anew what I call PCHS III next year.

I've been intimately involved with procurement and have made it clear what I want out of PCHS III, which is different than what we've had in PCHS II.

I want to get a lot more standardization, because it appeared as PCHS II evolved, just about anyone could select something and get it on PCHS, and that allowed them to buy it, and that did not serve us as well as I would have hoped in our standardization efforts.

So PCHS III will produce a much stronger standardized environment.

Under any move that we make from an IT reorg, I will control that hardware and software buy, and I will see that we get standardization and that we get common configurations out there through this contract.

THE CHAIRMAN. I don't know where you are in the letting of these contracts.

Mr. McFarland, should we not let these contracts until this legislation is in place, so that you've got this line of budget authority?

MR. MCFARLAND. We are still working under PCHS II, and will through a part of next year.

I believe PCHS III isn't due to come online or be let, if you will, the contract be let until about the middle of next year.

So we're at a point where nothing that you would do between now and then would get in the way of any aspect of trying to modernize that procurement vehicle.

THE CHAIRMAN. All right.

Admiral Cooper, the Navy uses a process where the Fleet expresses a need for a new system, provides requirements, and the systems commands work with the Pentagon and the Fleet users to build a system that meets the Fleet's needs.

The process is very structured and has rigorous reviews at many levels in the acquisition chain of command, does it not?

ADMIRAL COOPER. That's correct. Yes, sir.

THE CHAIRMAN. Do you similarly see a structure and would you like

to see a system very similar to that within the systems that you presently control?

ADMIRAL COOPER. Yes, sir.

THE CHAIRMAN. I'm going to give it to you.

This hearing is now concluded.

[Whereupon, at 12:08 p.m., the Committee was adjourned.]

APPENDIX

Statement of Honorable Lane Evans
Ranking Democratic Member
House Committee on Veterans Affairs
Full Committee Hearing, September 14, 2005

The Department of Veterans Affairs (VA) has struggled with effective management of its information technology (IT) resources for a number of years. Major system failures and delays have been identified by Congress, the Government Accountability Office, the VA Inspector General and other agencies to include independent contractors. The more egregious failures have garnered significant negative regional and national press coverage. In our fiscally strained environment, any amount of money is a terrible price to pay for a project failure. Yet, the legacy of the HR LINK$ and CoreFLS projects alone account for almost one billion dollars wasted. The automated benefits project known as VETSNET is now slowly lumbering down the right track after a number of stops, starts and wrong turns. The Committee estimates expenditures of $600 million over more than 10 years have been invested in VETSNET.

Since 2000, the Oversight and Investigations Subcommittee has diligently held six hearings directly related to information technology management at VA. That subcommittee has explored the responsiveness of VA to apply adequate resources to manage the portfolio of information technology systems in VA. First, VA struggled to comply with all of the requirements of the Clinger-Cohen Act; it took some time and effort for us to see even the appointment of a full time Chief Information Officer (CIO).

Other problems were identified during this array of subcommittee hearings. These include a lack of accountability for IT program management, inadequate authority of the CIO over IT programmatic and financial matters, unclear line control of cyber security personnel, a lack of a sense of urgency to complete required IT actions and inadequate elucidation business needs to support the IT development and acquisition processes.

The mountain of evidence indicates that a change in the status quo for IT management is required. VA has enlisted the services of a contractor to review the enterprise architecture at the Department and to recommend options for reorganization of the IT infrastructure. They broke little new ground from what the subcommittee had previously uncovered, but they described the problems and categorized the possible solutions with crystalline clarity. Moreover, they were

able to supply and organize data to support their observations and recommendations – this is very helpful in addressing the problem.

At today's hearing we will review the landscape of IT management at VA one more time -- this time from a full committee perspective. We hope to hear of success stories with new IT systems, but we must assure that management of IT is accomplished under a system that will assure the mission and business needs of the Administrations and other stakeholders are met with a high level of efficiency from a centralized – One-VA perspective. As voluntary internal efforts by VA to reorganize to meet this goal have failed so far, this Committee may need to take legislative action.

STATEMENT OF JEFFREY W. SEIFERT
ANALYST IN INFORMATION SCIENCE AND TECHNOLOGY POLICY
CONGRESSIONAL RESEARCH SERVICE

BEFORE

THE COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES
SEPTEMBER 14, 2005
VA IT Infrastructure Reorganization and the Role of the CIO

Mr. Chairman, and members of the Committee, thank you for the invitation to appear before you today to offer testimony on the background and role of chief information officers (CIOs) in the federal government. While the primary focus of today's hearing is on responsibilities and authority entrusted to the Office of the Chief Information Officer at the Department of Veterans Affairs (VA), my comments today will be restricted to the performance and challenges of federal CIOs more generally. As you are aware, the Congressional Research Service does not take a position on issues or legislation. Consequently, I will confine my remarks to the historical and organizational aspects of today's topic.

The Importance of Federal IT Management

The federal government spends more than $60 billion annually on information technology (IT) goods and services. As information technology becomes increasingly integrated into nearly all government processes, efforts to improve federal IT management have become more important. These include initiatives to develop a federal enterprise architecture, improve information security, and identify opportunities to facilitate information sharing. Consolidating authority over IT resources and clarifying who is accountable for specific functions is part of this process. However, the broad range of activities and fluid nature of federal information technology initiatives suggest that the level of consolidated control will likely depend on the size and nature of the responsibilities of each department.

Federal CIOs are on the front lines in implementing a wide range of e-government and homeland security initiatives. In the case of e-government a central area of concern is developing a comprehensive but flexible strategy to coordinate the disparate e-government initiatives across the federal government. As the initial round of e-government projects continue to become fully operational, OMB has stated it plans to focus attention on initiatives that consolidate information technology systems in six functional Lines of Business (LoB). These include financial management, human resource management, grants management, case management, federal health architecture, and information security. These initiatives were chosen, in part, because they represent core business functions common to many departments and agencies, and/or have the potential to reap significant efficiency and efficacy gains. These LoB initiatives are anticipated to create $5 billion in savings over 10 years.

In considering the VA, it may be instructive to took at another department. In the case of homeland security, one of the biggest challenges facing the Department of Homeland Security (DHS) is the ongoing effort to consolidate the computer and communications systems of the 22 agencies that comprise the Department. In many respects, DHS functions as a virtual department, connecting new and existing agencies into a network that capitalizes on their knowledge assets to facilitate information sharing and enhanced communication. Organizationally, this involves breaking down the "stovepipes" that have previously separated the agencies and developing an encompassing organizational culture that promotes cooperation and information sharing. Technologically, this involves integrating existing systems and infrastructures while simultaneously infusing new technologies as they are become available. A critical variable that will contribute to the success or failure of these objectives is the development and implementation of an enterprise architecture for the Department. An enterprise architecture serves as a blueprint of the business operations of an organization, and the technologies needed to carry out these functions. It is designed to be comprehensive, flexible, and scalable, to account for future growth needs. As the Department moves forward with its enterprise architecture plans, it will encounter several issues, including making choices between competing systems and reallocating resources and staff accordingly.

Origins of Establishment of Chief Information Officer (CIO) Position

During the mid-1990s, Congress considered several bills focusing on governmental reform and improved management of public resources. The option of establishing a single federal CIO was one of several proposals to address these problems. The success of CIOs in the private sector is often cited as an example for government to follow. However, the interest in establishing CIOs in the federal government was generated by the experience of local and state governments. At the time, forty states had some form of a CIO operating in a policy capacity, as did several major cities. For many, their experience demonstrated that there was a need for someone to articulate a "vision" of information resources that helped coordinate agency activities and goals rather than reinforce the artificial "stovepipes" that separated them. The idea of a federal CIO was ultimately dropped in favor of establishing a CIO in each of the major executive branch agencies, which was included as one of the provisions in the Information Technology Management Reform Act (ITMRA), which was enacted into law as Section E of the National Defense Authorization Act for Fiscal Year 1996, (P.L. 104-106). Another provision of P.L. 104-106 was the Federal Acquisition Reform Act (FARA) (Section D). FARA and ITMRA were collectively renamed the Clinger-Cohen Act of 1996 in the fiscal year 1997 Omnibus Consolidated Appropriations Act, (P.L. 104-208).

The statutory responsibilities of federal CIOs are delineated in Section 5125(b) of the Clinger-Cohen Act:

> (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with

chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency;

(2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and

(3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

In addition, as the individuals primarily responsible for IT capital planning and investment control in their respective departments, federal CIOs are required to report to their department heads. Besides the Clinger-Cohen Act, other laws that affect or modify CIOs' responsibilities include the Paperwork Reduction Act of 1995, the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), the Federal Records Act, the Freedom of Information Act, and the Privacy Act of 1974. Although these responsibilities suggest that federal CIOs are the primary officials in charge of planning, acquiring, and maintaining IT resources in their respective departments and agencies, the Clinger-Cohen Act does not *explicitly* identify federal CIOs as having any budgetary control or authority over IT resources.

Chief Information Officers Council

Following the passage of the Clinger-Cohen Act, President Clinton established the Chief Information Officers Council by Executive Order 13011, *Federal Information Technology*, on July 16, 1996. The CIO Council was later codified into statute with the passage of the E-Government Act of 2002 (P.L. 107-347) in December 2002. Section 101 of the E-Government Act adds chapter 36 "Management and Promotion of Electronic Services" to Title 44 of the United States Code. Among other provisions, this chapter delineates the membership and responsibilities of the CIO Council, which is described as the "principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources."[1] The membership of the CIO Council includes, the CIOs of the major executive branch departments and agencies; the CIOs of the Central Intelligence Agency (CIA), Army, Navy, and Air Force; the Administrator of the Office of Electronic Government; the Administrator of the Office of Information and Regulatory Affairs (OIRA); the Deputy Director for Management of the Office of Management and Budget (OMB), who serves as the chairperson of the CIO Council; and any other officer or employee of the United States designated by the chairperson. The Administrator of the Office of E-Government leads the activities of the CIO Council on behalf of the chairperson and the Vice Chair is elected from the membership. The CIO Council meets monthly and currently has three committees to address specific information technology management concerns such as enterprise architecture development, IT workforce issues, and information technology best practices. The committees work to help facilitate the growth of government standards, share best practices, and help agencies work to be in compliance with reform legislation such as the Government Performance and Results Act (GPRA).

[1] 3603 (d).

The statutory responsibilities of the CIO Council are delineated in Section 3603 of Chapter 36 U.S.C., as stated in the E-Government Act:

> (1) Develop recommendations for the Director on Government information resources management policies and requirements.
>
> (2) Share experiences, ideas, best practices, and innovative approaches related to information resources management.
>
> (3) Assist the Administrator in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.
>
> (4) Promote the development and use of common performance measures for agency information resources management under this chapter and title II of the E-Government Act of 2002.
>
> (5) Work as appropriate with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40, and maximize the use of commercial standards as appropriate, including the following:
>
> > (A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.
> >
> > (B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.
> >
> > (C) Standards and guidelines for Federal Government computer system efficiency and security.
>
> (6) Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management.
>
> (7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

Evolving Role of Federal CIOs

As IT projects have become more integrated into the function of a department or agency, the role of CIOs has evolved as well. While CIOs were once commonly thought of as "technocrats," they are now being called upon not only for their technological expertise, but also to provide strategic leadership in the areas of policy, budget, and contract oversight. Federal CIOs serve the role of change agents for business modernization and transformation. They must possess strong management, leadership, and communication skills. The CIO's relationship with top-level department decisionmakers can also be critical to successfully implementing IT and e-government initiatives. This suggests that, in selecting a department-level CIO, one needs to select individuals who have a deep contextual understanding of the mission and functions of an organization, but who also bring a wide range of experiences and perspectives to the position.

Inherent to the nature of their responsibilities, CIOs need to look at their departments horizontally, across a department, rather than vertically, such as at a single program or function. Likewise, there is a need to be able to exercise control over resources horizontally, across a department, in part to break down so-called "stovepipes" and "islands of automation" that can be created when resources and programs are developed vertically. However, this perspective can frequently put the CIO at odds with his/her counterparts, such as program managers, whose responsibilities may foster a more vertical view of the department and its assets. For example, whereas CIOs may want to move the department to adopt a standardized software platform for desktop computers in order to facilitate interoperability and lower costs, program managers may oppose this approach on the basis that it reduces their decisionmaking authority to procure and develop assets used in the delivery of services. This clash of perspectives is frequently one of the root causes of the most significant challenges federal CIOs face.

Challenges Facing CIOs

Since the creation of the department-level chief information officer position, a number of obstacles have been attributed to undermining the CIOs' abilities to carry out their responsibilities. For example, at a July 2004 hearing of the House Committee on Government Reform's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, in his opening statement, the Subcommittee Chairman highlighted some of the more pressing issues related to federal CIOs. These included the disparity between the average tenure of an agency CIO (23 months) and the amount of time it takes to effect change and shepherd large projects (3-5 years); CIOs' lack of control over all IT investment in their agencies; the growing range of CIO responsibilities; and the reporting relationships between CIOs and senior management as well as subordinates.[2]

In its 2004 annual survey of federal chief information officers, the Association for Federal Information Resource Managers (AFFIRM) asked respondents to rank order the most important

[2] Opening statement of the Hon. Adam Putnam: House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, *Where's the CIO? The Role, Responsibility and Challenge for Federal Chief Information Officers in IT Investment Oversight and Management*, 108th Cong., 2nd sess. (Washington: GPO, 2004), p. 4.

challenges they faced. The top ten reported challenges, starting with the most important challenge cited, include:

- *Aligning IT and organizational mission goals*
- Using IT to improve service to customers/stakeholders/citizens
- *Obtaining adequate funding for IT programs and projects*
- *Formulating or implementing an enterprise architecture*
- Hiring and retaining skilled professionals
- Managing or replacing legacy systems
- *Developing agency-wide IT accountability*
- *Unifying "islands of automation" within lines of business (across agencies)*
- *Implementing and controlling IT capital planning and investment management across the agency*
- Simplifying business processes to maximize the benefit of technology[3]

Six of the top ten reported challenges (shown in italics above) are directly related to the CIO's ability to exercise department-wide authority over IT personnel, assets, and resources. As e-government and homeland security initiatives become more sophisticated and move beyond their demonstration project phases, they begin to assume a department-wide, or even government-wide character. Consequently, the CIO's authority over relevant resources can be crucial to the longer term implementation and success of these initiatives.

Although the specific issues may differ slightly from year to year, there is general agreement that the biggest challenges facing federal CIOs are not technical, but instead, organizational. Decentralized organizations can pose especially trying challenges for CIOs, whose primary role includes coordinating resources and personnel from a horizontal, centralized perspective in an effort to effect transformation of the organization. A factor frequently cited by experts on federal IT management that affects the CIO's performance is whether or not he/she has a seat at the management table. Although the Clinger-Cohen Act requires that department-level CIOs report to the Secretaries of their respective departments, in practice this is not always the case. Instead, they may be reporting to officials one, two, or possibly three levels below the department secretary. While there is some debate regarding whether there is no substitute for reporting directly to the department secretary, or if reporting to an alternative senior official, such as a chief management officer is sufficient, there is clear agreement that being able to influence top-level decisionmaking can be critical to the CIO's ability to carry out his/her responsibilities. Access to, or direct participation in, decisions regarding funding issues and the allocation of resources can have a significant impact on agency IT budgets and whether various initiatives and programs are adequately funded. However, simply having a seat at the management table may not be sufficient if other parts of the department can act autonomously in areas that either undermine or mitigate attempts by the CIO to develop enterprise-wide standards. To that end, there appears to be a growing interest on the part of some departments and agencies to expand their CIOs' authority and control over all of their respective department's IT budgetary and

[3] AFFIRM, *The Federal Chief Information Officer: Ninth Annual Top Ten Challenges Survey*, (Washington: December 2004), p. 11.

information resources, and in some cases, IT-related personnel as well, rather than leaving some control in the hands of project managers and other department officials.

Selected Recent Attempts by Federal Departments and Agencies to Address Challenges

The Clinger-Cohen Act divides responsibility for federal IT management among three primary entities; OMB, department heads, and department CIOs. If the performance of any one of these entities is reduced, or diminished, then federal IT management as a whole can suffer. As a result of organizational resistance to transformational change, it is possible that CIOs may need additional tools and authority to carry out their responsibilities as the federal government continues to move into the 21st century. To that end, there appears to be a growing awareness of the importance of budgetary control to IT management, and some departments have begun addressing this issue.

For example, earlier this year, following the high-profile failure of its Virtual Case File (VCF) initiative, designed to provide Federal Bureau of Investigation (FBI) agents with a computerized case management system at their desktops, the FBI announced it was implementing a new strategic approach to information technology. Specifically, the strategy includes centralizing management of FBI IT under the FBI's Office of the Chief Information Officer (OCIO), creating several IT governance boards, implementing an enterprise architecture and an IT investment strategy, and granting the OCIO "budgetary authority over all FBI IT funds."[4]

In an effort to both strengthen federal CIOs' budgetary authority and enhance congressional oversight, some observers have suggested consolidating a department's entire IT spending under a single budgetary line item. However, the possibility of attempting to define a department's entire IT spending under a single budgetary line item may be complicated by the object classes used to identify particular expenditures, because each object class may include a variety of similar, but unrelated, expenditures.[5] Consequently, some attempts to address the issue of CIO budgetary control do not necessarily extend to a department's entire IT investment, but only to specific initiatives. For example, in the President's FY2006 budget proposal, the Department of Justice (DOJ) is to receive funding to facilitate and improve information sharing. These monies are to be placed in a centralized fund, the Justice Information Sharing Technology (JIST) account, which in turn is to be controlled by the DOJ CIO. The rationale provided for centralizing control over these monies is to:

---

[4] Federal Bureau of Investigation, FBI Information Technology Fact Sheet, June 8, 2005, available at: [http://www.fbi.gov/pressrel/pressrel05/factsheet.htm].

[5] IT-related expenditures can be classified into at least six object classes. These include 23.3 Communications, Utilities, and Miscellaneous Charges; 25.1Advisory and Assistance Services; 25.2 Other Services; 25.7 Operation and Maintenance of Equipment; 26.0 Supplies and Materials; and 31.0 Equipment. A more complete explanation of what is specifically included and excluded from each of those object classes is explained in Section 83 of OMB Circular No. A-11, 2004, available online at: [http://www.whitehouse.gov/omb/circulars/a11/current_year/s83.pdf]. Revised guidance for reporting information technology investments for the FY 2006 budget formulation process are explained in Section 53 of OMB Circular No. A-11, 2004, available online at:
[http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf].

> ensure that investments in information sharing technology are well-planned and aligned with the Department's overall information technology (IT) strategy and enterprise architecture, and that all DOJ components are able to operate in a technologically unified environment, particularly with respect to preventing terrorist attacks on the United States.[6]

Efforts to consolidate IT investment management decisions can also be complicated by a lack of comprehensive accounting of a department's IT resources and responsibilities at the outset. For example, in its March 2005 report regarding the OCIO's budget, the Inspector General at the Department of Transportation (DOT) found that the consolidation of department-wide IT responsibilities, including management of its telephone switching network and provision of network services to the department's operating administrations (OAs), begun in FY2003, was not accompanied by a comparable level of budgetary and contract services oversight. Among the problems specifically identified in consolidating OCIO control over systems originally maintained by the eleven individual OAs, was an incommensurate transfer of project management and budget authority and duplicative funding requests made by the OCIO and the OAs. In response, the DOT IG made nine recommendations for the DOT CIO to follow, including "analyzing performance gaps among duplicate systems in the 11 common businesses" in order to "recommend to the Investment Review Board how consolidating these systems should be funded and managed," and to improve coordination between the OCIO and the OAs to avoid duplicate funding requests for performing similar tasks.[7]

Conclusion

In closing, information technology management has been a long-standing challenge for many federal departments and agencies. The general problems facing the Department of Veterans Affairs are not unlike those facing CIOs in other executive branch departments and agencies. However, the challenges of harmonizing the acquisition, development, and maintenance of information resources across the department, including its three major subcomponents, the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration (NCA), are considerable. By enhancing the authority of the CIO, the Department of Veterans Affairs may be able to better address some of its information technology management challenges in the future. Thank you for your attention. I welcome any questions.

---

[6] U.S. Office of Management and Budget, *Budget of the U.S. Government, Fiscal Year 2006: Appendix*, (Washington: GPO, 2005), p. 672.

[7] Department of Transportation, Office of the Secretary, Office of the Inspector General, *Office of the Chief Information Officer's Budget*, Report FI-2005-055, March 31, 2005, pp. 12-13.

United States Government Accountability Office

GAO

Testimony before the Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
September 14, 2005

VETERANS AFFAIRS

The Critical Role of the Chief Information Officer Position in Effective Information Technology Management

Statement of Linda D. Koontz
Director, Information Management Issues

GAO-05-1017T

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-05-1017T, a testimony before the Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

In carrying out VA's mission of serving the nation's veterans and their dependents, the agency relies extensively on information technology (IT), for which it is requesting about $2.1 billion in fiscal year 2006. VA's vision is to integrate its IT resources and streamline interactions with customers, so that it can provide services and information to veterans more quickly and effectively.

Fully exploiting the potential of IT to improve performance is a challenging goal for VA, as it is throughout government. The Clinger-Cohen Act of 1996 addressed this challenge by, among other things, establishing the position of chief information officer (CIO) to serve as the focal point for information and technology management within departments and agencies.

The Committee requested that GAO discuss the role of CIOs in the federal government, as well as provide a historical perspective on the roles and responsibilities of VA's CIO. In developing this testimony, GAO relied on its previous work at VA as well as on the CIO role across government, including a 2004 review of CIOs at major departments and agencies.

www.gao.gov/cgi-bin/getrpt?GAO-05-1017T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

September 14, 2005

VETERANS AFFAIRS

The Critical Role of the Chief Information Officer Position in Effective Information Technology Management

What GAO Found

CIOs play a critical role in managing information and technology within federal agencies. According to GAO's 2004 review, CIOs generally held wide responsibilities and reported to their agency heads or other top level managers. In general, CIOs reported that they were responsible for key information and technology management areas; for example, all the CIOs were responsible for five key areas (capital planning and investment management, enterprise architecture, information security, strategic planning for information technology and information resource management, and information technology workforce planning). However, in carrying out their responsibilities, the tenure of federal CIOs was often less than the length of time that some experts consider necessary for them to be effective and implement changes: the median tenure was about 2 years, and the most common response regarding time required to be effective was 3 to 5 years. In contrast, CIOs were generally helped in carrying out their responsibilities by the background and experience they brought to the job: most had background in information technology (IT) or related fields, and many also had business knowledge related to their agencies. Other factors that help CIOs meet their responsibilities include (1) being supported by senior executives who recognize the importance to their missions of IT and an effective CIO; (2) playing an influential role in applying IT to business needs; and (3) being able to structure their organizations appropriately. At the same time, CIOs cited several challenges, of which the two most frequently mentioned were implementing effective IT management and obtaining sufficient and relevant resources.

Over time, the CIO position at VA, as well as information and technology management as a whole, has received increased attention at the department. After several years with CIOs whose primary duty was not information and technology management or who were serving in an acting capacity, the department appointed a full-time permanent CIO in August 2001. In 2002, the department proposed further strengthening the position and centralizing IT management, recognizing that aspects of its computing environment were particularly challenging and required substantial management attention. In particular, the department's information systems and services were highly decentralized, and a large proportion of the department's IT budget was controlled by the VA's administrations and staff offices. To address these challenges, the Secretary issued a memo in 2002 announcing that IT functions, programs, and funding would be centralized under the department-level CIO. This realignment held promise for improving accountability and enabling the department to accomplish its mission. The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively account for and manage its IT spending.

Mr. Chairman and Members of the Committee:

Thank you for inviting us to take part in your discussion of the information technology organization at the Department of Veterans Affairs (VA) and the role of the Chief Information Officer (CIO). In carrying out its mission of serving our nation's veterans, the department relies heavily on information technology, for which it is requesting about $2.1 billion in funding for fiscal year 2006. The CIO will play a vital role in ensuring that this money is well spent and that information technology is managed effectively. As we have previously reported, an effective CIO can make a significant difference in building the institutional capacity that is needed to improve an agency's ability to manage information and technology and thus enhance program performance.

At your request, we will discuss the role of CIOs in the federal government, as well as providing a historical perspective on the roles and responsibilities of VA's CIO.

In developing this testimony, we reviewed our previous work in this area. All work covered in this testimony was performed in accordance with generally accepted auditing standards.

Results in Brief

Since the Clinger-Cohen act established the CIO position in 1996, federal CIOs have played a central role in managing information and technology within federal agencies. According to CIOs at major departments and agencies, they generally held wide responsibilities and reported to their agency heads or other top level managers.[1] In general, CIOs reported that they were responsible for key information and technology management areas; for example, all the CIOs were responsible for five key areas (capital planning and investment management, enterprise architecture, information

[1] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (July 21, 2004).

security, strategic planning for information technology and , information resource management, and information technology workforce planning). In carrying out these responsibilities, the tenure of federal CIOs was often less than the length of time that some experts consider necessary for them to be effective and implement changes: the median tenure was about 2 years, and the most common response regarding time required to be effective was 3 to 5 years. In contrast, CIOs were generally helped in carrying out their responsibilities by the background and experience they brought to the job. Although their background was varied, most had background in information technology (IT) or related fields, many having previously served as CIOs; many also had business knowledge related to their agencies, having previously either worked at the agency or in an area related to its mission. Other factors that help CIOs meet their responsibilities effectively are described in guidance[2] that we have issued; key among these are (1) being supported by senior executives who recognize the importance to their missions of IT and an effective CIO; (2) playing an influential role in applying IT to business needs; and (3) being able to structure their organizations appropriately. At the same time, CIOs cited several challenges, of which the two most frequently mentioned were implementing effective IT management and obtaining sufficient and relevant resources.

Over time, VA has devoted increased attention to the CIO position and to IT management. After going for 2½ years after the passage of the Clinger-Cohen Act without a CIO, followed by 2 years with an executive whose time was divided among CIO and other major duties, and then 1 year with an acting CIO, the department appointed a full-time permanent CIO in August 2001. Since then, the department proposed further strengthening the position and centralizing IT management, recognizing that aspects of its computing environment were particularly challenging and required substantial management attention. In particular, the department's information systems and services were highly decentralized, and a large proportion of the department's IT budget was controlled by

[2] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

the VA's administrations and staff offices. To address these challenges, the Secretary issued a memo in 2002 announcing that IT functions, programs, and funding would be centralized under the department-level CIO. In our view, this realignment held promise for improving IT accountability and enabling the department to accomplish its mission. The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively account for and manage its approximately $2.1 billion in planned IT spending.

Background

VA comprises three major components: the Veterans Benefits Administration (VBA), the Veterans Health Administration (VHA), and the National Cemetery Administration (NCA).[3] VA's mission is summed up in its mission statement, a quotation from Abraham Lincoln: "to care for him who shall have borne the battle and for his widow and his orphan." VA carries out this mission by providing benefits and other services to veterans and dependents.

The department's vision is to be a more customer-focused organization, functioning as "One VA." This vision stemmed from the recognition that veterans think of VA as a single entity, but often encountered a confusing, bureaucratic maze of uncoordinated programs that put them through repetitive and frustrating administrative procedures and delays. The "One VA" vision is to create versatile new ways for veterans to obtain services and information by streamlining interactions with customers and integrating IT resources to enable VA employees to help customers more quickly and effectively. This vision will require modifying or replacing separate information systems with integrated systems using common standards to share information across VA programs and with external partner organizations, such as the Department of

[3] VBA provides nonmedical benefits to veterans and their dependents; VHA provides services through the nation's largest health-care system; and NCA provides burial services in 115 national cemeteries.

Defense. Accordingly, effective,management of its IT programs is vital to VA's successful achievement of its vision and mission.

Table 1 shows a breakdown of VA's approximately $2.1 billion IT budget request for fiscal year 2006. Of the total, VHA accounted for approximately $1.8 billion, VBA approximately $150 million, and the National Cemetery Administration (NCA) approximately $11 million. The remaining $84 million was allocated to the department level.

Table 1: Breakdown of VA's Fiscal Year 2006 Information Technology Budget Request (in millions)

Organization	Request	
VHA	$1835	88%
VBA	150	7%
NCA	11	<1%
Department	84	4%
Total	**$2080**	

Source: GAO analysis of VA data.

CIO Plays Major Role in IT Management

The Congress has long recognized that IT has the potential to enable federal agencies to accomplish their missions more quickly, effectively, and economically. However, fully exploiting this potential presents challenges to agencies. Despite substantial IT investments, the federal government's management of information resources has produced mixed results. One of the ways in which the Congress has addressed this issue was to establish the CIO position; an agency's CIO serves as the focal point for information and technology management within an agency.

Legislative Evolution of Agency CIO Role

For more than 20 years, federal law has structured the management of IT and information-related activities under the umbrella of

information resources management (IRM).[4] The IRM approach was first enacted into law in the Paperwork Reduction Act of 1980.[5] The intention of the Congress was to provide for a coordinated approach to managing federal agencies' information resources, addressing the entire information life cycle, from collection through disposition, with the ultimate goal of improving the efficiency and effectiveness of government while reducing the "paperwork burden" on the public.[6]

The 1980 Paperwork Reduction Act centralized governmentwide IRM responsibilities in the Office of Management and Budget (OMB), giving OMB specific policy-setting and oversight duties regarding individual IRM areas, such as records management, privacy, and the acquisition and use of IT.[7] Agencies were given responsibility for carrying out their IRM activities in an efficient, effective, and economical manner in compliance with OMB policies and guidelines. The law also required that each agency head designate a senior official, reporting directly to the agency head, to carry out the agency's responsibilities under the law.

In 1996, the Clinger-Cohen Act established the position of agency CIO by giving this title to the "senior IRM official" mentioned in the Paperwork Reduction Act and specifying additional responsibilities for this position.[8] Among these responsibilities, the Clinger-Cohen

[4] IRM is the process of managing information resources to accomplish agency missions and to improve agency performance.

[5] Pub. L. 96-511 (Dec. 11, 1980).

[6] That is, the burden of responding to government information collections: forms, surveys, and questionnaires.

[7] The 1980 Paperwork Reduction Act referred to this as "automatic data processing and telecommunications equipment," a term that has since been replaced by "IT."

[8] Pub. L. 104-106, February 10, 1996. The law, initially entitled the Information Technology Management Reform Act, was subsequently renamed the Clinger-Cohen Act in Pub. L. 104-208, September 30, 1996.

act required that the CIOs in the 24 major departments and agencies[9] have IRM as their "primary duty."[10]

The view of the Congress as reflected in current law is thus that CIOs should play a key leadership role in ensuring that agencies manage their information functions in a coordinated and integrated fashion in order to improve the efficiency and effectiveness of government programs and operations.

CIO Responsibilities and Reporting Relationships

Besides their statutory responsibilities, CIOs have other responsibilities that can contribute significantly to the successful implementation of information systems and processes. In July 2004, we interviewed 27 CIOs at major agencies[11] on their roles, responsibilities, and challenges, among other things. For this report, we identified major areas of CIO responsibilities that were either statutory requirements or critical to effective information and technology management.[12] Altogether, we identified the 13 areas shown in table 2.

[9] The 24 major departments and agencies are specified in 31 U.S.C. 901.

[10] The E-Government Act of 2002 reiterated agency responsibility for information resources management. Pub. L. 107-347, December 17, 2002.

[11] The 27 agencies covered by our report were the Departments of Agriculture, the Air Force, the Army, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, the Navy, State, Transportation, the Treasury, and Veterans Affairs; and the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[12] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (July 21, 2004).

Table 2: Major Areas of CIO Responsibility

Area of responsibility	Description	Applicable laws
IT/IRM strategic planning	Performing strategic planning for all information and information technology management functions	44 U.S.C. 3506(b)(2)
IT capital planning and investment management	Planning and management of IT capital investments	44 U.S.C. 3506(h), 40 U.S.C. 11312 & 11313
Information security	Ensuring agency compliance with the requirement to protect information and systems	44 U.S.C. 3506(g) and 3544(a)(3)
IT/IRM human capital	Helping agency meet IT/IRM workforce needs	44 U.S.C. 3506(b), 40 U.S.C. 11315(c)
Information collection/paperwork reduction	Reviewing agency information collection proposals to maximize the utility and minimize public paperwork burden	44 U.S.C. 3506(c)
Information dissemination	Ensuring that information dissemination activities meet policy goals such as timely and equitable public access to information	44 U.S.C. 3506(d)
Records management	Ensuring that agency implements and enforces records management policies and procedures under the Federal Records Act	44 U.S.C. 3506(f)
Privacy	Ensuring agency compliance with the Privacy Act and related laws	44 U.S.C. 3506(g)
Statistical policy and coordination	Performing statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes	44 U.S.C. 3506(e)
Information disclosure	Ensuring appropriate information access under the Freedom of Information Act	44 U.S.C. 3506(g)
Enterprise architecture[a]	Developing and maintaining the enterprise architecture defining the agency's mission and the information and IT needed to perform it	OMB guidance
Systems acquisition, development, and integration[a]	Controlling the acquisition, development, and integration of IT systems	44 U.S.C. 3506(h)(5), 40 U.S.C. 11312

Area of responsibility	Description	Applicable laws
E-government initiatives[a]	Supporting initiatives to use IT to improve government services to the public and internal operations	44 U.S.C. 3506(h)(3), E-Government Act of 2002, other laws and guidance

Source: GAO analysis.

[a]The last three areas of responsibility—enterprise architecture; systems acquisition, development, and integration; and e-government initiatives—are not assigned to CIOs by statute; they are assigned to the agency heads by law or guidance. However, in virtually all agencies, the agency heads have delegated these areas of responsibility to their CIOs.

According to our report, CIOs were generally responsible for the key information and technology management areas shown in the table, although not all CIOs were completely responsible for all areas.[13] For example:

- All the CIOs were responsible for five areas (capital planning and investment management, enterprise architecture, information security, IT/IRM strategic planning, and IT workforce planning).
- More than half had responsibility for six additional areas (systems acquisition, major e-government initiatives, information collection/paperwork reduction, records management, information dissemination, and privacy).
- Fewer than half were responsible for two areas (information disclosure and statistics).

It was common for CIOs to share responsibility for certain functions, and in some cases responsibilities were assigned to other offices. For example, systems acquisition responsibility could be shared among the CIO and other officials, such as a procurement executive or program executive; disclosure could be assigned to general counsel and public affairs, while statistical policy could be assigned to offices that deal with the agency's data analysis.[14] Nevertheless, even for areas of responsibility that were not assigned

[13] The acting CIO at VA at the time of the review responded that the CIO was responsible for all the activities except for statistical policy and coordination.

[14] This is particularly the case in agencies that contain Principal Statistical Agencies, such as the Bureau of Economic Analysis (Department of Commerce), Bureau of Justice Statistics (Department of Justice), Bureau of Labor Statistics (Department of Labor), and others.

to CIOs, agency CIOs generally reported that they contributed to the successful execution of the agency's overall responsibilities in that area.

In carrying out their responsibilities, CIOs generally reported to their agency heads. The Paperwork Reduction Act—as well as our guidance[15]—generally calls for CIOs to report to their agency heads,[16] forging relationships that ensure high visibility and support for far-reaching information management initiatives. For 19 of the agencies in our review, the CIOs stated that they had this reporting relationship. In the other 8 agencies, the CIOs stated that they reported instead to another senior official, such as a deputy secretary, under secretary, or assistant secretary. In addition, 8 of the 19 CIOs who said they had a direct reporting relationship with the agency head noted that they also reported to another senior executive, usually the deputy secretary or under secretary for management, on an operational basis. According to members of our Executive Council on Information Management and Technology,[17] what is most critical is for the CIO to report to a top level official.

Tenure and Backgrounds of CIOs

Federal CIOs often remained in their positions for less than the length of time that some experts consider necessary for them to be effective and implement changes. At the major departments and agencies included in our review, the median time in the position of permanent CIOs whose time in office had been completed was about 23 months.[18] For career CIOs, the median was 32 months; the

[15] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

[16] The Homeland Security Act of 2002 states that the CIO for the Department of Homeland Security shall report to the Secretary of Homeland Security or to another official as directed by the Secretary. As allowed by the law, the Secretary has directed the CIO to report to the Under Secretary for Management.

[17] This panel of industry, state government, and academic experts provides outside expertise to GAO on information technology issues.

[18] We did not include acting CIOs in this calculation, unless the acting CIO was later put in the permanent position. We calculated tenure since the enactment of the Clinger-Cohen Act (1996).

median for political appointees was 19 months. To the question of how long a CIO needed to stay in office to be effective, the most common response of the CIOs (and former agency IT executives whom we consulted) was 3 to 5 years. Between February 10, 1996, and March 1, 2004, only about 35 percent of the permanent CIOs who had completed their time in office reportedly had stayed in office for a minimum of 3 years. The gap between actual time in office and the time needed to be effective is consistent with the view of many agency CIOs that the turnover rate was high, and that this rate was influenced by the political environment, the pay differentials between the public and private sectors, and the challenges that CIOs face.

In contrast, the CIOs interviewed for our report were generally helped in carrying out their responsibilities by the background and experience they brought to the job. The background of the CIOs varied in that they had previously worked in the government, the private sector, or academia, and they had a mix of technical and management experience. However, virtually all had work experience or educational backgrounds in IT or IT-related fields; 12 agency CIOs had previously served in a CIO or deputy CIO capacity. Moreover, most of the them had business knowledge related to their agencies because they had previously worked at the agency or had worked in an area related to the agency's mission.

Success Factors and Challenges of CIOs

To allow CIOs to serve effectively in the key leadership role envisioned by the Congress, federal agencies must use the full potential of CIOs as information and technology management leaders and active participants in the development of the agency's strategic plans and policies. The CIOs, in turn, must meet the challenges of building credible organizations and developing and organizing information and technology management capabilities to meet mission needs.

In February 2001, we issued guidance[19] on the effective use of CIOs, which describes the following three factors as key contributors to CIO success:

- Supportive senior executives embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision making.
- Effective CIOs have legitimate and influential roles in leading top managers to apply IT to business problems and needs. Placement of the position at an executive management level in the organization is important, but in addition, effective CIOs earn credibility and produce results by establishing effective working relationships with business unit heads.
- Successful CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with knowledge of business processes, market trends, internal legacy structures, and available IT skills, this understanding is necessary to ensure that the CIO's office is aligned to best serve agency needs.

The CIO study that we reported on in July 2004 also provides information on the major challenges that federal CIOs face in fulfilling their duties.[20] In particular, CIOs view IT governance processes, funding, and human capital as critical to their success, as indicated by two challenges that were cited by over 80 percent of the CIOs: implementing effective information technology management and obtaining sufficient and relevant resources.

- *Effective IT management.*

  Leading organizations execute their information technology management responsibilities reliably and efficiently. A little over 80 percent of the CIOs reported that they faced one or more challenges related to implementing effective IT management practices at their agencies. This is not surprising given that, as we have previously

[19] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

[20] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

reported, the government has not always successfully executed the IT management areas that were most frequently cited as challenges by the CIOs—information security, enterprise architecture, investment management, and e-gov.[21]

- *Sufficient and relevant resources.*
  One key element in ensuring an agency's information and technology success is having adequate resources. Virtually all agency CIOs cited resources, both in dollars and staff, as major challenges. The funding issues cited generally concerned the development and implementation of agency IT budgets and whether certain IT projects, programs, or operations were being adequately funded.

  We have previously reported that the way agency initiatives are originated can create funding challenges that are not found in the private sector.[22] For example, certain information systems may be mandated or legislated, so the agency does not have the flexibility to decide whether to pursue them. Additionally, there is a great deal of uncertainty about the funding levels that may be available from year to year.

  The government also faces long-standing and widely recognized challenges in maintaining a high-quality IT workforce. In 1994 and 2001, we reported on the importance that leading organizations placed on making sure they had the right mix of skills in their IT workforce.[23] About 70 percent of the agency CIOs reported on a

[21] See, for example, GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: Jan. 1, 2003); *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, GAO-04-49 (Washington, D.C.: Jan. 12, 2004); *Information Technology: Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts*, GAO-04-40 (Washington, D.C.: Nov. 17, 2003); and *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-03-95 (Washington, D.C.: January 2003).

[22] GAO, *Chief Information Officers: Implementing Effective CIO Organizations*, GAO/T-AIMD-00-128 (Washington, D.C.: Mar. 24, 2000).

[23] GAO, *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1, 1994) and GAO-01-376G.

number of substantial IT human capital challenges, including, in some cases, the need for additional staff. Other challenges included recruiting, retention, training and development, and succession planning.

In addition, two other commonly cited challenges were communicating and collaborating (both internally and externally) and managing change.

- *Communicating and collaborating.*
  Our prior work has shown the importance of communication and collaboration, both within an agency and with its external partners. For example, one of the critical success factors we identified in our guide focuses on the CIO's ability to establish his or her organization as a central player in the enterprise.[24] Ten agency CIOs reported that communication and collaboration were challenges. Examples of internal communication and collaboration challenges included (1) cultivating, nurturing, and maintaining partnerships and alliances while producing results in the best interest of the enterprise and (2) establishing supporting governance structures that ensure two-way communication with the agency head and effective communication with the business part of the organization and component entities. Other CIOs cited activities associated with communicating and collaborating with outside entities as challenges, including sharing information with partners and influencing the Congress and OMB.

- *Managing change.*
  Top leadership involvement and clear lines of accountability for making management improvements are critical to overcoming an organization's natural resistance to change, marshaling the resources needed to improve management, and building and maintaining organizationwide commitment to new ways of doing business. Some CIOs reported challenges associated with implementing both changes originating from their own initiative and changes from outside forces. Implementing major IT changes can

[24] GAO-01-376G.

involve not only technical risks but also nontechnical risks, such as those associated with people and the organization's culture. Six CIOs cited dealing with the government's culture and bureaucracy as challenges to implementing change. Former agency IT executives also cited the need for cultural changes as a major challenge facing CIOs. Accordingly, in order to effectively implement change, it is important that CIOs build understanding, commitment, and support among those who will be affected by the change.

Effectively tackling these reported challenges can improve the likelihood of a CIO's success. Until these challenges are overcome, federal agencies are unlikely to optimize their use of information and technology, which can affect an organization's ability to effectively and efficiently implement its programs and missions.

Roles and Responsibilities of the CIO Position at VA Have Evolved over Time

Since enactment of the Clinger-Cohen Act in 1996, the roles and responsibilities of VA's Chief Information Officer have evolved. From lacking a CIO entirely, the department has taken steps to address the challenges posed by its multiple widespread components and its decentralized information technology and services.

In June 1998, VA assigned CIO responsibility to a top manager.[25] However, we reported in July 1998[26] that the person holding the CIO position at VA had multiple additional major responsibilities, as this person also served as Assistant Secretary for Management, Chief Financial Officer, and Deputy Assistant Secretary for Budget. According to the act, the CIO's primary responsibility should be information and technology management. Noting that VA's structure

[25] Section 5604 of the Clinger-Cohen Act specifically created the position of Chief Information Officer at VA effective August 8, 1996. See 38 U.S.C. § 310.

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

was decentralized, its IT budget was large, and its CIO faced serious information and technology management issues, we recommended that the Secretary appoint a CIO with full-time responsibilities for IRM. Concurring with the recommendation, VA established the position of Assistant Secretary for Information and Technology to serve as its CIO.

As of May 2000, however, the position of Assistant Secretary for Information and Technology was vacant, and as we reported at the time,[27] it had been unfilled since its creation in 1998. The Secretary then created and filled the position of Principal Deputy Assistant Secretary for Information and Technology, designating that person as VA's acting CIO until an Assistant Secretary could be appointed. The Secretary also realigned IRM functions within VA under this position, which reported directly to the Secretary.

As we reported,[28] the Principal Deputy Assistant Secretary was involved in IT planning issues across the department. In addition to advising the Secretary on IT issues, he served as chair of the department's CIO Council and as a member of the department's Capital Investment Board, and he worked with the CIOs in VBA and VHA (at the time, NCA had no CIO). According to this official, one of his priorities was to ensure that IT activities in VBA and VHA were in concert with VA's departmentwide efforts.

In August 2001, VA filled the CIO position. In March 2002,[29] we testified that this hiring was one of the important strides that the Secretary of Veterans Affairs had made to improve the department's IT leadership and management, along with making a commitment to reform the department's use of IT.

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

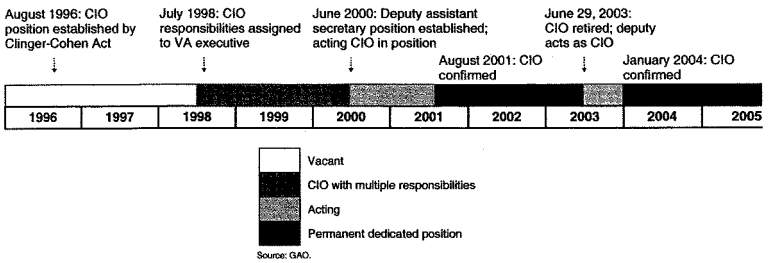
[28] GAO, *Information Technology: Update on VA Actions to Implement Critical Reforms*, GAO/AIMD-00-74 (Washington, D.C.: May 11, 2000).

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

On June 29, 2003, the CIO retired after a tenure of almost 2 years (about the median length of tenure for federal CIOs, as discussed above); the current CIO was confirmed in January 2004.

Figure 1 is a time line showing the history of the CIO position at VA since the passage of the Clinger-Cohen Act.

Figure 1: Time Line of CIO Tenure at VA



Source: GAO.

VA Proposed to Realign its IT Organization in Response to IT Management Challenges

Our prior work highlighted some of the challenges that the CIO faced as a result of the way the department was organized to carry out its IT mission.[30] Among these challenges was that information systems and services were highly decentralized, and the VA administrations and staff offices controlled a majority of the department's IT budget. For example, in VA's information technology budget for fiscal year 2002 of approximately $1.25 billion, VHA controlled about $1.02 billion (over 80 percent), whereas the department level controlled about $60.2 million (less than 5 percent).

[30] GAO, *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist*, GAO-01-550T (Washington, D.C.: Apr. 4, 2001) and *VA Information Technology: Progress Made, but Continued Management Attention Is Key to Achieving Results*, GAO-02-369T (Washington, D.C.: Mar. 13, 2002).

In addition, we noted that there was neither direct nor indirect reporting to VA's cyber security officer—the department's senior security official—thus raising questions about this person's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. The more than 600 information security officers in VA's three administrations and its many medical facilities throughout the country were responsible for ensuring the department's information security, although they reported only to their facility's director or to the chief information officer of their administration.

Given the large annual funding base and decentralized management structure, we testified that it was crucial for the departmental CIO to ensure that well-established and integrated processes for leading, managing, and controlling investments are commonplace and followed throughout the department. This is consistent with the finding in our CIO review that implementation of IT management practices was a challenge; over half of federal CIOs identified IT investment management specifically.

Recognizing weaknesses in accountability for the department's IT resources and the need to reorganize IT management and financing, the Secretary announced a realignment of the department's IT operations in a memorandum dated August 2002. According to the memorandum, the realignment would centralize IT functions, programs, workforce personnel, and funding into the office of the department-level CIO. In particular, several significant changes were described:

- The CIOs in each of the three administrations—VHA, VBA, and NCA—were to be designated deputy CIOs and were to report directly to the department-level CIO. Previously, these officials served as component-level CIOs who reported only to their respective administrations' under secretaries.
- All administration-level cyber security functions were to be consolidated under the department's cyber security office, and all monies earmarked by VA for these functions were to be placed under the authority of the cyber security officer. Information

security officers previously assigned to VHA's 21 veterans integrated service networks[31] would report directly to the cyber security officer, thus extending the responsibilities of the cyber security office to the field.

- Beginning in fiscal year 2003, the department-level CIO would assume executive authority over VA's IT funding.

In September 2002,[32] we testified that in pursuing these reforms, the Secretary demonstrated the significance of establishing an effective management structure for building credibility in the way IT is used, and took a significant step toward achieving a "One VA" vision. The Secretary's initiative was also a bold and innovative step by the department—one that has been undertaken by few other federal agencies. For example, of 17 agencies contacted in 2002, 8 reported having component-level CIOs, none of which reported to the department-level CIO. Only one agency with component-level CIOs reported that its department-level CIO had authority over all IT funding.

We also noted that the CIO's success in managing IT operations under the realignment would hinge on effective collaboration with business counterparts to guide IT solutions that meet mission needs, and we pointed out the importance of the three key contributors to CIO success described in our 2001 guidance (discussed earlier).[33]

Although we have not reviewed the current status of this proposed realignment or VA's current organizational structure, it remains our view that the proposed realignment held promise for building a more solid foundation for investing in and improving the department's accountability over IT resources. Specifically, under

[31] The veterans integrated service network (VISN) is the basic budgetary and planning unit of the veterans health care system. Funding and other resources are distributed through the VISN. Each VISN covers a geographic area that encompasses a population of veteran beneficiaries.

[32] GAO, *VA Information Technology: Management Making Important Progress in Addressing Key Challenges*, GAO-02-1054T (Washington, D.C.: Sept. 26, 200s).

[33] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).

the realignment the CIO would assume budget authority over all IT funding, including authority to veto proposals submitted from subdepartment levels. This could have a significant effect on VA's accountability for how components are spending money.[34]

To sum up, the CIO plays a vital role in ensuring that VA's funds are well spent and in managing information technology to serve our nation's veterans. In our view, the realignment of VA's IT organization proposed in 2002 held promise for improving accountability and enabling the department to accomplish its mission. The additional oversight afforded the CIO could have a significant impact on the department's ability to more effectively account for and manage its proposed $2.1 billion in planned IT spending.

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

Contacts and Acknowledgements

For information about this testimony, please contact Linda D. Koontz, Director, Information Management Issues, at (202) 512-6240 or at koontzl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Barbara Collier, Lester Diamond, Barbara Oliver, and Eric Trout.

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

8405 Greensboro Drive, 6th Floor
McLean, VA 22102

Telephone: +1-703-226-4700
Facsimile: +1-703-226-4702
gartner.com

Gartner.

14 September 2005

The Honorable Steven Buyer
Chairman, House Committee on Veterans Affairs
U.S. House of Representatives, 109th Congress
335 Canon House Office Building
Washington, DC 20515

Mr. Chairman:

On behalf of Gartner Inc., I am honored to submit my testimony for inclusion in the formal record regarding the Department of Veterans Affairs (VA) information technology infrastructure reorganization.

The attachment contains my written testimony. As a nongovernmental witness I have also included a copy of my biography, and information on my organization including a statement disclosing the amount of all contracts with the VA during the past two fiscal years by Gartner. All information is provided to the best of my abilities.

I look forward to sharing my insights and recommendations to improve the information technology organization within the VA.

Sincerely,

Michael Pedersen

Michael Pedersen
Managing Vice President
Gartner Consulting

Attachment: Written testimony, Gartner Disclosure, Witness Biography

Written Testimony
Michael L. Pedersen
Managing Vice President, Gartner Consulting

Mr. Chairman and members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing regarding the Department of Veterans Affairs (VA) information technology (IT) reorganization.

I am a Managing Vice President within the consulting division at Gartner, the leading provider of research and analysis on the global information technology industry. Unlike many of our competitors, Gartner does not offer implementation services that would compromise our independence and objectivity. I have over 20 years of experience in developing and deploying IT to fulfill business and mission objectives. My specific expertise is in IT governance, investment management and organizational redesign — services that support the performance improvement efforts of IT organizations.

Gartner Consulting[1] partnered with Topgallant Partners in October 2004 to pursue an open solicitation to assess whether the VA's IT personnel assets are appropriately aligned to efficiently deliver world-class IT program management, operational support and systems design and development services. The Topgallant Partners/Gartner team was awarded a contract in December 2004 for this assessment. I was the lead consultant and subject matter expert on this assessment and directed the activities to fulfill the contract objectives and deliver the results in close cooperation with Topgallant Partners. The balance of my testimony provides the key findings from our assessment, our supporting analysis and recommendations for the VA to appropriately align its IT personnel. This information is drawn directly from the detailed project deliverables and executive summary submitted to the VA, and was presented to VHA, VBA and NCA senior management in addition to the Secretary and Deputy Secretary.

The Purpose of Our Assessment

The Department of Veterans Affairs Office of Information & Technology (OI&T) and related VA IT organizations support a large, complex, well-performing, but ultimately aging set of infrastructure, applications and support technologies. OI&T has launched a OneVA Departmental initiative to buttress and grow OI&T's ability to contribute to the VA's successful completion of its mission.

This organizational assessment project is a first step toward measurably increasing VA IT's *Value For Our Vets* — that is, for demonstrably growing VA IT's ability to develop and deploy new, veteran-centric systems despite flat or declining budgets.

Our assessment first baselined how VA IT operates today. We then identified organizational models that increase VA IT's value: models that offer greater efficiencies, economies of scale, and value add back to the mission. We then charted the path VA IT can follow to deploy its new organizational model. At its conclusion we proposed a new organization that truly delivers Value For Our Vets.

A three (3) phase assessment was undertaken by Gartner Consulting:

1. Define an "As Is" perspective of the VA's current organizational capability;
2. Identify Potential "To Be" Organizational Models that appropriately align IT personnel assets; and,
3. Create an Implementation Plan to identify the critical activities to transition to the recommended organization.

Schedule and Process

Work was begun in January 2005 with deliverables formally submitted in May 2005. During the course of this contract, extensive data collection, interviewing, surveying and analysis was conducted. The need to

[1] Contract was awarded to the team of Topgallant Partners and META Group Consulting. META Group was subsequently acquired by Gartner in April 2005 during this assessment.

have an accurate understanding of the issues at the VA was balanced with the practical nature of conducting the assessment in a timely and cost-effective manner for the VA. To that end our efforts led us to:

- Interview 72 staff among VA business executives, IT executives and staff within all three Administrations and OI&T itself. These interviews formed the basis to identify issues with current organizational structure that hinders IT performance improvement efforts. We offered to interview as many staff as the Administrations believed were necessary to fully understand their environment and issues, and extended the project by 30 days to schedule and conduct these additional interviews. These interviews occurred at VA hospitals, regional offices and field offices throughout the United States.

- Survey 110 IT staff to profile their work activities. These profiles allow staff to self-select the amount of time spent on mission-driving work, compensating work, and non-mission driving work.

- Survey 27 IT staff regarding their deployment of enterprise architecture and planning process relative to leading practice as defined by Gartner. The survey submissions were compared to Gartner's database of leading firms to gauge VA's maturity in deploying enterprise architecture planning relative to the broad marketplace.

- Conduct workshops with key functional leaders within VHA, VBA, NCA and OI&T regarding their perspectives on the functional responsibilities they require to be effective in supporting the VA's mission.

While the number of participants who provided input to our study is small relative to the overall number of VA staff, the Topgallant/Gartner team offered and was directed by each Administration to interview and survey specific business and technology executives. The team "went where the Administrations directed" to engage staff who were best positioned to give us the information necessary to make informed decisions. It is our position that this data collection fairly and accurately represents the VA's situation.

Topgallant Partners/Gartner "As Is" Findings

We conducted a thorough "As-Is" analysis of VA IT during the first phase of this contract. Key findings from our "As-Is" analysis are summarized below across five (5) key analysis domains:

1. Functional Analysis
2. Organizational Analysis
3. Issues Analysis
4. Strategic Analysis
5. Enterprise Architecture Analysis

Our findings within each analysis domain are as follows.

Functional Analysis

Functional Analysis gauges how responsibility for core IT functions are distributed across an IT organization. This analysis gives insight into 'who does what', providing the framework needed to create a more efficient, more effective "To Be" IT organization.

Functional Analysis Key Findings

Excessive duplication of IT assets and inefficiencies exists within VA IT. The Functional Analysis indicates that VA IT is a "self-replicating" organization, creating internal (though surmountable) barriers for improvement opportunities. All core IT functions are performed nationally by organizations within VA IT. Additionally, within VBA and VHA, core IT functions are delivered by regional or local organizations (e.g., VISNs, Medical Centers). These distinct IT service delivery organizations operates independently based

on reporting structure employing formal and informal collaboration with other local and regional organizations within the Administrations. OI&T and Administration IT organizations have developed policies and standards to guide product development and service delivery for their customer base. Initial portfolio management, enterprise architecture, and security governance processes are under way within VA IT.

VA Implication

The OneVA mission (as defined in the 2003–2008 Strategic Plan for Employees) will require significant time and cost to realize in the current IT model given the different operating models in place throughout the VA IT organizations.

Organizational Analysis

Organizational analysis examines how an IT organization functions today with regard to people and processes. Using anecdotal insights gained from interviews and process information gained from surveys and document reviews, this analysis results in a high-level picture of the organization's culture embodied in distinct norms as well as its performance history. This portrait of the organization is a foundation for building a successful change management plan in any arena, but especially where culture is a critical enabler of success. We characterize norms as the implicit, thoroughly accepted ground rules that substantially shape how an organization acts, both internally and toward the external world. Norms are the product of an organization's history and environment. They evolve slowly; most often reflecting behaviors learned when the organization was performing well and largely content or during periods when undue stresses tested the organization and its personnel.

Organizational Analysis Key Findings

The VA IT Organizational Analysis indicated that four powerful norms substantially shape how VA IT currently operates. These norms are outlined below with additional detail and the implication that all of these norms, when considered together have on the organization:

1. **One Voiced Mission, Many Methods**

   The VA IT Organizational Analysis revealed that there is a broadly stated (though informally defined) mission that bonds all VA employees, regardless of function or hierarchical level: "Serve the Veteran." While each area of the organization embraces this broadly-stated mission, there are significant differences in how each area believes that goal should be accomplished.

   The lack of underlying principles to bind the organization to a mission (whether clearly stated by the Department or not) leads to differences between month-to-month (even year-to-year) priorities, goals and planning. This was pervasive and repeatedly observed at all levels of the organization. This is especially true when looking from the field to centralized functions.

2. **Investment (in) Accountability**

   Budgets are very fluid in the VA and — beyond the big numbers — there's not much accountability for how and when money is spent. Budgets are stretched as the organization sees fit. If you don't have the money you need, there's a likelihood you can get it by working your connections, so money is simply shifted. This allows managers to build and operate individual IT operations.

   Everyone agrees that budgets/money should be tracked and accountability should be attached but there's a fundamental difference in what that means to various groups of people. The result is an inability to capture, track and influence IT investments across the VA as a whole.

3. **Relationships Rule**

   While there are processes and rules in place for major IT functions (e.g., budgeting, project management) assets within the VA ebb and flow, based on needs that arise. The organization is relatively agile and responsive, with most assets being centered within the healthcare aspects of the business.

A large portion of the population within VA IT is comprised of long-tenure employees — they "grew up" in the VA world. Therefore, they learned an appropriate set of skills to be successful, skills centered on negotiation, flexibility and working your relationships with others. Political appointees have short tenure, so the CIO leadership is generally viewed as temporary and ineffective.

4. **Everyone Owns Assets**

   Since success was primarily built on relationships & fluid budgets, leaders throughout the VA built "mini-organizations" (self-replicating), where all assets - both people and technology - were within arm's reach. This way, if there was a need or problem, a leader could reach out (literally, if necessary) to the responsible party. Thus, a cultural norm was created — higher proximity to assets equals better service and responsiveness.

VA Implication

We observed that these norms allow VA IT to be the IT organization it chooses to be. We do not doubt VA IT personnel's commitment to the mission of VA. However, organizations within VA IT are allowed a variety of methods to fulfill the mission, enjoy flexible budgets, adopt informal ways of work, and have access to assets. Further, the current norms allow IT personnel to believe that they, and only they, can deliver against the mission. So people act accordingly, replicating assets and activities at all levels of the organization. Ironically, their desire to deliver – to serve the Veteran - creates enormous duplication and inefficiencies because of the norms in place.

Role specialization, centralized functions, common methodology, reusability, and standardization are viewed as risky in the current environment because these methods decrease the perceived power any one individual has over his or her own work. There is no doubt that resources are wasted funding a self-replicating IT organization.

Issues Analysis

The Issues Analysis highlights the key performance, operating, and organizational issues identified by VA personnel during in-person interviews. Issues were analyzed and prioritized by our project team to reflect the degree to which the comments reflect how VA IT delivers against its mission

Issues Analysis Key Findings

The Issues Analysis highlighted three key findings:

1. Lack of alignment between OI&T and the Administrations — Issues identified by OI&T personnel correlate very weakly with those identified by Administration personnel. Interestingly, though, issues identified by Administration personnel correlate very well across the three Administrations. These data points confirm that OI&T's view of the world differs markedly from that shared by the Administrations
2. Intensely self-referential nature of the majority of expressed concerns — Of the Top 10 Issues identified during our interviews, nine of 10 issues identified by VA IT personnel relate specifically to OI&T itself. Only one "business issue" made the Top 10 list.
3. Defensive Nature of the Administrations' current relationship with OI&T — We observed that there were few issues shared by all groups. Those issues shared by most groups largely continued the "everything must be local" argument. VA IT personnel feel they are *forced* to do everything at every level, otherwise their work will not be done. They must *defend* their right to do the work they think they should do.

Most importantly, this Issues Analysis highlights just how difficult it will be to make VA IT less of a self-replicating IT organization. We believe that the norms that allow VA IT to replicate assets and activities at all levels must be addressed before VA IT's leadership can successfully redress the imbalances currently observed across VA IT.

VA Implications

This Issues Analysis highlights just how difficult it will be to make VA IT less of a self-replicating IT organization. The lack of alignment between OI&T's concerns and the Administrations' concerns shows just how differently the Administrations view the world than OI&T does. The self-concerned nature of everyone's perspective gives an acute appreciation that "who does what" is a central issue for everyone across VA IT.

The energy with which individuals defend what their organization does — or should do — sharply underscores the emotional investment to current modes of organization and operation. We believe that the efforts to centralize specific sets of currently dispersed assets or activities, will engender enormous, heartfelt, but ultimately destructive, responses if not managed by the VA leadership directly. The norms that allow VA IT to replicate assets and activities at all levels must be addressed before VA IT's leadership can successfully redress the imbalances currently observed across VA IT.

Strategic Analysis

Strategic Analysis measures the degree to which the work currently completed by each part of VA IT actually contributes to the successful completion of our mission and identifies potential efficiencies and savings that can be realized through work changes.

Strategic Analysis Key Findings

The VA IT Strategic Analysis indicates that VA IT personnel spend 27 percent of their time on work that directly contributes to VA IT's successful completion of mission. Over one-half of their time is spent on work that does not contribute to mission; most of this work is related to internal administration. The participating VA IT personnel also spend very little time interacting with customers. We believe that achievable reductions in work that does not drive mission can help VA IT substantially improve your Value to the Vets.

VA Implications

The IT organization needs to gain a substantial increase in the proportion of work that is directly aligned with VA IT's mission. This implies a proportionate decrease in work that does not contribute to your mission, including substantial reductions in Non-Mission driving work and similar reductions in Compensating work. How? Define the major IT processes using industry standard models (e.g., ITIL) then challenge the organization to reduce the work that does not contribute directly to mission. Led correctly, we've seen organizations achieve significant, measurable improvements in six to nine months.

Enterprise Architecture Analysis

Enterprise Architecture (EA) is a top-down, business strategy driven planning process designed to bridge the gap between an organization's future-focused business strategy and the portfolio of IT efforts that will support that strategy. Our analysis sought to assess VA IT senior staff's alignment with the key dimensions of EA. The stronger the alignment (represented by maturity scale) the greater the potential for success in future planning efforts.

Enterprise Architecture Analysis Key Findings

Analysis of the VA's response to the Enterprise Architecture Survey indicates a positive, markedly higher belief in the role and use of enterprise architecture across the VA IT than expected based on interviews. The word "belief" in part reflects that these are unvalidated responses vs. observed behaviors from a detailed study. Nonetheless, as the survey defines enterprise architecture as a planning process, this indicates the VA's IT organization has a strong understanding of the importance of such activities relative to other organizations with similar challenges. This is an encouraging sign from which to build long-term, sustainable value from IT initiatives that can be directly applied back into the VA's challenge in creating Value For Our Vets.

VA Implications

The VA has established an enterprise-wide understanding of strategic planning as evidenced in above average maturity rating. Though above average, the (unvalidated) ratings do not represent a level of maturity required to consistently delivery business value from complex IT initiatives (e.g., HDR, data center consolidation). We believe that efforts to strengthen inter-Administration planning efforts (by further developing the VA's enterprise architecture program) are critical to value delivery. Such efforts, when successful, frame a future IT state that key stakeholders in OI&T and Administration IT can identify and embrace independent of organizational structure.

The summary of the "As Is" Analysis is that change is required to meet an emerging imperative — Value For Our Vets — that is demonstrably growing VA IT's ability to develop and successfully deploy new, *veteran-centric* systems despite flat or declining budgets.

Topgallant Partners/Gartner "To Be" Analysis

The Topgallant Partners/Gartner team used the "As Is" baseline, leading industry practice in commercial and government organizations, and emerging IT trends to evaluate potential "to Be" models for the VA that have potential to mitigate the issues established within the "as Is" baseline.

A useful guide in determining appropriate information technology organizational models for the VA is to consider the VA's Value Discipline.[1] This useful business planning approach argues that no firm can be "all things to all people." Customers – in this case, the end users of the IT services - control the marketplace and their expectations of value are rising rapidly and changing, based on past performance. Organizations must choose one value discipline in which to excel while reaching market parity in the other two disciplines. Selecting a discipline is "a central act that shapes every subsequent plan a company makes."

To change the VA IT's orientation from servicing the Veteran to Value For Our Vets, the IT organization must excel in the Customer Intimacy discipline and attain parity in Operational Excellence and Product Leadership. This requires substantial changes in the manner in which VA's IT organization is structured in addition to its supporting organizational constructs. Customer intimacy involves not only a change in organizational structure but also in the underlying work processes, staff role definitions, the outcome of its work (IT Services), measurement framework and a new culture. All told, these dimensions include:

1. Organizational Structure — the structure in which the IT organization delivers value at a risk level that is tolerable to the Department and best supports the OneVA mission
2. Processes — the critical IT processes and their interfaces required for customer intimate IT delivery
3. Roles — the IT management practices, roles, and accountabilities required for customer-intimate IT delivery
4. IT Services — Define the IT services that are valued and readily understood by the VA's business community
5. Guiding Principles — the IT policies that establish focus, governance, and a decision-making fabric within and between VA's IT and business communities
6. Performance Management — the high-level analysis of IT performance relative to peers in government, insurance, and healthcare
7. Culture and Norms — the changes required in the underlying culture and norms to effect behavior change

Our "To Be" analysis presented insights, options and recommendations within each of the seven dimensions and are outlined below.

---

[1] *The Discipline of Market Leaders,* Treacy and Wiersema, 1995, Addison Wesley

Organizational Structure

Several organizational models (including no change – the status quo) were analyzed to resolve the issues uncovered within the VA. Two models had the greatest potential application at the VA:

1. Federated — where centralized planning, technology operations (e.g., data centers, networks) and budgeting/financial are controlled by a Chief Information Officer (CIO) with Business applications developed and supported by application teams in each business line (e.g., Medical Care, Pension, Housing, Finance). A governance process with strong investment management practices guides the alignment between these groups.
2. Centralized — where all VA IT is organized into single entity reporting to a Chief Information Officer (CIO). Key functional entities reporting directly to the CIO include business applications, infrastructure & operations, customer relations (advocates for the business), enterprise architecture, data & information management, security management, and IT finance.

Federated Model Benefits— Several benefits may be attained by implementing this model at the VA. These include allowing business leaders to develop the application portfolio unique to their missions; achieve economies of scale across all VA by managing the infrastructure through a central function (assuming the consolidation of physical assets); and allowing the business unit IT team to be responsive to Administration mission demands.

Federated Model Risks— the risks to VA from this model include difficulty in attaining OneVA mission objectives because of the defined barriers in culture, unaligned investment priorities across Administrations, and differences in technology and process which hinders effort to create veteran-centric systems. This approach also requires sustained executive commitment to IT investment mgmt process (unattained to date within the VA), is a significant scope of change to manage given the intended consolidation of physical assets and is deemed a modest organization disruption. We expect such an effort will extend the envisioned VHA data center consolidation program to VA wide initiative; however, with the physical assets being currently under the control of local offices/regions ("Everyone owns assets" norm identified earlier) this itself will require significant change management effort.

Centralized Model Benefits— This approach provides the greatest opportunity to successfully execute OneVA mission objectives; it maximizes asset utilization (projects, staff, technology) and achieves economies of scale across all VA by managing the infrastructure through a central function; and through common organization will more rapidly mature the IT investment management process across VA's IT program portfolio.

Centralized Model Risks— The potential risks from implementing this model are of course the significant organizational disruption and scope to manage (it is a big bang). It also increases the complexity for the centralized organization to align its resources with Administration mission priorities e.g., strong portfolio mgmt required); requires strong user orientation (e.g., service level agreements, IT service catalogs) to be successful which is not in place at VA. It is important to note that a chargeback mechanism is necessary (communicating costs against service level at a minimum; whether they are recovered or not) to ensure "value for the money" is established between the business and IT organizations.

Both the Centralization and the Federated options are viable organizational models to achieve OneVA mission objectives; however, our analysis shows that the Centralization option requires a shorter time horizon to attain similar benefits than the Federated option. The centralized model has the greater potential to realize efficiencies in IT delivery, improve mission program delivery success (e.g., VetsNet, HealtheVet), and establish a OneVA veteran-centric capability. All important elements to create Value for our Vets.

Success in the Federated option requires a highly-mature, well-functioning IT investment management process in order to align each Administration and OI&T. This alone is a significant change in identified norms that extends the time to benefit for this option.

Success in the Centralization option requires executive leadership to rapidly change the underlying processes and norms. Bringing assets under the control of a single CIO both accelerates the maturing of

the IT investment management process and improves the potential benefit realization from OneVA mission investments.

Given the poor state of the VA's IT investment management process and the stated demand to drive benefits over a shorter horizon (as defined in the VA Strategic Plan for Employees), we recommend the Centralization option to maximize the opportunity to create Value For Our Vets. The details of our study defined a functional-based organizational model for the VA. Transitioning from the status quo to the recommended centralized option is not a single event. It is a multi-phased program in itself to ensure minimal disruption in VA mission activities. It is important to note that given the significant cultural barriers in existence at the VA, third party services will be required to support the needed knowledge transfer, facilitation and oversight to achieve full realization in a timely fashion.

Processes

Our "As Is" analysis found for the most part, inconsistent and poorly documented processes without key performance indicators (KPIs). It is important to realize that process re-engineering leads not only to greater efficiency (do more with same resource levels) but also improvement in underlying service (being able to create consistency and quality in IT service delivery across different locations and organizational units). When common IT processes are used across the organization it creates consistency in management of the VA IT environment and better return on technology dollars. Before any changes are implemented we recommend that process re-engineering is undertaken across the primary processes that drive IT performance. Those processes include Service Level Management, Problem Management, Incident Management, Change Management, Configuration Management, Asset Management and Capacity Management

Our "To Be" model final state envisions documented, consistently applied processes; effective governance when modifying the processes; and, use of key performance indicators to ensure process performance and accountability during their delivery.

Roles

Even after VA IT establishes a new organizational structure, it still needs to specify where, and by whom, each IT service will be accomplished. Our "As-Is" analysis showed that IT activities are extensively duplicated across VA IT. The recommended organization structure requires that roles and responsibilities (with clearly assigned functional accountability) are assigned to minimize the duplication of activity.

IT Services

There are emerging efforts to formalize an "IT Services" approach (e.g., Austin Automation Center Franchise Fund, VISN Memorandums of Understanding) across the VA. These disparate efforts have several notable successes including Austin's franchise fund rates which appear consistent with industry pricing. However, the predominant approach is based on informal service definitions and service-level agreements with a "whatever it takes" orientation. This has led to local optimization at the expense of enterprise consistency and efficiencies.

We recommend that VA build on efforts in OI&T and field organizations to formally define its IT services, service levels and pricing and align these efforts with market expectations and Administration mission requirements.

Guiding Principles

IT policies (guiding principles in commercial sector) enhance organizational structure by creating a culture of interdependence among organizations; mitigating potential conflicts among differing goals, groups, and processes; and building a solid foundation for processes.

To guide the new organization structure, VA IT must define and implement a single set of institutionalized and accepted policies and performance standards. Defining a common and cohesive vision for VA IT through policy creation will guide the desired behavioral changes needed to become an even more veteran-centric organization, functioning as a single, comprehensive provider of technology services. Our

recommendations for VA IT policies chart the course for emerging norms including Alignment and Consistency, Value and Stewardship, Process and Outcomes and Mutual Accountability

Performance Management

Performance management is the basis from which IT value is measured and communicated to the VA business community. The lack of a consistent, enterprise performance management program puts the OneVA mission at risk by its inability to identify performance shortcomings and re-alignment necessary to drive IT initiatives.

The VA must develop a performance management program to complement the OneVA mission objectives. Performance management must be based on industry comparable performance levels and have at its core:

- Common measurement objectives, definitions and reporting structures built on a balanced scorecard approach
- Transparency in reporting to gain credibility and foster change
- Integration with the IT service catalog in addition to operational process maturity, and governance model execution

Culture and Norms

In the current state, culture is created by history and precedent. Culture then shapes how the organization actually works. Leaders cannot change culture and norms directly. Short of an overwhelming crisis, the power of precedent — "how we do things around here" — is far more powerful than any executive's orders.

Fortunately, though, leaders can control how an organization works. And changing how your organization actually works — revising how power and money flows across the organization, recasting how the underlying processes are linked together, and reinforcing and rewarding desired behaviors — will, over time, lead to improvements in VA's culture and norms.

The team envisioned four norms that the VA could consider as target states to support the centralization option:

1. Drive for Alignment and Consistency — Virtually everyone with whom we spoke agreed that alignment and consistency are beginning to emerge across VA IT. However, the pace of change needs to significantly increase to achieve alignment and consistency in the targeted areas of operations. Communications is critical during the transformation process.
2. Focus on Value and Stewardship — VA IT needs to better align the organization around the notion of Value For Our Vets. This begins with a renewed commitment to becoming measurably more efficient in the allocation and use of resources while increasing accountability for IT investments through executive-driven governance.
3. Focus on Process and Outcomes — Our "As-Is" analysis indicates that VA IT personnel rely excessively on personal relationships to get things done. VA IT needs to foster consistent processes across all IT functions and must commit to a common set of performance outcomes and metrics.
4. Drive for Mutual Accountability — Personal integrity and commitment to mission is observed across VA IT. However, VA IT needs to balance accountability for mission and accountability for the resources that are used to accomplish this mission. Better-defined processes (e.g., SDLC, ITIM, EA, delivery processes) support this emerging norm.

The Topgallant Partners/Gartner Transition Plan

The transition to any new organizational model will be difficult. Several formation guidelines have been defined to guide the VA's effort to the recommended centralization model:

- Minimize interruption to VA mission activities by managing risk inherent with change. This of course means no interruption to healthcare delivery and no slowdown or stoppage of benefit payments and servicing veterans
- Control change through formal, programmatic and executive-endorsed approach across clearly-defined work streams (e.g., EIB/budgeting, SDLC, service delivery, workforce planning)
- Authoritative team to monitor PMO and provide "ombudsman" for issue escalation
- Drive as fast as possible to new organizational structure (target 2007 budget cycle for implementation of new governance process on key IT investments)
- Recognize and resolve barriers to change; Be inclusive — drive change within and throughout VA, not through top down messaging alone
- Measure progress against a "Case for Change" to guide reprioritization of effort as well as staff communications
- Increase control of IT investments through centralization of VA's ITIM process and strengthened governance to better guide staff activities

These guidelines allowed us to frame a transition approach along four stages as follows:

Stage 1: Mobilize for Change (Estimated Duration: 30 days)

To minimize risk in implementing a new organization, this stage prepares VA for transformation by establishing the Transformation Program Office (PMO). This effort includes building the "Case for Change" — packaging of change for broad consumption throughout the VA by all staff, framing an IT operating model, establishing PMO governance, building the ongoing communications plan, and appointing the team to lead the program office.

Stage 2: Build the Foundation (Estimated Duration: 120 days)

To build the underlying framework for organizational transformation, this stage defines the IT operational, financial and management processes to manage the transformation to the new VA IT operating model. Also, workforce plans are developed into a single responsibility. The stage ends with a "community event" to roll out operating model to top ~500 IT managers.

Stage 3: Implement the Transition (Estimated Duration: 120 days)

To transform the organization to new VA IT operating model, the new organization structure is implemented and staff are re-assigned to new responsibilities; new operating model processes are piloted (e.g., SDLC, delivery processes); and, plans to rationalize hard assets (e.g., networks, servers, data centers) across all VA organizational entities is initiated.

Stage 4: Optimize for Value (Estimated Duration: on-going)

To realize Value For Our Vets, VA staff refine service delivery processes, workforce capabilities, and organizational responsibilities for continuous improvement of IT service delivery; performance measurement reporting provides feedback regarding needed changes.

Mr. Chairman, this concludes my statement. Thank you again for the opportunity to discuss such an important matter to support our veterans. I would be pleased to respond to any questions that you or other members of the Subcommittee may have at this time.

Gartner Organization Disclosure

Gartner, Inc. is the leading provider of research and analysis on the global information technology industry. Our goal is to support enterprises as they drive innovation and growth through the use of technology. We help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of technology.

Gartner clients trust in our rigorous standards that safeguard the independence and objectivity of our research and advice. With $894 million in revenue in 2004, and more than 45,000 clients and 75 locations worldwide, we are the clear market leader.

Gartner serves a global client base consisting primarily of chief information officers (CIOs) and other senior IT and business executives in corporations and government agencies. We also serve technology companies and the investment community.

Armed with trusted advice provided by Gartner, our clients can make better and more confident technology decisions that will enhance the performance and cost-efficiency of their IT infrastructure or support strategic business objectives such as innovation, growth or competitive advantage. We play a unique role in the marketplace, analyzing vast amounts of information on IT supply and demand. This analysis not only allows technology users to make smarter purchasing decisions, it also helps technology companies create products that better serve users' needs. Furthermore, by helping to make technology more valuable to our client organizations, we also make executives more valuable to their enterprises.

The foundation for all Gartner products is our independent research on IT issues. The findings from this research can be delivered through several different media, depending on a client's specific business needs, preferences and objectives:

- Gartner Intelligence — research content and advice for IT professionals, technology companies and technology investors in the form of reports, briefings or events.
- Gartner Executive Programs — peer networking services and membership programs designed specifically for CIOs and other senior executives.
- Gartner Consulting — customized engagements that allow CIOs and other business executives to apply our knowledge to their specific situation, with an emphasis on outsourcing, performance improvement and IT management

Gartner provides customized project consulting and strategic advice to CIOs and other senior business executives. Our consulting services are provided by 550 senior consultants and focus on selected areas that are critical to clients today. Unlike many competitors, Gartner does not offer implementation services that would compromise our independence and objectivity.

In addition to supporting the majority of the Fortune 500 commercial organizations, Gartner is also highly experienced in developing IT solutions that meet the unique challenges faced by federal agencies as they attempt to serve the public's needs. Budgeting, procurement and re-engineering are just some of the issues Gartner consultants have addressed in the public sector arena.

Our business with the VA across all its product lines (and inclusive of META Group) is approximately US$463,000 in fiscal 2004 and US$1,068,000 in fiscal 2005.

Witness Biography

Michael Pedersen is a Managing Vice President at Gartner Consulting, where he specializes in IT governance, value management (balanced scorecards, IT investment management) and organizational redesign — services that support the performance improvement efforts of IT organizations. His skill is in applying leading go-to-market practices at large, end-user organizations to support a business-oriented approach to IT service delivery. His responsibilities at Gartner Consulting involve managing its Eastern region consulting organization including business development, client delivery and associate development.

Mr. Pedersen joined Gartner in April 2005 with the acquisition of META Group, where he spent 11 years. He most recently led its Americas region consulting business, reporting directly to its CEO. Previously, he worked at Ernst & Young and Booz-Allen Hamilton in technology planning capacities for commercial and government clients. Mr. Pedersen received a B.S. in physics from Clarkson College of Technology in 1983 and an M.S. in computer science from Brooklyn Polytechnic in 1988.

Statement of
Gordon H. Mansfield
Deputy Secretary
Department of Veterans Affairs
Before the
Committee on Veterans' Affairs
U.S. House of Representatives
September 14, 2005
****

Thank you, Mr. Chairman. I am pleased to appear before this Committee on behalf of the Secretary and the Department to discuss with you the Department of Veterans Affairs (VA) information technology infrastructure reorganization assessment.

The Department's business is the health and well-being of our nation's veterans. To ensure mission success, it is imperative that we employ all means at our disposal, including information technology, in the most effective way possible.

Some history of how VA's IT infrastructure and organization have evolved may prove useful to the Committee. For at least 25 years prior to 1990, VA's IT program was centralized. VA was elevated to cabinet level in 1988, and in FY 1989 the VA IT organization was led by an Assistant Secretary for Information Resources Management. In July 1990, under a belief that decentralized operations provide for better management of VA facilities, the Department decentralized resources to the Administrations and staff offices for VA's IT systems design and applications development, systems operations, and systems oversight, along with four data processing centers. The remaining IT oversight program was placed under

the Chief Financial Officer (CFO). Then, in accordance with the Clinger-Cohen Act of 1996, VA formally established the position of Assistant Secretary for Information and Technology (CIO), but the IT oversight program remained aligned under the CFO and decentralization of VA's IT program continued.

At his confirmation hearing in January 2001, Secretary-designee Principi stated that he was committed to ending stovepiped systems in VA. In August 2001, VA's first Assistant Secretary for Information and Technology was appointed: Dr. John A. Gauss, a recently retired Rear Admiral who had headed Navy's Space and Naval Warfare Systems Command. During his service to VA, Dr. Gauss worked to stand up a credible departmental IT program to better serve our veterans. He attempted to develop a VA enterprise architecture, build an effective IT project review and approval process, begin the modernization of our telecommunications infrastructure and stand up a world-class cyber security program for VA.

Secretary Principi directed the centralization of the Department's IT program, including authority over personnel and funding, in the Office of the Assistant Secretary for Information Technology effective October 1, 2002. A team of executives from across VA was convened to design a centralized IT organization for VA. The Secretary approved a centralized reorganization plan on May 14, 2003. The reorganization involved the immediate detail and eventual permanent reassignment of 97 employees from the Administrations in the areas of telecommunications support and cyber security (field VISN level ISOs). The Administration level chief information officers were renamed as Deputy CIO's and designated as

being "dual hatted," meaning they would take their technical direction from the CIO but remain employees of their existing parent organizations and take their business direction from the Administration in which they resided.

The result of this reorganization was a matrix organization which, over time, VA came to realize was not best suited for a large, geographically dispersed organization that is highly dependent on information technology to deliver services.

Robert N. McFarland was confirmed by the Senate on January 22, 2004 as the second Assistant Secretary for Information and Technology. Under his leadership, a rigorous IT review process, disciplined project management methodology and an IT portfolio management system have continued to evolve. We are in the final phase of rebuilding our nationwide telecommunications infrastructure, beginning the consolidation of some infrastructure assets, and implementing aggressive cyber security and privacy programs to ensure the protection of our infrastructure and veterans' personal information. We submitted the VA Enterprise Architecture design to OMB in June 2005 and received a score of 3.0, significantly higher than the previous score of 1.25. We continue to refine it.

A strong Enterprise Architecture is critical to any effort to bring down our stovepiped systems and replace them with integrated systems. The score of 3.0 is significant progress in this information technology area and signals that we are steadfastly working to build a foundation for systems integration and standardization.

In the wake of the difficulties with CoreFLS, as a new Deputy Secretary, I asked Assistant Secretary McFarland to undertake a study of our IT system and to pursue outside assistance if necessary. In December 2004 he contracted with The Gartner Group to conduct an Organizational Assessment of VA IT.

This assessment was to enhance the effectiveness of VA's IT by first baselining how it operates today, then developing organizational models that increase VA's IT value (in terms of greater efficiencies, economies of scale, and added business value), and finally, charting the path VA IT can follow to deploy its new organizational model to truly deliver value. The completed assessment was delivered to the Assistant Secretary for Information and Technology in May 2005, and the Secretary, the Deputy Secretary and the Under Secretaries were then briefed.

A decision is forthcoming. The next step will be to systematically and methodically plan, organize, and transition to the new organization.

The study proposed five different alternatives, as follows.

Option 1 – Status quo. Currently, VA IT resources are operated and managed within a highly decentralized management structure. The Department's CIO manages a central office staff of approximately 350 government employees and a direct budget of approximately $50M per year. While the CIO is charged with overall responsibility for the successful management of all VA IT resources (in FY05, $1.6B and approximately

5400 IT FTE) the CIO has no direct management control or organizational authority over any of these resources. The CIO provides policy guidance, budgetary review and general oversight via indirect supervision (dotted line) of the Administration and staff office CIO's. Within some of the Administrations, the CIO does not directly supervise or have authority over the majority of IT resources in the field and must also provide policy guidance, budgetary review and general oversight via indirect supervision.

Option 2 -- Regional Option. Under this option, VA would be divided into three to five geographically based subdivisions. Within each of these, a Deputy CIO would control all IT assets (Operations, Staff Functions, and Systems Development) and be responsible for all service delivery within that region. These Deputy CIO's would report directly to the VA CIO.

Option 3 – Administration-Centric Option. Under this option, VA would be divided by Administration and Staff Offices and a Deputy CIO for each would control all IT assets (Operations, Staff Functions, and Systems Development) and be responsible for all service delivery within that Administration or Staff Office. These Deputy CIO's would report directly to the VA CIO.

Option 4 – Federated Option. Under this option, VA would separate operational responsibilities and IT systems development responsibilities into separate domains. All IT operational service delivery personnel and the budget associated with their support (to include all non-medical IT equipment, maintenance, and contractor support) would come under the direct supervision of a national organization that reports directly to the

CIO's office. This organization would be charged with delivering all IT-related operational services to all elements of VA based upon a negotiated and formally agreed upon set of specific standard IT services delivered according to a clearly understood and documented set of service-level-agreement standards. Under a federated approach, IT systems development responsibility remains with the Administrations or staff office business units. The Administrations and staff offices directly manage all systems-development FTE and budget authority. The CIO clearly maintains overall responsibility for the successful management of these resources and continues to provide IT budget oversight, policy, and program management direction for the Department.

Option 5 – Centralized Option. Under this option, all VA IT personnel resources, assets, and budget would be under the direct supervision of the VA's CIO. This centralized IT organization would be charged with delivering all IT-related operational and systems development services to all elements of the VA based upon a negotiated and formally agreed upon set of specific standard IT services and systems development standards delivered according to a clearly understood and documented set of service level agreement standards. Under this option the Administrations remain responsible for system and user requirements definition, service delivery standards development, and end user participation in systems development acceptance criteria development and testing.

The organizational assessment is one tool we are using to decide how to improve our IT programs. We are determined to move forward and implement the changes necessary for a world-class IT program that

increases efficiencies and performance. From better utilization of resources, any savings can be reinvested in direct services to veterans.

The IT operation today has evolved over time and has included the services of many talented and dedicated professionals. Their efforts are paying off. For example, in terms of cyber security, VA IT systems are certified and accredited, and external independent gateways have been reduced.

We will build upon their successes. It is vital that any reorganization not adversely impact services to veterans or unnecessarily affect our employees. We know there are no simple "light-switch" solutions to be found in any model, but we are committed to managing these changes for the good of the Department.

Mr. Chairman, top-level executives of this Department have been involved in the evaluation of alternative organizational models, and understand the importance of this endeavor. There is an understanding that cultural change has to take place and buy-in must occur at the lower-worker level. We also know that it isn't just the IT reorganization that is involved. The Department is considering changes at the CFO level, in logistics, in finances, in our collections, and our efforts to comply with OMB's Circular A-123, "Management's Responsibility for Internal Control."

As we implement this reorganization, we remain mindful of the successes recently acknowledged – accomplishments with which our IT team had considerable involvement. For example, in just the past six months, no

fewer than five major publications have attested to VA's leadership of private and Government health care providers across almost every measure.

- A Rand report published in the *Annals of Internal Medicine* ranked the overall quality of VA medical care as significantly higher than any other health care system in the country.

- An article in the *Washington Monthly,* entitled, *'The Best Care Anywhere,'* rated VA as the recognized leader in the health care industry. It pointed out that, ten years ago, veterans' hospitals were in deep crisis ... but that today, and I quote, *'VA is producing the highest quality care in the country. VA's turnaround points the way towards solving America's health care crisis.'*

- An editorial in the prestigious *Journal of the American Medical Association,* referred to VA as *'a bright star'* within the health care profession for its cutting-edge dedication to patient safety.

- Last month, in their review of *'America's Best Hospitals,' U.S. News and World Report* titled their article on VA as, *'Military Might: VA Hospitals are Models of Top-Notch Care.'*

- And just on August 22, on the front page, the *Washington Post* ran a headline that read *Revamped Veterans' Health Care Now a Model.*

Further, on April 27, 2004 President Bush chose the VA Medical Center in Baltimore to announce his commitment to ensuring that all U.S. citizens have an electronic health record in the next 10 years. In doing so, he held out VA's fine example. The reorganization of our resources will enable VA to be the benchmark in the development and implementation of Health information technology solutions and standards as both an example and national leader in this arena.

I would say all those assessments are right on target. We view the Veterans Health Administration as the vanguard for national standards for electronic medical records, now the rest of the nation does as well. Our health IT systems – and the quality of our employees – helped us reap these headlines. Clearly, we are delivering more services to more veterans each and every year. And, this was accomplished under our current structure.

Our IT successes are also facilitating the business of claims processing and benefit delivery in the face of daunting demands:

- VA provides monthly compensation and pension benefits totaling $32 billion to over 3.5 million veterans and beneficiaries. Disability claims increased by 33% from 2000 to 2004. Last year alone, VA added nearly 240,000 new beneficiaries to the compensation and pension rolls.

- By the end of this fiscal year, over 750,000 veterans will have received decisions on their disability claims, and we will have

processed an additional 1.5 million pension, dependency, and other adjustments to beneficiaries' accounts. Even with the increased claims volumes, we have reduced by 30 percent the length of time veterans must wait for decisions on their claims over the last three years.

- We are also providing in excess of $2.5 billion in Education benefits to over 500,000 beneficiaries, and are working to rehabilitate nearly 95,000 service-disabled veterans through our Vocational Rehabilitation and Employment Program.

I would also note that In December 2004, the American Customer Satisfaction Index announced the National Cemetery Administration earned a customer satisfaction rating of 95 out of a possible 100 points – the highest score ever received by a federal agency or private organization. In the survey, both the ratings for respect shown to loved ones and maintenance of VA cemeteries as National Shrines received a score of 97. The report called this finding "an outstanding score by any standard of ACSI measurement and for any context, public or private." NCA was able to achieve this through the support of IT in all aspects of cemetery and memorial services, from the timely acquisition of veteran headstones with accurate inscriptions to the nationwide gravesite locator available to the public on the World Wide Web.

This concludes my statement. Thank you, Mr. Chairman, for the opportunity to discuss these important matters. I am prepared to answer any questions you might have.

Post Hearing Questions for the Record from
Chairman, The Honorable Steve Buyer
House Committee on Veterans' Affairs
September 14, 2005 Hearing on
Questions on Information Technology Infrastructure Reorganization

1. There have been numerous major VA IT investments that have failed. Who was in charge of each of the following programs when they began: VETSNET, CoreFLS, and VISTA? Who is currently in charge of managing these programs? What are the current costs and total costs to date for these programs?

When the Veterans Benefits Administration (VBA) initiated VETSNET, Rhoda R. Mancher, Director, Office of Information Technology, was the manager in charge. The present manager is Adair Martinez, VA Deputy Chief Information Officer for Benefits. VBA has invested a total of $69.1 million on VETSNET applications. The VA budget for fiscal year 2005 includes $16.9 million for VETSNET.

CoreFLS costs to date are $304 million. At start up (1999), CoreFLS Executive Manager was Edward A. Powell, Assistant Secretary for Management. Currently, Robert N. McFarland, Assistant Secretary for Information and Technology, has oversight responsibility.

Craig Luigart recently was named VHA's Chief Information Officer. He is the present manager for VistA. At start up, Dr. Robert Kolodner MD, VHA Health Informatics Officer, provided oversight responsibility.

The expected obligations for operating and maintaining VistA Legacy in FY 2005 are $437.7 million. Of this, $247 million is for salaries for the approximately 2,800 full time employees (FTE) in the medical centers that run the program and our maintenance staff, $138.7 million is for hardware and software maintenance contracts, $44.6 million is for equipment and software and $7.4 million is for supplies, travel and other related costs.

Spending for VistA Legacy from FY 1999 thru 2005 was $2.861 billion. The supporting records are available in the FY 2001 Office of Management and Budget (OMB) Exhibit 53 and thereafter. Consistent with OMB reporting requirements, VistA Legacy project costs are available in Department records from FY 1999 through 2005.

2. One of the significant contributing factors to the problems associated with the CoreFLS program was that the same contractor hired by VA to provide independent advice and assistance was then given responsibility to implement the program. One of the conclusions of the Carnegie Mellon report on CoreFLS was that in allowing this, VA created an inherent conflict of interest. What is VA doing to prevent contractors hired to provide independent information

Technology (IT) advice and assistance from then being hired to implement the work and approach they recommend?

VA program management and contracting personnel are trained in Government ethics and work closely together to identify conflicts of interest and the appearance thereof. Additionally, the One-VA Enterprise Program Management Office (EPMO) was formed on August 8, 2004, it is designed to improve and standardize the management of IT projects and the IT Portfolio by defining VA-wide policies, procedures and best practices, providing tools to facilitate the successful management, reporting and oversight of VA's IT project. When fully implemented, EMPO will conduct periodic Program Management Reviews (PMRs) of all major projects. A key component of reviews will focus on the acquisition strategy, supporting acquisition plans and implementation. This will provide a greater level of scrutiny of the contracting process and ensure that contracting strategies are sound and proper. Administrations will be encouraged to implement similar internal reviews to ensure appropriate contracting methodologies are used.

3. Which of the Gartner Report's recommended options has the VA chosen to address the reorganization of the IT infrastructure? What is the Department's implementation plan, and has implementation begun?

In the wake of the difficulties with CoreFLS, as a new Deputy Secretary, I asked Assistant Secretary McFarland to undertake a study of our IT system and to pursue outside assistance if necessary. In December 2004 he contracted with The Gartner Group to conduct an Organizational Assessment of VA IT.

This assessment was to enhance the effectiveness of VA's IT by first baselining how it operates today, then developing organizational models that increase VA's IT value (in terms of greater efficiencies, economies of scale, and added business value), and finally, charting the path VA IT can follow to deploy its new organizational model to truly deliver value. The completed assessment was delivered to the Assistant Secretary for Information and Technology in May 2005, and the Secretary, the Deputy Secretary and the Under Secretaries were then briefed.

A decision is forthcoming. The next step will be to systematically and methodically plan, organize, and transition to the new organization.

ceiling for HealtheVet. This review will be completed once the final IT budget distribution is determined by VA's Chief Information Officer.

5. The Committee praised VA for its preparation and responsiveness in the aftermath of Hurricane Katrina. VA principals have informed us that VA's ability to download electronic medical records onto tapes at the New Orleans Veterans Affairs Medical Center (VAMC) and physically transfer them to the Houston VAMC contributed to that success. We understand that the record tapes had to be reconfigured to be accessed, that the down-loaded data was more than four hours old and that radiographic images were not accessible until the New Orleans VAMC server was back in operations. Please advise us if VA's efforts to ensure real-time medical information on a 24/7 basis is a reality today at all locations VA-wide?

Response: It is important to note that the VistA systems in New Orleans did not fail; they remained online supporting the Houma and Baton Rouge clinics until after the evacuation. The need to move the tapes was a result of the failure of the commercial wide-area network. VistA backup tapes were transported from the New Orleans VAMC to the Houston VAMC and subsequently allowed the electronic medical records to be viewed across the country. These tapes were created as part of the routine backup process every medical center is expected to perform on a nightly basis. VistA database backups are scheduled to run nightly, usually starting after midnight with completion in the early morning. No reconfiguration of the data was necessary to make the original back up tapes available nationwide. Because New Orleans continued to support the Houma and Baton Rouge clinics, it was necessary to merge the final back up which contained the data of the two still operating clinics. This was accomplished without major difficulty.

The VistA system remains on-line and available to users before, during, and after the backup. VistA users continually interact with the database in real-time. The completed backup tapes are then removed and moved to a safe location such as commercial data storage companies or another VAMC. If a medical center were to experience an event that destroyed their current VistA database, these backup tapes would be either restored to new replacement hardware at the original site or transported to another location for restoration, as was done with New Orleans at Houston.

Backup tapes always represent the database at the point in time the backup is complete. Each change to the database is stored in a journal file in order to keep the database current. The journal files are also moved to tape for safe storage. Even a backup tape as old as several weeks could be used for full recovery, if all the journal files are applied to make it current. A backup restored to a remote location can be kept nearly current by transfer of journal files from the original system. While working on lessons learned from Katrina and Rita, VA and one of our systems vendor partners, developed a procedure to automatically reduce the

size of these journal files and send them over the network to the Office of Information (OI) located in Silver Spring, Maryland. VA used this process in anticipation of Hurricane Wilma. Although this capability was not needed in response to Wilma, if it had been necessary, any or all of the VistA databases could have been restored and made current.

The New Orleans imaging system is currently being rebuilt at the Little Rock VAMC. The optical disks are being inspected, cleaned, and put into new storage cases. It may be another month before all the New Orleans images are accessible. However, the description of what is contained on those images is available in VistA so that the provider will know what imaging studies have been performed.

VistA Imaging is comprised of a wide range of motion and still images and is not limited to radiology images; e.g., x-ray, CAT scan, magnetic resonance images, etc. VA does not currently have Continuity of Operations (COOP) for imaging and this is one of the requirements under consideration for the VistA Imaging Reengineering project. COOP for imaging is challenging because of the massive amount of data involved. The largest VistA databases would be of moderate size, less than 500 gigabytes; the imaging system at a large active VAMC could be up to 40 times larger.

VistA information systems are real-time 24/7 and the tapes that allowed New Orleans to be hosted at Houston were created through normal VistA system management practices. The logistics of transporting tapes during an evacuation proved problematic. In response to lessons learned during the current hurricane season, we have instructed field staff to transport backup tapes to safe locations well in advance and to use the new procedures to keep the information current, ensuring that the back up tapes and changes are accessible. Additionally, VA is developing and implementing a centralized Health Data Repository that will serve as a national store for data contained in the veteran's health record. VA intends to transition to Regional Data Processing Centers that will be fully COOP'd and will have a higher degree of hardening than our existing computer rooms. Our COOP plan will include the ability to sustain telecommunications in the event of a wide-area network failure. Further planning in response to the lessons learned from Katrina is underway and VA is looking at other ways to mitigate risk and maximize the efficiency of our existing systems as we move in these new directions.

6. What is the current status, to include expenditures to date, of VA's Core Financial and Logistics System in Bay Pines, FL?

Response: Expenditures to date (end of FY 2005) were $233.47 million for the CoreFLS program. Bay Pines and the other pilot sites for CoreFLS reverted back to the legacy systems effective October 2004.

7. It is the Committee's understanding that VA was considering a joint use facility for the VBA data center and the VHA data center at the Great Lakes Health Care System at Hines, IL? When does VA intend on rendering a decision to proceed with this joint venture?

Response: VA's CIO reviewed the proposed options for a VHA and VBA joint use of a Data Center facility located at the Great Lakes Health Care System in Hines, Illinois. The decision was that none of the proposed options were viable and immediately put the whole project on hold until after the IT Operations re-organization. The VA CIO did, however, recommend one minor immediate move to permit VISN 12 to relocate some IT equipment from medical center space to the VBA data center. A final decision will be made following IT reorganization to incorporate the option that is best for the entire IT Operations environment.

Attachments:

1) **Copy of the Carnegie Mellon Action Dashboard with Milestones**
2) **Definition of Terms and Description of HealtheVet components**
3) **Two copies of Carnegie Mellon Evaluation Phase I and Phase II Outbriefs**

Questions for the Record
Chairman, Steve Buyer and Ranking Democractic Member Lane Evans
House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
25 October 2005

The Department of Veterans' Affairs Efforts to Provide Better Accountability for its Information Technology Spending

1. Provide two copies of the Carnegie Mellon University (CMU) evaluation of the HealtheVet-VistA program that was delivered to VA in early 2005. With regards to the report's recommendations, what is VA's remediation plan to include implementation mile-stone dates, and how has VA addressed each on CMU's criticisms and recommendations?

Response: Two copies of the Carnegie Mellon/Software Engineering Institute (CM/SEI), (SEI Independent Technical Assessment Phase I outbrief dated December 3, 2004, and SEI Independent Assessment Phase II outbrief dated February 4, 2005) briefing of the HealtheVet-VistA program are being provided as requested. (Attachment 3) Please note that the information reflected in this briefing, as noted by CM/SEI, is incomplete without the verbal presentation.

With regard to the report's recommendations, the following comments are made: The CM/SEI evaluation offered a fair assessment of the early phases of the HealtheVet-VistA program by identifying a number of issues that would need to be addressed for successful program implementation and execution. The Department of Veterans Affairs (VA) agreed with the findings. VA has revised its original plan to address the weaknesses identified by SEI and implement their recommendations. VA has also engaged experts in the areas identified as critical, including CM/SEI, to participate at all levels of the HealtheVet planning and execution process. Specific actions taken to date include:

- Engaged VA's Deputy Secretary and his staff, and other direct leadership from the highest levels of the VA/VHA (Veterans Health Administration) organization, in weekly program implementation and execution reviews.
- Established at the Department level an Enterprise Project Management Office (EPMO) to integrate Department of Defense (DoD)/PMI and industry best practices into VA project and program management; EPMO given additional responsibilities and authority to conduct independent reviews, and to provide for enterprise executive governance and oversight.
- Reassigned the developer of the EPMO governance model to the position of Chief Information Officer (CIO) for VHA. Additionally, this newly appointed VHA CIO has extensive and proven major IT program management experience.
- Backfilled the EPMO position with the Navy's former Program Manager of the Year to continue the development of the EPMO to maturity.

- Established a comprehensive draft 'Blue Print' architecture for HealtheVet, which is currently in peer review and eventually in external independent review.
- Established a Requirements Determination team to develop "top-level" user-defined requirements set with an internal due date of March 30, 2006.
- Establishing a comprehensive communications team for internal and external coordination and outreach.

Specific ongoing actions include:

- Instituting an extensive requirements development and prioritization process to ensure that end-user requirements are being identified and met within funding guidelines.
- Instituting a transformational organizational realignment of all programs and projects to ensure synergy and interoperability across the different business portfolios; Systems-of-systems management approach is similar to the proven DoD Program Executive Office model.
- Taking action to fill key VHA IT (Information Technology) leadership positions with proven major IT Program Managers.
- Utilizing Independent Validation and Verification throughout the programs life cycle including pre-initiation.

Additionally, with the assistance of CM/SEI, CM/SEI recommendations have been formulated into specific action plans and goals that can be executed and measured. Progress on these recommendations is reported to the Deputy Secretary on a monthly basis. A copy of the Carnegie Mellon Action Dashboard with milestones is provided as attachment 1. Also included is a definition of terms and description of HealtheVet components in attachment 2.

2. Provide two copies of the CMU evaluation of VETSNET and any intermediate or interim report from CMU on VETSNET within five calendar days of VA receiving the deliverable product.

Response: Veterans Benefits Administration (VBA) has received a draft report that is currently under review. There are no intermediate or interim reports to be delivered from CMU for this evaluation.

3. Provide an update regarding the status of data transfers between the Veterans Benefits Administration (VBA) and the Veterans Health Administration (VHA) to identify veterans with service connected conditions who should not be billed for VHA care.

Response: On November 7, 2005, VHA released its WebHINQ application, which provides client tier and system to system access to VBA's new corporate system as well as the Benefits Delivery Network (BDN) and Beneficiary Information Records Locator System (BIRLS). This enhancement allows VHA to retrieve, in response to queries and unsolicited data transmissions, information

on veterans' service-connected disabilities, including the affected extremities, original and current effective dates of the evaluation percentages and the effective date of the combined evaluation percentage upon which the compensation award is based. WebHINQ also retrieves a more descriptive disability code than currently retrieved by VHA.

Once the WebHINQ project is fully deployed, VHA will be performing a one-time update of all enrollees' disability information to upgrade the veteran's service-connected rating information in their health eligibility records. VHA has completed a rigorous data validation to ensure that complete and accurate information is being received from VBA and updated in the VHA Enrollment system and within the VistA systems at each involved VA facility.

To date, VHA has successfully updated almost 160,000 veterans' health eligibility records with greater than six (6) service-connected conditions. This was accomplished by monthly updates of records in VHA after comparison with records in VBA's Veterans Information Tracking Adjudication Log (VITAL).

4. The HealtheVet-VistA project is planned to replace the existing VistA (Legacy) health care processing system by rehosting, replacing, enhancing and/or reengineering current health information applications to process on a new technology platform. In 2003, scheduling replacement for HealtheVet-VistA was an approved capital investment. What is the status, to include expenditures to date, of the HealtheVet-VistA project?

Response: HealtheVet is the follow-on IT program (system-of-systems) to VistA. HealtheVet–VistA is one of nine Office of Management and Budget (OMB) 300 projects that make up the FY-06 HealtheVet program. HealtheVet–Vista includes five major core components –Rehosting, Data Standardization, Platform, and Common Services, and My HealtheVet. Attachment 2 provides a more detailed summary of definition and supporting projects. The HealtheVet-VistA projects, in conjunction with the eight other VHA OMB 300 projects, are building blocks to achieve a user-defined modern Health Care Environment (HealtheVet 2012). It should be noted that the various HealtheVet–Vista projects, on completion, will provide incremental & immediate benefits to the HealtheVet current and future capability.

Costs associated with the HealtheVet-VistA OMB 300 are:
Total expenditure to date (9/30/05): $45.7M

Cost associated with Scheduling Replacement are:
Total expenditure to date (9/30/05): $58.4M

VA is currently in the process of reviewing all of the major project milestones for 2006 based on the Congressional action on the 2006 budget and the funding

ceiling for HealtheVet. This review will be completed once the final IT budget distribution is determined by VA's Chief Information Officer.

5. The Committee praised VA for its preparation and responsiveness in the aftermath of Hurricane Katrina. VA principals have informed us that VA's ability to download electronic medical records onto tapes at the New Orleans Veterans Affairs Medical Center (VAMC) and physically transfer them to the Houston VAMC contributed to that success. We understand that the record tapes had to be reconfigured to be accessed, that the down-loaded data was more than four hours old and that radiographic images were not accessible until the New Orleans VAMC server was back in operations. Please advise us if VA's efforts to ensure real-time medical information on a 24/7 basis is a reality today at all locations VA-wide?

Response: It is important to note that the VistA systems in New Orleans did not fail; they remained online supporting the Houma and Baton Rouge clinics until after the evacuation. The need to move the tapes was a result of the failure of the commercial wide-area network. VistA backup tapes were transported from the New Orleans VAMC to the Houston VAMC and subsequently allowed the electronic medical records to be viewed across the country. These tapes were created as part of the routine backup process every medical center is expected to perform on a nightly basis. VistA database backups are scheduled to run nightly, usually starting after midnight with completion in the early morning. No reconfiguration of the data was necessary to make the original back up tapes available nationwide. Because New Orleans continued to support the Houma and Baton Rouge clinics, it was necessary to merge the final back up which contained the data of the two still operating clinics. This was accomplished without major difficulty.

The VistA system remains on-line and available to users before, during, and after the backup. VistA users continually interact with the database in real-time. The completed backup tapes are then removed and moved to a safe location such as commercial data storage companies or another VAMC. If a medical center were to experience an event that destroyed their current VistA database, these backup tapes would be either restored to new replacement hardware at the original site or transported to another location for restoration, as was done with New Orleans at Houston.

Backup tapes always represent the database at the point in time the backup is complete. Each change to the database is stored in a journal file in order to keep the database current. The journal files are also moved to tape for safe storage. Even a backup tape as old as several weeks could be used for full recovery, if all the journal files are applied to make it current. A backup restored to a remote location can be kept nearly current by transfer of journal files from the original system. While working on lessons learned from Katrina and Rita, VA and one of our systems vendor partners, developed a procedure to automatically reduce the

size of these journal files and send them over the network to the Office of Information (OI) located in Silver Spring, Maryland. VA used this process in anticipation of Hurricane Wilma. Although this capability was not needed in response to Wilma, if it had been necessary, any or all of the VistA databases could have been restored and made current.

The New Orleans imaging system is currently being rebuilt at the Little Rock VAMC. The optical disks are being inspected, cleaned, and put into new storage cases. It may be another month before all the New Orleans images are accessible. However, the description of what is contained on those images is available in VistA so that the provider will know what imaging studies have been performed.

VistA Imaging is comprised of a wide range of motion and still images and is not limited to radiology images; e.g., x-ray, CAT scan, magnetic resonance images, etc. VA does not currently have Continuity of Operations (COOP) for imaging and this is one of the requirements under consideration for the VistA Imaging Reengineering project. COOP for imaging is challenging because of the massive amount of data involved. The largest VistA databases would be of moderate size, less than 500 gigabytes; the imaging system at a large active VAMC could be up to 40 times larger.

VistA information systems are real-time 24/7 and the tapes that allowed New Orleans to be hosted at Houston were created through normal VistA system management practices. The logistics of transporting tapes during an evacuation proved problematic. In response to lessons learned during the current hurricane season, we have instructed field staff to transport backup tapes to safe locations well in advance and to use the new procedures to keep the information current, ensuring that the back up tapes and changes are accessible. Additionally, VA is developing and implementing a centralized Health Data Repository that will serve as a national store for data contained in the veteran's health record. VA intends to transition to Regional Data Processing Centers that will be fully COOP'd and will have a higher degree of hardening than our existing computer rooms. Our COOP plan will include the ability to sustain telecommunications in the event of a wide-area network failure. Further planning in response to the lessons learned from Katrina is underway and VA is looking at other ways to mitigate risk and maximize the efficiency of our existing systems as we move in these new directions.

6. What is the current status, to include expenditures to date, of VA's Core Financial and Logistics System in Bay Pines, FL?

Response: Expenditures to date (end of FY 2005) were $233.47 million for the CoreFLS program. Bay Pines and the other pilot sites for CoreFLS reverted back to the legacy systems effective October 2004.

7. It is the Committee's understanding that VA was considering a joint use facility for the VBA data center and the VHA data center at the Great Lakes Health Care System at Hines, IL? When does VA intend on rendering a decision to proceed with this joint venture?

Response: VA's CIO reviewed the proposed options for a VHA and VBA joint use of a Data Center facility located at the Great Lakes Health Care System in Hines, Illinois. The decision was that none of the proposed options were viable and immediately put the whole project on hold until after the IT Operations re-organization. The VA CIO did, however, recommend one minor immediate move to permit VISN 12 to relocate some IT equipment from medical center space to the VBA data center. A final decision will be made following IT reorganization to incorporate the option that is best for the entire IT Operations environment.

Attachments:

1) **Copy of the Carnegie Mellon Action Dashboard with Milestones**
2) **Definition of Terms and Description of HealtheVet components**
3) **Two copies of Carnegie Mellon Evaluation Phase I and Phase II Outbriefs**

Carnegie Mellon Action Dashboard

November 2005

Area	Status	Definition	Status Summary	Key Success Factors
1) **Develop a HeV strategic plan**	Version 2 delivered 10/31/05.	•Objectives •Enabling Strategies	Key Accomplishments: ▪10/31/05: Version 2 of the strategic plan was delivered ▪1/31/06: Strategic Plan version 2.1: Continued evolution of components of the strategic plan based on work with CM/SEI and others ▪3/31/06: Strategic Plan Version 2.2: incorporate recommendations from FY07 transition workgroup to be delivered	Addresses CM Prerequisite for Success *"Define the HeV Vision And The Transition Path"* and *"Develop A Framework to Meet HeV Program Lifecycle Needs"*
2) **Define the future state of healthcare that the IT environment must support**	Version 2 delivered 10/31/06.	•Validate HealtheVet-VistA draft strategic plan •Identify current issues •Identify needed future capabilities •Business areas for inclusion are clinical, administrative, financial, research, education	Key Accomplishments: ▪6/30/05: Version 1 of HeV Strategic Plan (Including Vision, Mission, Objectives, Enabling Strategies) was delivered •7/13/05: completed documentation describing the approach for business capabilities focus group meetings •10/31/05: Strategic plan V2 containing a high level view of the near term operational capabilities was delivered •10/31/05: Core group of clinical capabilities defined and provided to business owners for validation. • 1/31/05: Operational scenarios to be documented based on input from FY 07 transition workgroup	Addresses CM Prerequisite for Success *"Define the HeV Vision And The Transition Path"*

Carnegie Mellon Action Dashboard

Area	Status	Definition	Status Summary	Key Success Factors
3) Define VHA OI governance model	Initial draft of governance model delivered 8/31/05	• Defines decision-making process • Establishes guidelines for issue identification and escalation • Defines areas of control and levels of authority • Establishes accountability	Key Accomplishments: ▪8/2/05: Action plan completed for HeV Governance, anticipating validation pass through SP group ▪8/19/05: Completed Action Plan for HeV Governance ▪8/31/05: Completed first draft HeV program Governance model ▪1/31/06: First update of the draft governance plan to accommodate sub-level management plans to be completed ▪1/31/06: Pilot Risk and Configuration Management processes initiated ▪1/31/06 Initial draft of VA/VHA organizations defining governance structures that will influence program governance will be provided	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*
4) Define VHA OI operational model	Action plan for operational model delivered 8/31/05	• Define future operational organization in terms of functions • Define required key roles and responsibilities • Describe organization and interaction of different lines of services • Describe any future competency centers required • Define external relationships (e.g., EPMO, Steering Committees, Internal and External Liaisons, etc.)	Key Accomplishments: ▪6/30/05: Completed overview of HeV Operational Model ▪7/29/05: Completed definition of HeV Operational Model including required roles and responsibilities delivered ▪ 8/19/05 Completed Action Plan for implementation of HeV Operational Model ▪11/30/05: Completion HPMO staff model ▪3/31/06: Transition workgroup to deliver FY 07 migration roadmap that will provide the operational capabilities that will be rolled out ▪3/31/06: VHA OI operational model completed based on reorganization	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*
5) Develop organizational structure based on operational model	On target for October 31, 2005 deliverable	• Develop organization chart • Assign key personnel • Obtain approval of VHA and VA executives • Implement organizational change	Key Accomplishments: ▪ 11/30/05: HPMO staff model will be completed	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*

Carnegie Mellon Action Dashboard

Area	Status	Definition	Status Summary	Key Success Factors
6) Develop draft tactical plan	Tactical work plans Delivered on 9/30/05. FY06 work validated against business requirements on 10/31/05	• Decompose strategic plan (the 'what') into the tactical (the 'how') • Map to CM/SEI findings and OI planned responses	Key Accomplishments: ▪9/30/05: completed tactical work plans for each Management Objective/Enabling Strategy ▪10/31/05: completed the connection of current FY06 work efforts to business objectives and requirements ▪1/31/06 Pilot sequencing plan process ▪1/31/06 Pilot change management ▪3/31/06: Tie action plans to outcomes of transition plan workgroup	Addresses CM Prerequisite for Success "*Manage To Realistic, Changing Program/Technical Options And Risks*"
7) Roll individual tactical plans into single master plan	On target for November30, 05 deliverable	• Ensure alignment of master plan with strategic plan • Engage business owners with tactical plan prioritization	Key Accomplishments: ▪10/28/05: Completed the definition of TWP's which will be able to be rolled into the Master Action Plan ▪10/31/05 Completed the alignment of FY06 HealtheVet VistA projects to the VA/VHA strategic plan. ▪3/31/06: Complete the alignment of all VHA IT projects to the VA/VHA strategic plan	Addresses CM Prerequisite for Success "*Develop A Framework To Meet HeV Program Lifecycle Needs*"
8) Adjust FY06 funds based on prioritized tactical plan	10/31/05 project alignment to funding availability complete		Key Accomplishments: ▪ 10/31/05 FY06 Completed the alignment of all HealtheVet VistA projects to the VA/VHA strategic plan and balanced project costs against available funding. ▪3/31/05: Complete the alignment of all VHA IT projects to the VA/VHA strategic plan and balance project costs against available funding.	

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Characterize System Quality Attributes	In-process	•Establish classes of quality attributes for Architecture •Mine current doc's for quality attributes/business drivers •Validate quality attributes/business drivers •Load quality attributes into requirements repository	Key Accomplishments: -10/31/05: Completed the development of a document detailing business drivers from different HVV sources, validated business drivers and included as part of V2 of strategic plan 10/31/05 - Finalized list of critical quality attributes and incorporate into HealtheVet Requirements Management Repository. 10/31/05: Identified the essential clinical and veteran capabilities created as part of V2 of the strategic plan 11/05/05 - Completed quality attribute tradeoff analysis. 12/05/05 - Begin phased operationalization of HealtheVet Requirements Management processes, including full traceability to two projects.
Define migration path from legacy system	In-process	•Identify Intermediate states and their business value •Delineate applications and services scope •Establish validation lab	Key Accomplishments: ▪10/31/05: completed high-level intermediate states of HVV (Roadmap Version 1) ▪1/31/06: Pilot sequence planning process. ▪3/31/06: Complete Transition Roadmap Version 2

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Establish verifiable requirements for critical architectural decisions	In-process	•Verity that SOA is viable for very large, integrated organization •Determine scalability of the service-based approach •Develop priority list of prototyping efforts that address key architectural issues •Prototype Architectural Capabilities	Key Accomplishments: ▪9/29/05 Received briefing from Gartner Group regarding viability of SOA ▪10/31/05: completed initial draft of technical risks that must be address ▪1/31/06 Develop the list of Prioritized prototyping efforts. ▪3/31/06: Incorporation of prototyping efforts into V1 of transitional roadmap document
Tightly coupled HVV activities to support moving forward a large scale system of systems	In-process	•Define responsibilities for PMO	Key Accomplishments: •10/31/05: Completed Roles and Responsibilities of PMO •11/30/05: finalize HPMO organizational structure •3/31/06: phase 1 staffing of HPMO to 90%

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Stakeholders need to share a common understanding	In-process	•Validate scope of HVV •Develop a Communication Plan •Develop a Governance Plan	Key Accomplishments: ▪8/17/05 Delivered draft of Governance model ▪9/2/05 Delivered draft of Stakeholder list for Communication plan ▪ 8/19/05: Finalization of Governance Action Plan (behind schedule, awaiting feedback, updated projected completion 10/31/05) ▪10/31/05 completed 2 page briefing on scope and vision of HealtheVet ▪2/28/06: Communications plan complete ▪1/31/06: Governance plan updated based on information from transition planning workgroup ▪3/31/06:Governance plan updated based on information from transition planning workgroup

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Establish a plan which provides for tracking, managing, controlling and reporting	In-process	• Define a Risk Management Planning process • Develop an action Plan to support tracking and Implementation • Define a sequencing plan for HVV	Key Accomplishments: ▪ 10/3/05 – Revised SEI recommendations incorporated into Master Action Plan ▪ 10/4/05 – Risk management tool selection memo submitted for approval ▪ 10/5/05 – Prototype of automated status reporting capability completed ▪ 10/18/05 – Automated status reporting capability rolled out; working through assignment issues ▪ 10/25/05 – Risk management GAP Analysis submitted for approval ▪ 10/27/05 – Submitted updated project plan ▪ 10/27/05 – Continued review of Integrated Risk Mgmt Plan ▪ 11/02/05 – Completed strategic plan review for proper action plan assignment ▪ 11/30/05 - Refine Master Action Plan with content, structure, and integration points ▪ 12/31/05: Risk Management process rolled out

Major Components of HealtheVet-VistA (FY06)

- **Rehosting:** Migration of existing M-based applications into the HeV architecture and data structures (J2EE-Based applications).
- **Common Services:** A "service oriented" architecture – similar software functions in different applications are isolated and streamlined so they can be coded once and reused many times.
- **Data Standardization:** The establishment of data standards across all VHA sites to ensure system interoperability and exchange of compatible information.
- **Platform:** Provision of the physical computing infrastructure, including licenses and support contracts to operate the HeV program.
- **My HealtheVet Connectivity:** A person-centered health portal providing veterans online access to electronic health records.

Description of HealtheVet-VistA Components – FY06

Platform

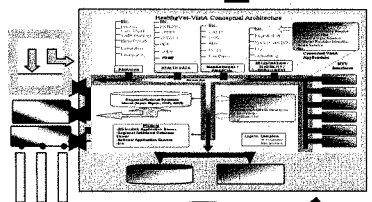
- Scheduling Infrastructure
- Spinal Cord Injury Infrastructure
- CPRS-R Infrastructure
- National Data Processing Centers
- Enterprise License Agreements

My HealtheVet Connectivity

- Electronic Access to VHA Electronic Health Records

Data Standardization

- Problem List
- Clinical Documents
- Immunizations
- Radiology
- Orders
- Encounters
- Adverse Reactions
- Clinical Procedures
- Consultations
- Dental
- Dietetics



Rehosting

- ADT-R
- App Dev Process Security
- CHDR
- Clinical Procedures
- CPRS-R
- Nursing
- VistA Imaging
- Vitals
- Spinal Cord Injury
- HeV Foundations

Projects, on completion, **provide incremental & immediate benefits** to HealtheVet current and future capability

Common Services

- Person Service- Demographics
- Person Service-Identity Management
- Delivery Service
- Administrative Data Repository (ADR)
- ADR Data Migration
- Application Preferencing Service
- National Provider Identifier
- Audit Service
- Enterprise Exception Log Service
- Institution File
- CS Maintenance Support

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

SEI Independent Technical Assessment Phase I Outbrief

VA HealtheVet-VistA

03 December 2004

Sponsored by the U.S. Department of Defense

Purpose of this Briefing

The brief presents the high-level summary of the Software Engineering Institute's (SEI's) Independent Technical Assessment (ITA) – Phase I of the Department of Veterans Affairs (VA) HealtheVet-VistA program. Phase I focused on Architecture and Engineering concerns.

This brief is incomplete without the accompanying oral presentation.

Acknowledgements

The SEI acknowledges and thanks the VA and their contractors for their support during the ITA

We would especially like to thank our primary points of contact

- M. Jay Eigenbrode
- Howard Green
- Jennifer Ford

Outline

Phase I Focus

Principal Findings

Principal Recommendations

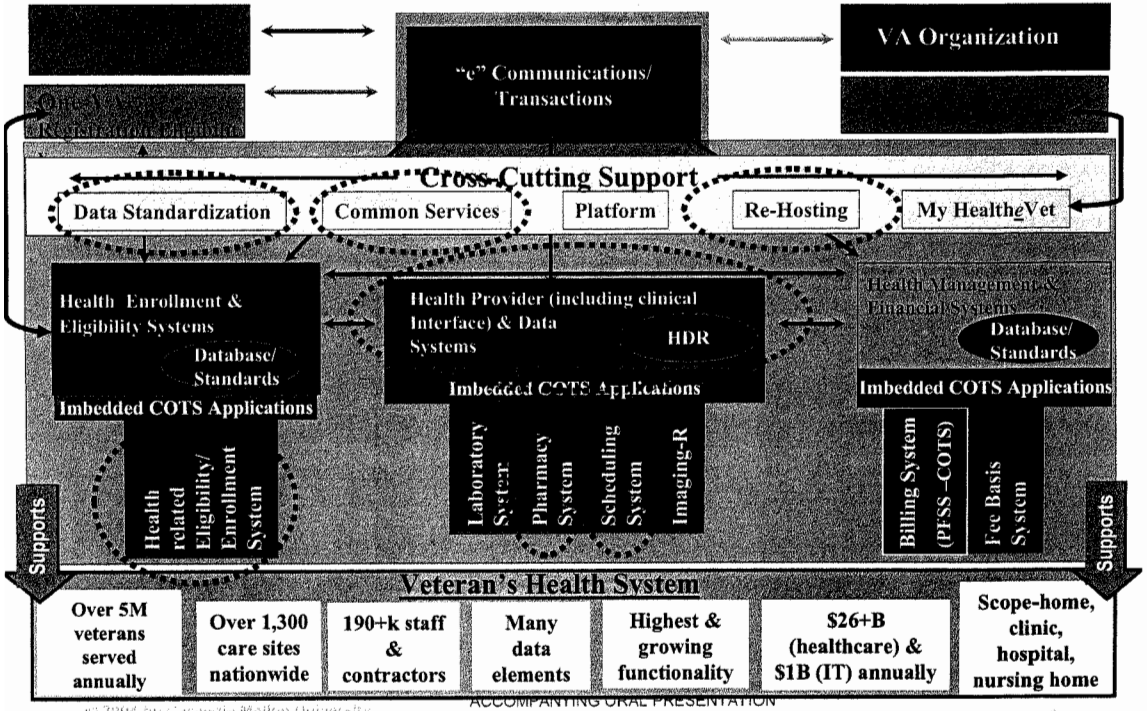
Summary

Phase II Focus

Phase I Focus – Is The HealtheVet-VistA (HeV) Architecture Viable?

Carnegie Mellon
Software Engineering Institute

What Did We Look At?



Phase I Focus – Is The HeV Architecture Viable? (1 of 2)

The SEI ITA team chose the following as a definition of viable: "capable of cost-effective use for its intended purpose"

To be viable, the HeV architectural approach must coordinate activities across:

- HeV as a system-of-systems
- Individual HeV systems (applications) and services
- All HeV software architectures

A viable HeV architecture must not only meet the functional requirements but also meet the non-functional or quality attribute requirements as well

Phase I Focus – Is the HeV Architecture Viable? (2 of 2)

At this point in the program, the architecture is potentially viable, but …

- **The VA has not sufficiently articulated the future state that the architecture is meant to support**
- **Verifiable requirements are lacking for critical architectural decisions**
- **While it is understood the "To Be" architecture will evolve, there are no defined intermediate states and no documented roadmap**

Should HeV Continue?

Yes

- The VA recognizes that they can not stay where they are and still meet future health care needs
- There is significant domain expertise and a strong base of institutional discipline around VistA
- Dedicated staff are focused on the VA mission & embrace the need for stronger planning and communications
- There is strong VA buy-in for a patient-centric vision for health care

However, the VA must immediately address fundamental issues to resolve the complex management and technical challenges facing HeV

Principal Findings

Principal Findings – Architecture Future State

Will HeV support the next generation of patient care, or will HeV support similar patient care as today, just a little better or faster?

- Future patient care has not been modeled
- Stakeholders do not share a common understanding
- Migration path from legacy has not been defined
- System-of-systems properties (essential capabilities, quality attributes) have not been defined, modeled, or validated

With no defined end goal (scope), all architecture and related technology choices are at risk

Principal Findings – Architecture Requirements

System Quality Attributes have not been characterized

- And once determined, how will they be validated and verified?

Requirements must support the future patient care model

Requirements from local extensions including Class III code are undefined in many cases

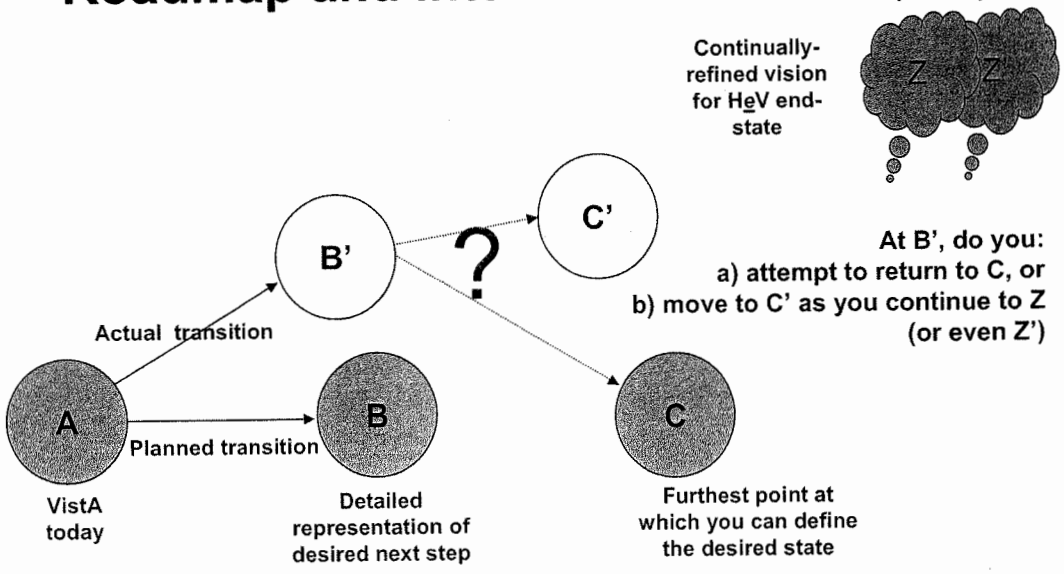
If not addressed, key system quality attributes (performance, security) will not meet stakeholder expectations

Principal Findings – Architecture Roadmap and Intermediate States (1 of 3)

There are no defined intermediate stable states, which are needed

- to break the problem into tractable pieces
- to make sure the pieces are fitting together
- to revalidate the requirements
- to allow the organization to absorb change and remain productive
- for program flexibility

Principal Findings – Architecture Roadmap and Intermediate States (2 of 3)



Principal Findings – Architecture Roadmap and Intermediate States (3 of 3)

Architectural uncertainties have not been identified and explored (e.g., service-based architecture, role-based access)

There is no systematic mechanism for mapping the HIA to the applications

- The HIA is making conceptual decisions for the long term direction
- The applications and services developers are making design decisions to meet immediate delivery dates

If not addressed, the pieces of HeV will not effectively work together – if at all – to meet operational needs

Principal Findings - Governance

Current HeV activities are loosely coupled and coordinated, but this is insufficient for moving forward to a large scale system-of-systems

Efforts to implement accountability have failed

Projects' dependencies coordinated via point-to-point discussions (expensive and inefficient)

Schedule is "best guess" and does not address risk mitigation activities

Legacy VistA governance practices – by themselves – are inadequate for HeV

Principal Findings – Scope of Change

In addition to transition to operations and support, the engineering and development organizations are experiencing enormous change

"…VistA was developed in an incremental and evolutionary manner over 25 years … HeV is a new grand design that is very schedule constrained …"

The VA faces unparalleled challenges to manage change to deliver an operationally viable HeV by 2010

Scope of HeV Changes

Current State	Architecture Impact?	End State
Waterfall, RAD development lifecycle	Y	IDL development life cycle
Free form data	Y	Highly structured data
Site specific terminology	Y	Applying national standards
Data view is form centric	Y	Data view is patient centric
Multiple local medical records; Local authority	Y	Single, logical, authoritative HDR

Scope of HeV Changes

Current State	Architecture Impact?	End State
Sequential files (application)	Y	Relational tables (model)
Locally running applications	Y	VistA local, VISN, national applications
Independent monolithic applications	Y	Integrated service-based applications
Source code deployment with local tailoring	Y	Centrally controlled extensions through APIs and parameters

Scope of HeV Changes

Current State	Architecture Impact?	End State
Automated, isolated updates	Y	Incremental, dynamic updates
Local access control	Y	Role-based with single sign-on
Application development team autonomy		Application development team high interdependence

Enablers and Barriers of Change

Enablers
Commitment
Actively engaged stakeholders
Patient focused
Consensus building
Clinical domain expertise
Innovative

Enablers and Barriers of Change

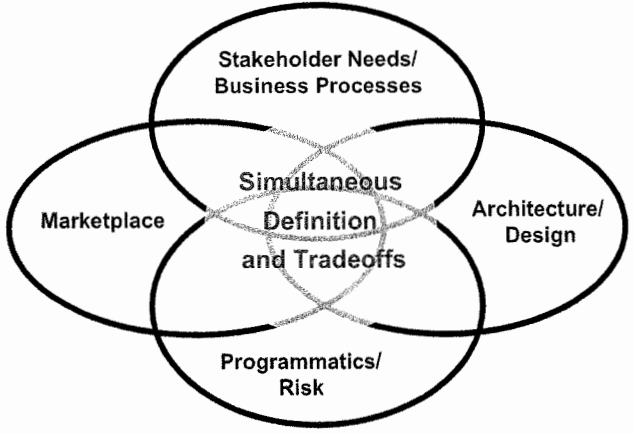
Barriers	
Reactive vs. proactive	VistA skill set
Limited understanding of true structure of legacy	Organizational stovepipes
Hard end dates	Project focused
Control and variability at individual sites	Consensus decision making
Application independence	"M" world assumptions
Highly complex organization	Individual hero actions

Principal Recommendations

Principal Recommendations – System-of-Systems

Recognize the Need for Simultaneous, Continuous Tradeoffs & Balancing

Establish a process for continuous evaluation and validation of decisions, both from a business and architectural point of view



Principal Recommendations – Future State

Refine "To Be" Business Process Models and Transition Plans

Characterize the facility and provider-level operational model

- Determine which operations will be revolutionized (reconceived) and which will be evolved
- Clarify the impact of entities external to the VA
- Inventory, then determine how HeV will handle local extensions including Class III code
- Involve all stakeholders now to conceive intermediate and future states
- Establish business value for each transition

Carnegie Mellon
Software Engineering Institute

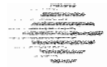
Principal Recommendations – Architecture

Refine "To Be" System Architecture and Develop Transition Plans

Iteratively refine the architecture using discovery and analysis

- Identify and characterize Quality Attribute requirements and tradeoffs
- Identify intermediate states and their associated business value
- Delineate applications & services scope within H**e**V
- Evaluate potential technologies within the context of the architecture and in combination with other technologies

Plan transition through intermediate states to H<u>e</u>V



Carnegie Mellon
Software Engineering Institute

Principal Recommendations – Architecture

Establish a HeV Architectural Validation Capability

Establish a validation lab that simulates the operational world and gather empirical evidence

Perform simultaneous, continuous evaluation and validation of decisions, both from a business and architectural point of view

- Performance analysis
- COOP
- Service-based architecture
- Multi-version deployment and update strategy
- Topology
- Support for local customization

Principal Recommendations – Architecture

Confirm the Viability of a Service-based Architecture Approach for HeV

Understand the risk of failure adopting a new, evolving technology, particularly with the HeV layered approach

Do significant prototyping

Determine scalability of the service-based approach

Identify alternatives

Stay involved in the service-based architecture community and take advantage of related experience

Principal Recommendations – Governance

Establish HeV Governance (1 of 2)

Strong, fully staffed, and empowered PMO is mandatory for success

The PMO should immediately focus on:

- Creating a coherent vision of the HeV system
- Articulating the relationship between HeV and the VA Enterprise Architecture/FEA
- Instituting a governance model as a mechanism for cost effective, timely decisions
- Defining a unified plan for the sequencing, execution and coordination of all HeV projects and deployment activities

Principal Recommendations – Governance

Establish HeV Governance (2 of 2)

The PMO should immediately focus on (cont'd):

- Doing a HeV-wide risk analysis, emphasizing risks across individual projects and architectural choices
- Guiding and adjudicating between the various levels of architecture, dependencies and cross-application requirements
- Understanding and minimizing (as much as possible) the impact on HeV from forces outside of the program

HeV needs a shared vision for a system-of-systems focus now

Principal Recommendations – Change Management

Develop and Implement Detailed Change Management Plans

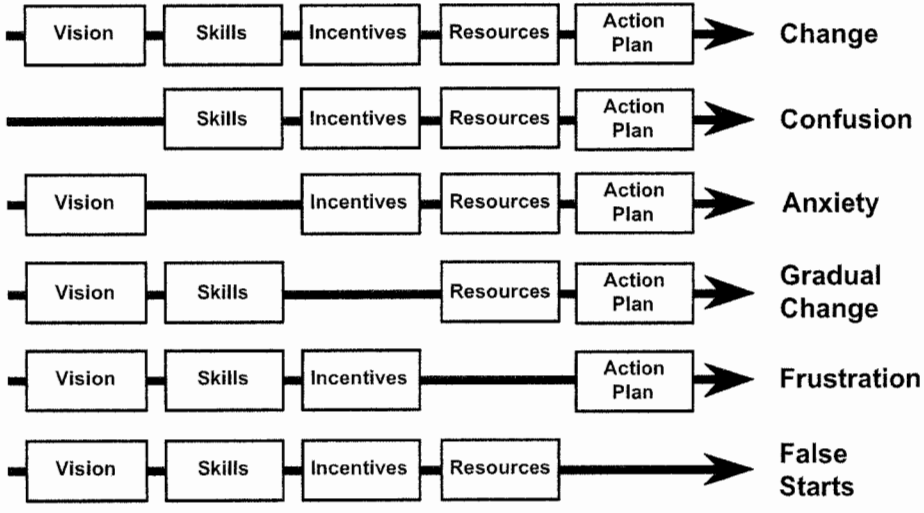
The plans must address

- All types of change H**e**V will bring to the VA, and who and how those changes impact
- The various stages of change
- The appropriate level of change the VA can deal with in a particular time frame

The H<u>e</u>V sequencing plans, schedules and budgets must include the change management activities

The VA must accept the responsibility for managing change

Enabling Factors



Summary

The high level of VA-native domain and proven track record with VistA is a strength – but does not predict success for HeV

"Staying the course" (working harder, not smarter) without fundamental changes in approaches and processes (e.g., governance, engineering, etc.) will result in failure

Phase II Focus

Phase II Focus

The ITA team started Phase II in parallel with the end of Phase I activities

The focus of Phase II includes

- Program management and project management
- Acquisition management
- Development environment
- Security
- Transition to operations and support

The briefing for Phase II is planned for the end of January

Backup Slides

Background

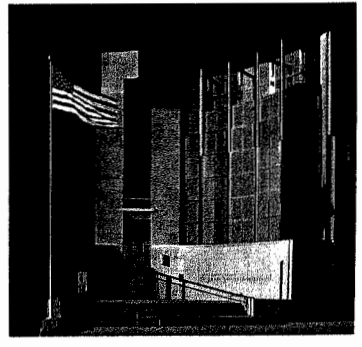
Software Engineering Institute (SEI) Overview

DoD R&D Laboratory FFRDC

Created in 1984, based on a recommendation of a DoD Joint Task Force, chaired by the Deputy Under Secretary of Defense (R&AT)

Mission: Advance the state of the practice of software engineering and software-intensive systems acquisition

Location: A college-level unit of Carnegie Mellon University with principal locations in Pittsburgh, PA and Arlington, VA



Background
ITA Fundamentals

An ITA is an objective evaluation of a program, typically conducted due to cost, schedule, or performance problems

The SEI HeV team conducted the ITA through:

- Planned interviews with the program stakeholders
- Fact-finding visits to facilities
- Facilitated architecture workshop

Carnegie Mellon
Software Engineering Institute

SEI ITA Team

Lisa Brownsword
Grady Campbell
Reed Little
Dr. Linda Levine

Dr. Liam O'Brien
Steve Palmquist, PE
Jim Smith
Mary Catherine Ward
Dr. Carol Woody

Architecture Definitions

A* system architecture *is a means for describing the elements and interactions of a complete system including its hardware elements and its software elements.

The* software architecture *of a program or computing system is the structure or structures of the system, which comprise software elements, externally visible properties of those elements and the relationships among them.

Bass, Clements, Kazman

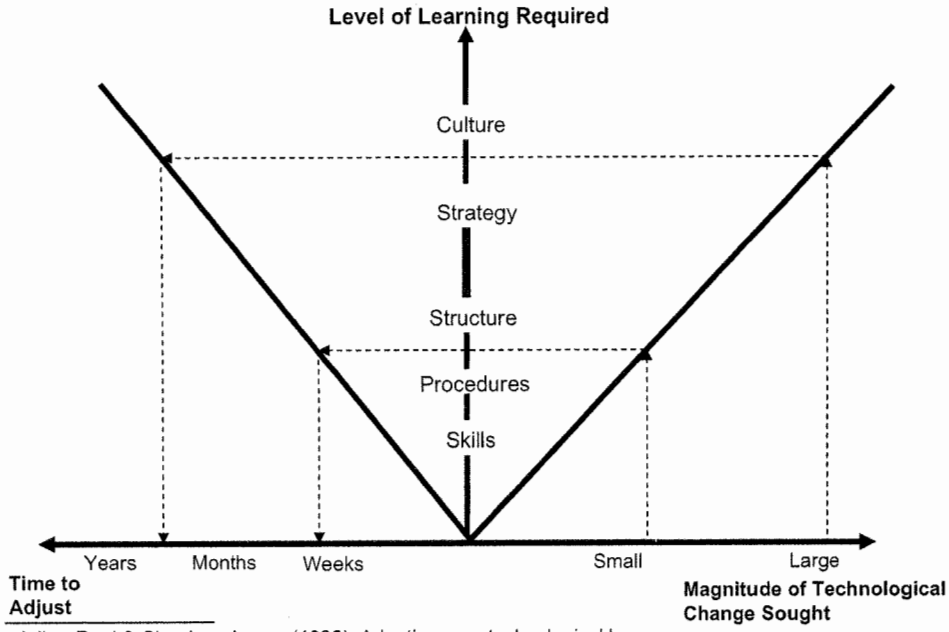
Quality Attribute Definitions

Quality attribute or non-functional requirements (such as for performance, maintainability, availability, security) drive the software architecture.

Quality attribute requirements stem from business/mission goals.

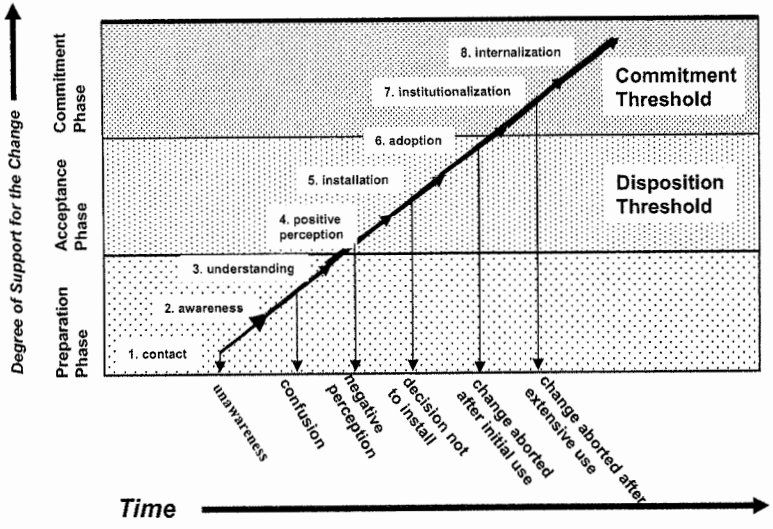
Carnegie Mellon
Software Engineering Institute

Technology: Time and Effort Scale for Implementation



Adler, Paul & Shenhar, Aaron. (1990). Adapting your technological base: The organizational challenge. *Sloan Management Review*.

People: Commitment to Change



Daryl R. Conner and Robert W. Patterson, Building commitment to organization change. *Training and Development Journal*, April, 1982.

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

SEI Independent Technical Assessment Phase II Outbrief

VA HealtheVet-VistA

04 February 2005

Sponsored by the U.S. Department of Defense

Purpose Of This Briefing

This brief presents the overall summary of the Software Engineering Institute's (SEI's) Independent Technical Assessment (ITA) of the Department of Veterans Affairs (VA) HealtheVet-VistA (HeV) program

It summarizes the findings from Phase I, outlines the findings from Phase II, and presents conclusions and recommendations encompassing the entire ITA

Acknowledgements

We are encouraged that the VA requested an independent review early in the HeV program

The SEI acknowledges and thanks the VA and their contractors for their support during the ITA

We especially want to thank our primary points of contact:

- M. Jay Eigenbrode
- Howard Green
- Jennifer Ford
- Amy Falconer
- Richard O'Neal

Outline

ITA Scope

Executive Summary

Phase I Summary

Phase II Findings

Prerequisites For Success

Summary

ITA Scope

ITA Scope

Program management structure

Technical execution and sequencing plan

Architecture framework, including key technology assumptions

Transition-to-operations and support planning

Other technical and program elements

Who We Talked To

Over 100 interviews at all levels of the VA including

- A cross cutting sample of the reengineering and rehosting projects at varying points in the life cycle
- Lynchpin projects such as Health Data Record, Data Standardization, MyHealth**e**Vet and Common Services
- Office of Information – key divisions
- Department resources (acquisition, security, privacy etc.)
- VISN 5 – VA Capitol Health Care Network

Visits to the following VA health care facilities

- Edward Hines Jr. VA Hospital
- Martinsburg VA Medical Center

HeV Program Elements

Elements planned to form HeV

- Seven existing OMB projects
  - Health Data Repository (HDR), Pharmacy, Scheduling, Registration, Eligibility, Enrollment (REE), Fee Basis, Patient Financial Services System (PFSS), Laboratory

- 2005 HeV OMB program
  - Common Services, Platform, MyHealtheVet, Data Standardization, Rehosting (100+ applications)

HeV Program Element Status

In Alpha Test

- Initial Common Services, CPRS-R, Scheduling, Blind Rehab, Spinal Cord Injury, Patient Advocate Tracking System, VPFS, Administrative Data Repository, REE, Bloodbank

In Beta Test:

- HDR (HDR Interim Message Store and HDR Historical)

Deployed or in deployment:

- Voluntary Service System, HDR (VDEF)

100+ applications still to be addressed

- Rehosted, reengineered, etc.

Executive Summary

The VA Has Strengths For Hev ...

VA recognizes they can not stay where they are and still meet future health care needs

There is significant clinical domain expertise

Dedicated staff are focused on the VA's mission

There is strong VA buy-in for a patient-centric vision for health care

Elements such as the electronic health record and data standardization are valued

… But Is Not Positioned For Success

PMO does not have the needed staff, authority, responsibility or operational procedures for a large scale system integration program

Technical execution and sequencing plans are not defined for the program and are minimally defined for the projects

Intended technologies are potentially viable, but the HeV architecture does not tradeoff and balance among the critical drivers necessary to make any architecture viable

Transition to operations and support planning does not address many of the steps needed to facilitate change

The VA Must Rethink HeV

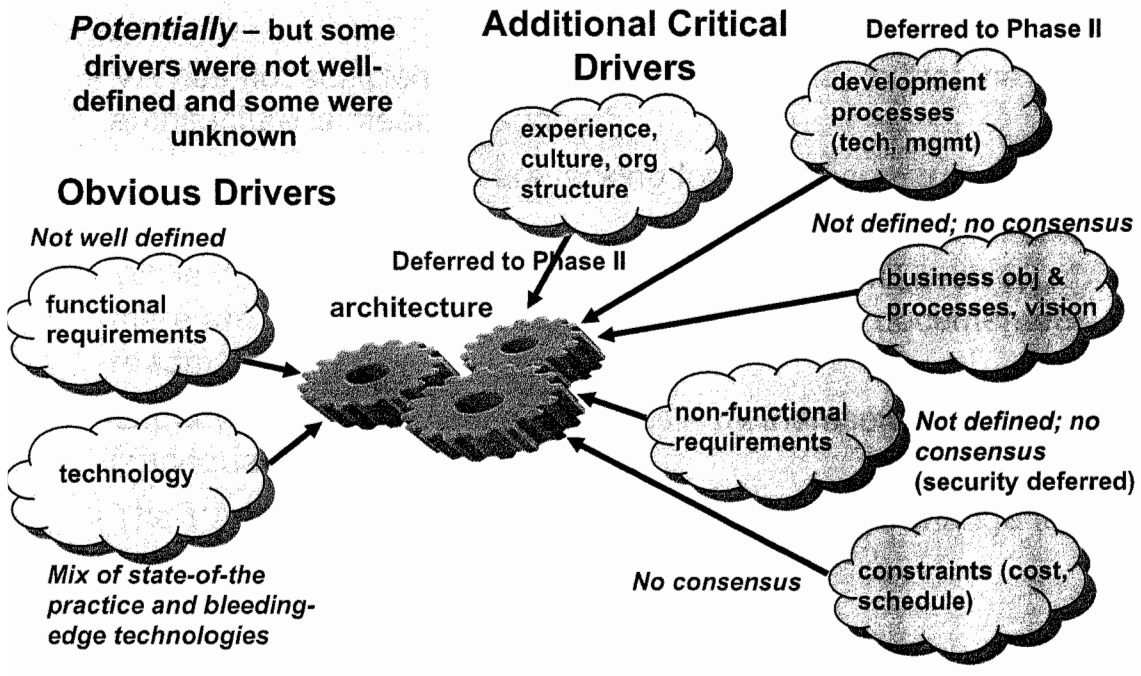
The VA cannot stay with VistA

however

Current plans are not realistic given the complexity and magnitude of HeV and the VA's ability to carry them out

Phase I Summary

End Of Phase I: Is HeV Architecture Viable?

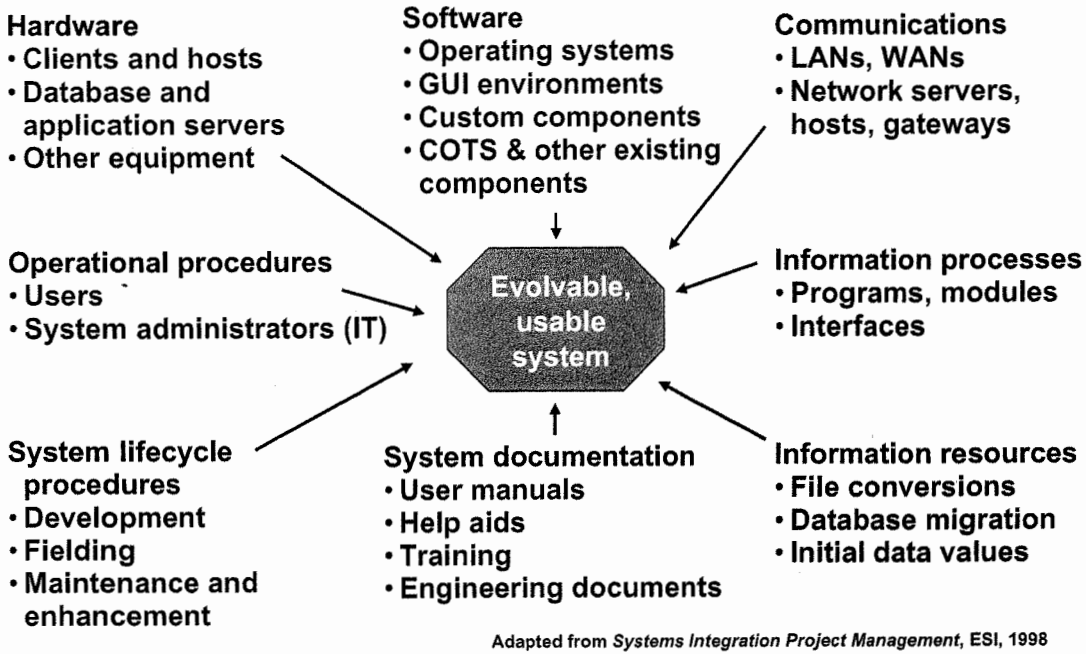


Phase I Findings Revisited

- VA has not sufficiently articulated the future state that the architecture is meant to support
- Verifiable requirements are lacking for critical architectural decisions
- While it is understood the "To Be" architecture will evolve, there are no defined intermediate states and no documented roadmap
- Legacy VistA governance practices – by themselves – are inadequate for H**e**V
- The VA faces unparalleled challenges to manage change to deliver an operationally viable H**e**V by 2010

Phase II Findings

HeV Is A System Integration Program



Adapted from *Systems Integration Project Management*, ESI, 1998

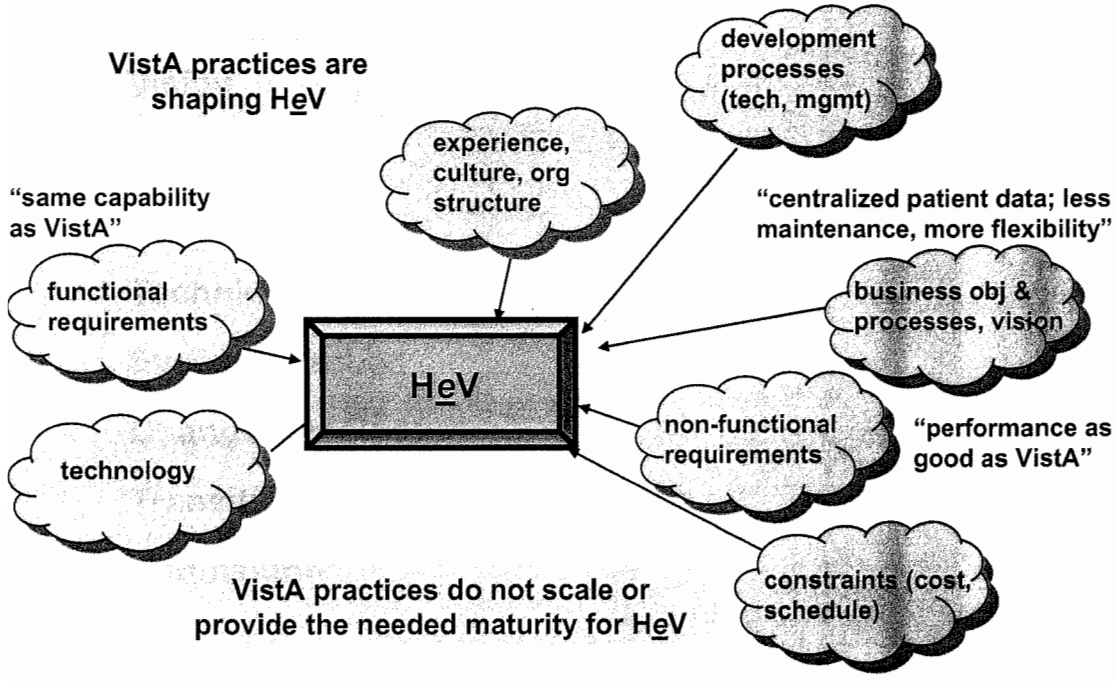
Essential Systems Integration Practices

System integration programs require very different skills, mindsets, methods & management

- **Management practices** – sequencing, monitoring, risk management, coordination
- **Engineering practices** – architectural definition & documentation, integration & test
- **Infrastructure management** – facilities & equipment
- **People management** – field transition & training, PMO and project training & career development
- **Project support** – planning, mentoring, auditing, recovery
- **Business alignment** – stakeholder relationships, business performance

Adapted from *Systems Integration Project Management*, ESI, 1998

Influence Of VistA: Barrier Or Enabler?



Phase II Findings

Vision

Management

Baselines

Technical

Systemic Issues

Change Readiness

Transition To Support

Acquisition

Phase II Findings – Vision

Current HeV vision is insufficient for action

- Not sufficiently defined, articulated or communicated
  - Elaboration needed for successful implementation is missing
  - Technology change has been substituted for vision articulation

Current knowledge is insufficient in key areas

- Medical/Clinical – **Sufficient**
- Large scale system integration – **Insufficient**
- Proposed technology products and standards – **Insufficient**
- Process discipline – **Insufficient**

Phase II Findings – Management

Program perspective is lacking
- Program-level engineering is missing
- Poorly-coordinated, application-centric projects drive technical decisions that have system-wide impacts

New PMO does not have authority, responsibility or staff
- Proposed composition is heavily oriented to oversight
- Does not support sufficient technical and management planning and decision making
- Structure does not address system integration challenges

Program relationships not well understood or managed
- Balance between VistA and HeV
- MyHealtheVet and HeV interaction

Phase II Findings – Management

No true, integrated HeV program picture (budget, schedule, risk, etc.)

Planning and actions do not always reflect evolving risks, constraints, and assumptions

- Deadlines at all cost; critical processes and procedures frequently eliminated to meet end dates
- Impact analysis and feedback cycles are ineffective for planning, scheduling, engineering and setting expectations

Subjective (at best) monitoring of project status

Phase II Findings – Baselines

VistA is complex; HeV is an order-of-magnitude more complex

- Management and coordination of elements
- Internal and external interfaces

Needed VistA and HeV baselines are missing or insufficient

- Management-type baselines (cost, schedule, resources etc.)
- Technical-type baselines (requirements, code, release baselines)
- Operational-type baselines
- Class 3 code at medical centers

Phase II Findings – Technical

Full lifecycle processes are insufficient

- Engineering discipline and technical standards are insufficient – configuration management, release management, testing, etc.
- IDL is neither embraced nor widely adopted because VistA development practices are seen as "good enough"
- Quality is checklist driven rather than results driven

Lack of disciplined, systematic risk, alternatives identification, tradeoff analyses

Experts are marginalized and not given latitude to contribute

Phase II Findings – Systemic Issues

Roles, responsibilities and resourcing are inefficient

- Many roles are "advisory" with no real authority
- "It's their job … I think"
- Specialized skills not bridged by generalists
- Broad stakeholder involvement is good, but default solution of being "involved earlier" and "working harder" is not a sufficient answer
- Adequate resources are usually not applied

Communication model is ineffective

- Lack of common terminology across stakeholder types
- Overly dependent on point-to-point discussions and broadcasts at the expense of structured collaboration and problem solving

Phase II Findings – Systemic Issues

Pattern of ineffective decision making and poor communications leads to multiple perspectives and confusion

- Many decisions are driven by unrealistic, subjective information
- Frequently, range of options considered is too narrow
- Decisions are not documented, disseminated, or enforced
- Authority and responsibility is unclear

Poor planning and management leads to reactive rather than proactive behaviors

Culture inhibits raising risks, issues, problems, or differing opinions

Phase II Findings – Change Readiness

No comprehensive organizational change management plan

- No clear understanding of all change management and training needs for H**e**V
  - Development, support, end-users, etc.
- Focus is on awareness and training; other stages of managing change are often ignored
- Organization cannot be productive in a constant state of turmoil due to unplanned change

Phase II Findings – Transition to Support

"Code is king"

- Current support model is heavily based on the ability to look at the code
- Trial patches affect only the local system

The VistA support model will be ineffective for HeV

- Doesn't address approaches to resolve problems introduced by the HeV environment such as a centralized data repository, multi-tiered platform, limited code access etc..

Phase II Findings – Acquisition

Introduction of new vendors for the Partnership Agreement contract will result in personnel instability

- The workforce may remain the same, but the anticipated migration from company to company will disrupt workflow
- Few have been processed through the new, tougher security criteria, and the lengthy upgrade process is already backlogged

Ineffective working relationships between the program and various acquisition organizations

- Acquisition brought in late in the process
- VA lacks sufficient formalism in acquisition planning and discipline in execution

Prerequisites For Success

Prerequisites For Success

Constitute Proper, Integrated HeV Program Governance

Define the HeV Vision And The Transition Path

Institute Effective, Standard Practices For VistA Now

Manage To Realistic, Changing Program/Technical Options And Risks

Develop A Framework To Meet HeV Program Lifecycle Needs

Constitute Proper, Integrated HeV Program Governance

HeV program office must be empowered, resourced, structured, trained and operate for large-scale systems integration

Project and program status assessments must be realistic and objective, used at decision points, and allow for "off ramps"

Fully-engaged stakeholders must be actively involved in decision making

Decision makers must have sufficient technical and change-management knowledge to understand the impact of their decisions

Define The HeV Vision And The Transition Path

HeV's future must be articulated – the VA must have a common understanding of where it is going

- "To be" business process models and system architecture

Legacy VistA environment must be baselined – the VA cannot gauge forward progress until it knows where it is

- Where the money goes (maintenance & development)
- What people do (developers, maintainers & users)
- What the applications are and do (including local variations)

A roadmap to go from legacy to HeV future must be defined with intermediate states

- Develop and implement change management plans
- Determine what capability will be in what increment

Institute Effective, Standard Practices For VistA Now

System-level elements missing from VistA include

- Requirements management
- Configuration management
- Release management
- Risk management
- Coordination of development teams
- Integration and test

System quality attributes must be articulated and traded off to form the foundation of an effective and viable HeV architecture

- Security in HeV environment introduces new risks

Manage To Realistic, Changing Program/Technical Options And Risks

A robust systems engineering process must be used to build, field, and sustain an effective system that balances all architectural drivers

Integrated, high fidelity lab must be used to explore alternatives and validate HeV instantiations

- Explore architectural and technology alternatives – e.g. confirm viability of service-oriented architecture approach
- Enable early discovery of requirements and design flaws
- Evaluate how functional & quality attributes are satisfied
- Use results to inform program decisions

Develop A Framework To Meet HeV Program Lifecycle Needs

Comprehensive framework for technology selection and deployment, appropriate for enterprise-wide rollout

- Address process, people, technology, culture, etc.
- Cradle-to-grave activities, such as
  - Project initiation
  - Solution definition
  - Approaches for alpha and beta (pilots)
  - Whole product design
  - Rollout
  - Operations, support and maintenance (including evolution)

Next Steps

VA leadership must provide direction and environment for change to reposition HeV program for success

- Focus efforts on high risk, high impact, high priority items
- Identify key players
- Assign ownership with decision-making authority
- Bring in outside help where necessary

Develop an action plan; manage as a project in-and-of itself

- Roles and responsibilities, resources, tasks
- Objective measures of progress and success

Summary

Sponsored by the U.S. Department of Defense

The VA Must Rethink HeV

Current approach for HeV is not viable

- Vision is insufficient for coordinated, cost-effective action
- A realistic, actionable program plan is missing
- Current engineering and management practices are insufficient for execution
- Architecture does not tradeoff and balance among critical program drivers
- Deployment strategies and transition to operations and support are not adequately defined

Until the VA satisfies the prerequisites for success, the HeV effort is unacceptably high risk

"Staying the course" will fail to deliver HeV

Backup Slides

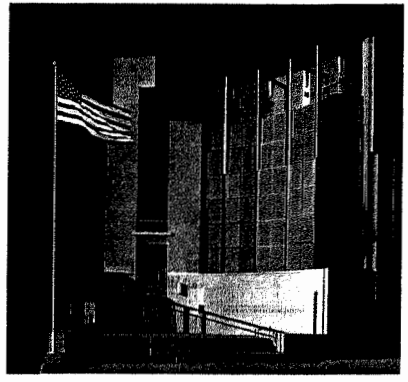
Software Engineering Institute (SEI) Overview

DoD R&D Laboratory FFRDC

Created in 1984, based on a recommendation of a DoD Joint Task Force, chaired by the Deputy Under Secretary of Defense (R&AT)

Mission: Advance the state of the practice of software engineering and software-intensive systems acquisition

Location: A college-level unit of Carnegie Mellon University with principal locations in Pittsburgh, PA and Arlington, VA



ITA Fundamentals

An ITA is an objective evaluation of a program, typically conducted due to cost, schedule, or performance problems

The SEI HeV team conducted the ITA through

- Planned interviews with the program stakeholders
- Fact-finding visits to facilities
- Facilitated architecture workshop
- Facilitated security workshop
- Document review

SEI ITA Team

Kate Ambrose
Lisa Brownsword
Grady Campbell
Reed Little
Dr. Linda Levine
Melissa Kasan
Dr. Liam O'Brien
Steve Palmquist, PE
Jim Smith
Mary Catherine Ward
Dr. Carol Woody

Backup – Phase I Summary

Phase I Focus – Is The HeV Architecture Viable?

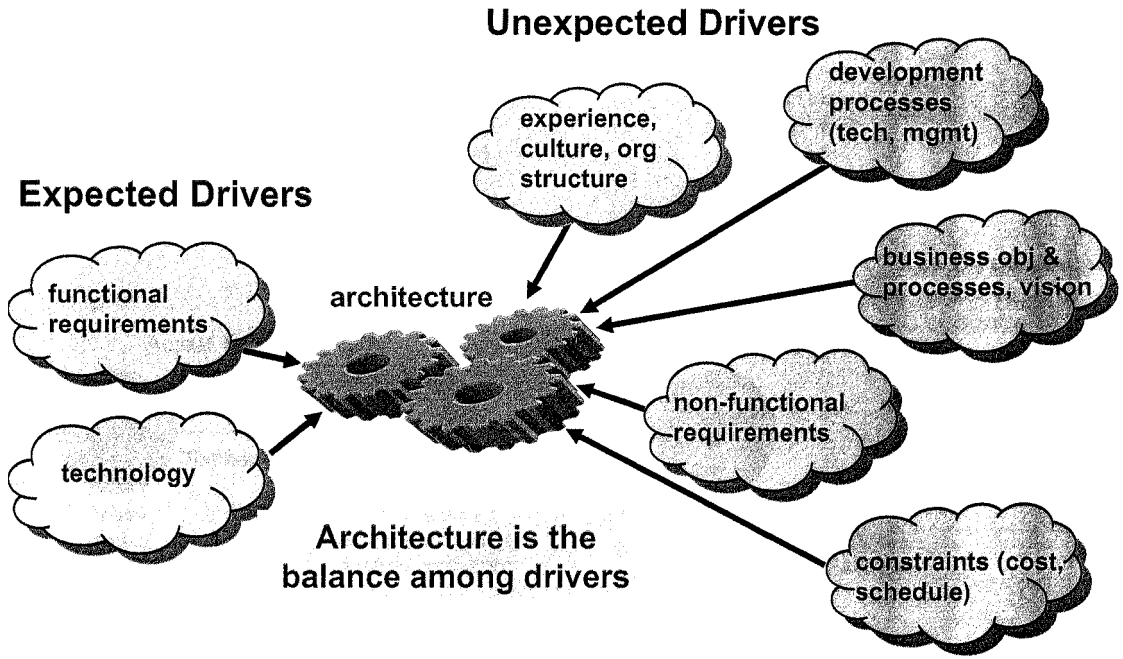
The SEI ITA team chose the following as a definition of viable: "capable of cost-effective use for its intended purpose"

To be viable, the HeV architectural approach must coordinate activities across:

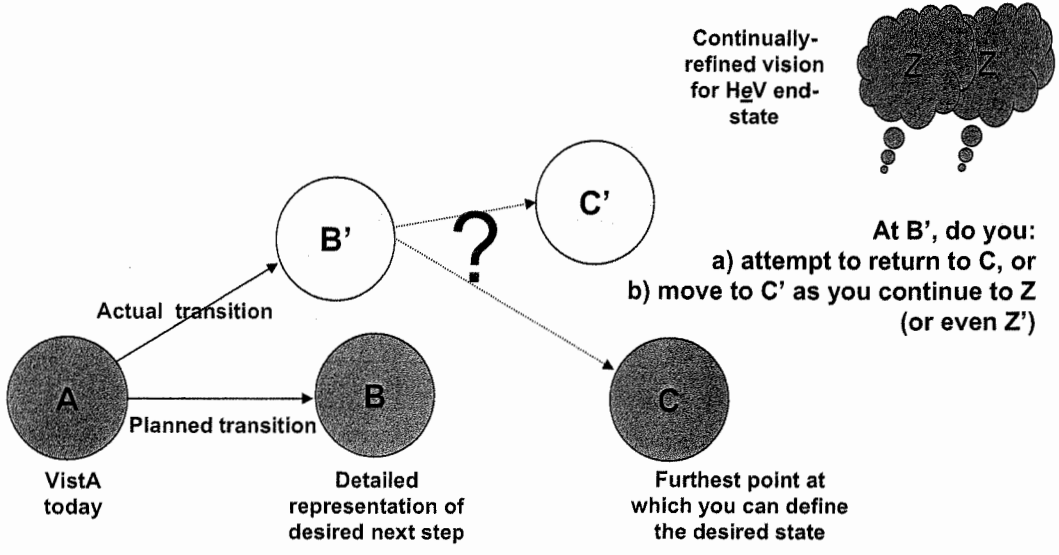
- HeV as a system-of-systems
- Individual HeV systems (applications) and services
- All HeV software architectures

A viable HeV architecture must not only meet the functional requirements but also meet the non-functional or quality attribute requirements as well

Drivers Of An Effective Architecture



Lack Of Architecture Roadmap And Intermediate States



Phase I Principal Finding – Scope Of Change

In addition to transition to operations and support, the engineering and development organizations are experiencing enormous change

"...VistA was developed in an incremental and evolutionary manner over 25 years ... HeV is a new grand design that is very schedule constrained ..."

The VA faces unparalleled challenges to manage change to deliver an operationally viable HeV by 2010

Backup – Proper, Integrated Governance

HeV PMO Responsibilities – 1

Establish HeV baseline requirements; ensure that evolving requirements are addressed or explicitly deferred

Validate that HeV overall program plan addresses all necessary components (projects)

Ensure that each HeV component has an appropriate project approach – and that the project follows it

HeV PMO Responsibilities – 2

Reconcile competing demands on resources, schedule and functionality

Ensure that all interactions (internal and external) are identified, characterized, tested and managed

Ensure that all interfaces (internal and external) are identified, characterized, tested and managed

Ensure major risks are identified and avoided, mitigated or accepted

HeV PMO Responsibilities – 3

Ensure that all specialty engineering concerns (security, reliability, etc.) are addressed or explicitly deferred

Ensure that HeV as a system is implemented & tested

Ensure that configuration management is adequate

Ensure that all aspects of HeV are effectively communicated to all appropriate stakeholders

Sample Types Of Expertise For The HeV PMO – 1

Business analysis & stakeholder management group

- Requirements

Change management group

- Training
- Mentoring

Integration & test group

Configuration & release management group

Adapted From *ESI Systems Integration Project Management 1998*

Sample Types Of Expertise For The HeV PMO – 2

System/software architecture group

- Interface control
- Various specialty engineering (non-functional requirements)
- COTS
- Legacy migration criteria and decisions

COTS procurement & license management

System component development teams (projects)

Adapted From *ESI Systems Integration Project Management 1998*

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Backup – Develop An Enterprise Framework

Sponsored by the U.S. Department of Defense

What People Need During Transition

Information: what's going to happen; when, how, & why; changes & updates

Inclusion: in the planning process; buy-in on the vision

Support: two way communication, help disengaging from the old, reassurance that they'll have a job, extra resources to manage the change, etc.

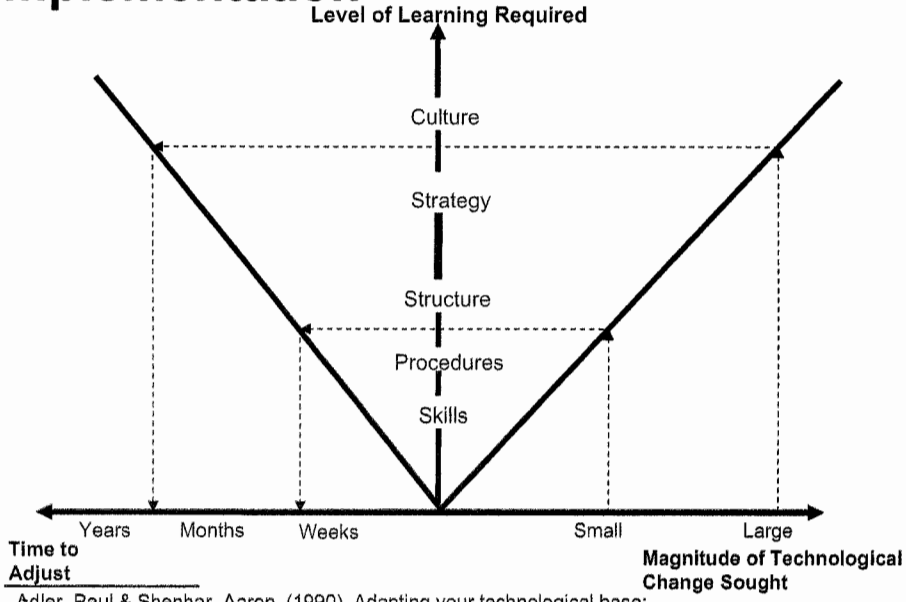
Safety: "islands of stability," anchors

Skills: training for new tasks, coaching for new roles

Freedom: from blame, so they will take risks

Rewards: intangible and tangible

Technology: Time And Effort Scale For Implementation



Adler, Paul & Shenhar, Aaron. (1990). Adapting your technological base: The organizational challenge. *Sloan Management Review*.

Backup - Security

Security is Currently Perceived as Low Priority

VA Infrastructure has security issues HeV inherits

- WAN not secure based on IG & OCIS studies, but sensitive information in clear text assumed secure
- OMB requires accreditation and certification (A&C) for FISMA
  - 600 VHA systems already in production need A&C
  - System ownership unassigned

VistA technology has limited security risk

- Technology (MUMPS, Cache) is not widely exploited
- Source code is published but not widely usable
- Infrastructure and applications are locally controlled and isolated

Security Success Is Project Dependent

HeV environment is high risk

- Technology is widely known and extensively exploited
- Shared source code can be widely used and analyzed
- Increased reliance on the WAN for movement of sensitive data (medical records, personal identity)
- Increased interdependence – shared common services

HeV architecture plans include robust security mechanisms

- Security mechanisms planned for the architecture and infrastructure
- Application security requirements are linked to mechanisms
- Independent oversight for projects - A&C by ASIS and Authority to Operate (ATO) from OCIS
- Transition plan for secure user sign-on from VistA to HeV

HeV Security Is Not Strongly Supported

Security resources for HeV are severely limited

- ASIS supports A&C for 45 projects with 4 security engineers
  - Relying on documents generated by projects - inconsistent
  - Support for direct validation is limited
- Rely on project reviews for project assurance validation – no formal metrics or measures
- System owners (who have not been identified) will be notified of risks and asked to take action
- Project resources and timetables do not include support for security testing - Security Controls Assessment (SCA) needed
- OCIS resources are limited (2 people) for ATO

Description of HealtheVet-VistA Components – FY06

Platform

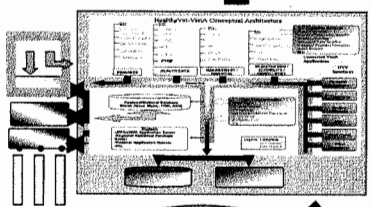
- Scheduling Infrastructure
- Spinal Cord Injury Infrastructure
- CPRS-R Infrastructure
- National Data Processing Centers
- Enterprise License Agreements

My HealtheVet Connectivity

- Electronic Access to VHA Electronic Health Records

Data Standardization

- Problem List
- Clinical Documents
- Immunizations
- Radiology
- Orders
- Encounters
- Adverse Reactions
- Clinical Procedures
- Consultations
- Dental
- Dietetics



HealtheVet

Rehosting

- ADT-R
- App Dev Process Security
- CHDR
- Clinical Procedures
- CPRS-R
- Nursing
- VistA Imaging
- Vitals
- Spinal Cord Injury
- HeV Foundations

Projects, on completion, **provide incremental & immediate benefits** to HealtheVet current and future capability

Common Services

- Person Service- Demographics
- Person Service-Identity Management
- Delivery Service
- Administrative Data Repository (ADR)
- ADR Data Migration
- Application Preferencing Service
- National Provider Identifier
- Audit Service
- Enterprise Exception Log Service
- Institution File
- CS Maintenance Support

Carnegie Mellon Action Dashboard

November 2005

Area	Status	Definition	Status Summary	Key Success Factors
1) **Develop a HeV strategic plan**	Version 2 delivered 10/31/05.	•Objectives •Enabling Strategies	Key Accomplishments: ▪10/31/05: Version 2 of the strategic plan was delivered ▪1/31/06: Strategic Plan version 2.1: Continued evolution of components of the strategic plan based on work with CM/SEI and others ▪3/31/06: Strategic Plan Version 2.2: incorporate recommendations from FY07 transition workgroup to be delivered	Addresses CM Prerequisite for Success *"Define the HeV Vision And The Transition Path"* and *"Develop A Framework to Meet HeV Program Lifecycle Needs"*
2) **Define the future state of healthcare that the IT environment must support**	Version 2 delivered 10/31/06.	•Validate HealtheVet-VistA draft strategic plan •Identify current issues •Identify needed future capabilities •Business areas for inclusion are clinical, administrative, financial, research, education	Key Accomplishments: ▪6/30/05: Version 1 of HeV Strategic Plan (Including Vision, Mission, Objectives, Enabling Strategies) was delivered ▪7/13/05: completed documentation describing the approach for business capabilities focus group meetings ▪10/31/05: Strategic plan V2 containing a high level view of the near term operational capabilities was delivered ▪10/31/05: Core group of clinical capabilities defined and provided to business owners for validation. ▪ 1/31/05: Operational scenarios to be documented based on input from FY 07 transition workgroup	Addresses CM Prerequisite for Success *"Define the HeV Vision And The Transition Path"*

Carnegie Mellon Action Dashboard

Area	Status	Definition	Status Summary	Key Success Factors
3) Define VHA OI governance model	Initial draft of governance model delivered 8/31/05	• Defines decision-making process • Establishes guidelines for issue identification and escalation • Defines areas of control and levels of authority • Establishes accountability	Key Accomplishments: ▪8/2/05: Action plan completed for HeV Governance, anticipating validation pass through SP group ▪8/19/05: Completed Action Plan for HeV Governance ▪8/31/05: Completed first draft HeV program Governance model ▪1/31/06: First update of the draft governance plan to accommodate sub-level management plans to be completed ▪1/31/06: Pilot Risk and Configuration Management processes initiated ▪1/31/06 Initial draft of VA/VHA organizations defining governance structures that will influence program governance will be provided	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*
4) Define VHA OI operational model	Action plan for operational model delivered 8/31/05	• Define future operational organization in terms of functions • Define required key roles and responsibilities • Describe organization and interaction of different lines of services • Describe any future competency centers required • Define external relationships (e.g., EPMO, Steering Committees, Internal and External Liaisons, etc.)	Key Accomplishments: ▪6/30/05: Completed overview of HeV Operational Model ▪7/29/05: Completed definition of HeV Operational Model including required roles and responsibilities delivered ▪ 8/19/05 Completed Action Plan for implementation of HeV Operational Model ▪11/30/05: Completion HPMO staff model ▪3/31/06: Transition workgroup to deliver FY 07 migration roadmap that will provide the operational capabilities that will be rolled out ▪3/31/06: VHA OI operational model completed based on reorganization	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*
5) Develop organizational structure based on operational model	On target for October 31, 2005 deliverable	• Develop organization chart • Assign key personnel • Obtain approval of VHA and VA executives • Implement organizational change	Key Accomplishments: ▪ 11/30/05: HPMO staff model will be completed	Addresses CM Prerequisite for Success *"Constitute Proper, Integrated HeV Program Governance"*

Carnegie Mellon Action Dashboard

Area	Status	Definition	Status Summary	Key Success Factors
6) Develop draft tactical plan	Tactical work plans Delivered on 9/30/05. FY06 work validated against business requirements on 10/31/05	• Decompose strategic plan (the 'what') into the tactical (the 'how') • Map to CM/SEI findings and OI planned responses	Key Accomplishments: ▪9/30/05: completed tactical work plans for each Management Objective/Enabling Strategy ▪10/31/05: completed the connection of current FY06 work efforts to business objectives and requirements ▪1/31/06 Pilot sequencing plan process ▪1/31/06 Pilot change management ▪3/31/06: Tie action plans to outcomes of transition plan workgroup	Addresses CM Prerequisite for Success *"Manage To Realistic, Changing Program/Technical Options And Risks"*
7) Roll individual tactical plans into single master plan	On target for November30, 05 deliverable	• Ensure alignment of master plan with strategic plan • Engage business owners with tactical plan prioritization	Key Accomplishments: ▪10/28/05: Completed the definition of TWP's which will be able to be rolled into the Master Action Plan ▪10/31/05 Completed the alignment of FY06 HealtheVet VistA projects to the VA/VHA strategic plan. ▪3/31/06: Complete the alignment of all VHA IT projects to the VA/VHA strategic plan	Addresses CM Prerequisite for Success *"Develop A Framework To Meet HeV Program Lifecycle Needs"*
8) Adjust FY06 funds based on prioritized tactical plan	10/31/05 project alignment to funding availability complete		Key Accomplishments: ▪ 10/31/05 FY06 Completed the alignment of all HealtheVet VistA projects to the VA/VHA strategic plan and balanced project costs against available funding. ▪3/31/05: Complete the alignment of all VHA IT projects to the VA/VHA strategic plan and balance project costs against available funding.	

Major Components of HealtheVet-VistA (FY06)

- **Rehosting:** Migration of existing M-based applications into the HeV architecture and data structures (J2EE-Based applications).
- **Common Services:** A "service oriented" architecture – similar software functions in different applications are isolated and streamlined so they can be coded once and reused many times.
- **Data Standardization:** The establishment of data standards across all VHA sites to ensure system interoperability and exchange of compatible information.
- **Platform:** Provision of the physical computing infrastructure, including licenses and support contracts to operate the HeV program.
- **My HealtheVet Connectivity:** A person-centered health portal providing veterans online access to electronic health records.

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Characterize System Quality Attributes	In-process	• Establish classes of quality attributes for Architecture • Mine current doc's for quality attributes/business drivers • Validate quality attributes/business drivers • Load quality attributes into requirements repository	Key Accomplishments: -10/31/05: Completed the development of a document detailing business drivers from different HVV sources, validated business drivers and included as part of V2 of strategic plan 10/31/05 - Finalized list of critical quality attributes and incorporate into HealtheVet Requirements Management Repository. 10/31/05: Identified the essential clinical and veteran capabilities created as part of V2 of the strategic plan 11/05/05 - Completed quality attribute tradeoff analysis. 12/05/05 - Begin phased operationalization of HealtheVet Requirements Management processes, including full traceability to two projects.
Define migration path from legacy system	In-process	• Identify Intermediate states and their business value • Delineate applications and services scope • Establish validation lab	Key Accomplishments: ▪10/31/05: completed high-level intermediate states of HVV (Roadmap Version 1) ▪1/31/06: Pilot sequence planning process. ▪3/31/06: Complete Transition Roadmap Version 2

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Establish verifiable requirements for critical architectural decisions	In-process	•Verity that SOA is viable for very large, integrated organization •Determine scalability of the service-based approach •Develop priority list of prototyping efforts that address key architectural issues •Prototype Architectural Capabilities	Key Accomplishments: ▪9/29/05 Received briefing from Gartner Group regarding viability of SOA ▪10/31/05: completed initial draft of technical risks that must be address ▪1/31/06 Develop the list of Prioritized prototyping efforts. ▪3/31/06: Incorporation of prototyping efforts into V1 of transitional roadmap document
Tightly coupled HVV activities to support moving forward a large scale system of systems	In-process	•Define responsibilities for PMO	Key Accomplishments: •10/31/05: Completed Roles and Responsibilities of PMO •11/30/05: finalize HPMO organizational structure •3/31/06: phase 1 staffing of HPMO to 90%

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Stakeholders need to share a common understanding	In-process	•Validate scope of HVV •Develop a Communication Plan •Develop a Governance Plan	Key Accomplishments: ▪8/17/05 Delivered draft of Governance model ▪9/2/05 Delivered draft of Stakeholder list for Communication plan ▪ 8/19/05: Finalization of Governance Action Plan (behind schedule, awaiting feedback, updated projected completion 10/31/05) ▪10/31/05 completed 2 page briefing on scope and vision of HealtheVet ▪2/28/06: Communications plan complete ▪1/31/06: Governance plan updated based on information from transition planning workgroup ▪3/31/06:Governance plan updated based on information from transition planning workgroup

Carnegie Mellon Action Dashboard

Carnegie Mellon Area	Status	Definition	Status
Establish a plan which provides for tracking, managing, controlling and reporting	In-process	• Define a Risk Management Planning process • Develop an action Plan to support tracking and Implementation • Define a sequencing plan for HVV	Key Accomplishments: ▪ 10/3/05 – Revised SEI recommendations incorporated into Master Action Plan ▪ 10/4/05 – Risk management tool selection memo submitted for approval ▪ 10/5/05 – Prototype of automated status reporting capability completed ▪ 10/18/05 – Automated status reporting capability rolled out; working through assignment issues ▪ 10/25/05 – Risk management GAP Analysis submitted for approval ▪ 10/27/05 – Submitted updated project plan ▪ 10/27/05 – Continued review of Integrated Risk Mgmt Plan ▪ 11/02/05 – Completed strategic plan review for proper action plan assignment ▪ 11/30/05 - Refine Master Action Plan with content, structure, and integration points ▪ 12/31/05: Risk Management process rolled out