WHICH VA IT ORGANIZATIONAL STRUCTURE WOULD HAVE BEST PREVENTED VA'S "MELTDOWN" IN INFORMATION MANAGEMENT

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 28, 2006

Printed for the use of the Committee on Veterans' Affairs

Serial No. 109-58

28-454.PDF

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2007

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

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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*
JOHN CAMPBELL, *California*

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*
JOHN T. SALAZAR, *Colorado*

JAMES M. LARIVIERE, *Staff Director*

CONTENTS

June 28, 2006

Page

Which VA It Organizational Structure Would Have Best Prevented VA's "Meltdown" In Information Management 1

OPENING STATEMENTS

Chairman Buyer 1
Hon. Bob Filner 3
Prepared statement of Mr. Filner 50
Hon. Sam Farr (introduction of his constituent, Robert J. Brandewie, Defense Manpower Data Center) 4

WITNESSES

Gauss, Hon. John A., Ph.D., President and Chief Operating Officer, FGM, Inc. (former Chief Information Officer, U.S. Department of Veterans Affairs) 7
Prepared statement of Hon. John A. Gauss 59
McFarland, Hon. Robert (former Assistant Secretary for Information and Technology, and former Chief Information Officer, U.S. Department of Veterans Affairs) 9
Howard, MG Robert T. (Ret.), Senior Advisory to the Deputy Seretary Supervisor, Office of Information Technology, U.S. Department of Veterans Affairs..... 10
Prepared statement of Hon. Robert Howard 61
Brandewie, Robert J., Director, Defense Manpower Data Center..... 12
Prepared statement of Mr. Robert Brandewie 67
Bresson, Jim, Vice President and Managing Partner, Gartner Consulting 14
Prepared statement of Mr. Jim Bresson 73

WHICH VA IT ORGANIZATIONAL STRUCTURE WOULD HAVE BEST PREVENTED VA'S MELTDOWN IN INFORMATION MANAGEMENT

WEDNESDAY, JUNE 28, 2006

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

The committee met, pursuant to call, at 10:40 a.m., in Room 334, Cannon House Office Building, Hon. Steve Buyer [chairman of the committee] presiding.

Present: Representatives Buyer, Bilirakis, Boozman, Filner, Brown of Florida, Brown-Waite, Udall, Salazar, Moran, Stearns, Herseth.

The Chairman. The full Committee of House Veterans' Affairs Committee will come to order June 28th, 2006.

Good morning, ladies and gentlemen. This is the fourth full Committee oversight hearing on the recent theft of sensitive information belonging to as many as 26.5 million veterans and 2.2 million servicemembers and their family members from a VA employee's home in May of 2006.

We will receive testimony today from current and former Department of Veterans Affairs' Chief Information Officers. This testimony will help us examine the VA's information technology reorganization and review the Secretary's decision to move to a federated model versus a centralized approach recommended by VA's own consultant, Gartner Consulting, which is one of the most leading-edge technology companies and they are experts with whom we have consulted.

That judgment was also in the complete opposite direction to that which the House had recommended in the passage of legislation last year.

This hearing will also focus on institutional barriers to an integrated departmental policy on cyber security and to protection of sensitive personal data presented by VA's current IT organizational structure.

Further, we will examine the implication of information security as it relates to the organization of VA IT. As we examine information management and security, two Federal statutes are of central impor-

tance, the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act of 2002, more commonly known as FISMA.

The Clinger-Cohen Act created a Chief Information Officer for each Federal agency. As defined by the Clinger-Cohen, the CIO's responsibilities include:

One, assisting the agency head to ensure that IT is acquired and information resources are managed in a manner that implements the policies and procedures of the agency;

Two, developing, maintaining, and facilitating a sound and integrated IT architecture for the agency;

And, three, promoting an effective and efficient design and operation of all major information resources management processes of the agency.

This Committee's examination of VA's information management over the past eight years have clearly shown the extent and impact of information management decentralization at the VA.

The Department's CIO is not fully empowered to enforce policy and cannot fulfill either the letter or the intent of Clinger-Cohen.

In our questioning last week of Tim McLain, the VA's General Counsel, we saw how the Department's lawyers in 2004 gave the narrowest of possible interpretations of then Secretary Anthony Principi's decision to centralize IT authority.

The General Counsel's questionable opinion that his directive was outside the statutory authority of FISMA, I believe, was a contributing factor to the 16 unmitigated vulnerabilities. I have referred to his legal opinion as a heterodox legal opinion.

The Federal Information Security Management Act or FISMA requires each agency to inventory its major computer systems, identify appropriate security protections, and develop, document, and implement an agency-wide information security program.

FISMA also requires an annual independent review of agency information security program. This review assesses the effectiveness of the information security programs, plans, and compliance of FISMA.

The Office of Management and Budget is then required to compile a summary of Federal government security performance and report to Congress on the implementation of FISMA.

In our hearing last week on academic and legal implications of the DA's data loss, I said the Department does not identify who is in charge of developing policy, implementing policy, or enforcing policy.

The March 2006 FISMA report confirms my statement, indicating VA received a grade of "F" in a category on establishing and following information security policy.

Today, despite evidence piled high over the years, the Department's refusal to get control of its IT systems undermines efficiency, threatens the security of sensitive information, and endangers pa-

tient safety, despite the fact of the unprecedented data compromise that has revealed much larger problems related to decentralization.

The centurions of the status quo in VA administrations, especially in its health administration, insist on protecting their turf, and veterans and families, I believe, could pay the price.

Today through the eyes of two former VA CIO's, Bob McFarland, Dr. John Gauss, we have unique opportunity to examine what occurred within the Department during the years that this evidence accumulated and was sadly disregarded by many who could have made a difference.

We also welcome General Bob Howard, the VA's Acting Assistant Secretary for Information and Technology; Robert Brandewie is the Director of Defense Manpower Data Center; and Jim Bresson is a Managing Partner and Vice President of Gartner Consulting.

Gentlemen, we thank you in advance for your willingness to be here and to contribute to these proceedings. I believe your insights today will be extremely important.

I also would like to recognize in the audience today, we have veterans from the Merchant Marines of World War II. We thank you for your presence. We welcome you to the Veterans' Affairs Committee room, and we thank you for your service to country. You and your generation truly have made a difference in freedom of the world and you left liberty in your footsteps.

I would like you to know we have some votes that are now about to occur. I will recognize Mr. Filner for an opening statement. And then I would welcome the Merchant Mariners to meet. There is a room directly behind.

And what I will have is when we leave, I will turn you over to Kelly Craven, our Staff Director. Kelly is right here. Kelly, if you will stand up. And I will have Committee staff speak with the Merchant Mariners.

Mr. Filner.

MR. FILNER. Thank you, Mr. Chairman, and thank you for your courtesy to the Mariners who are here.

As you know, many are in their late seventies and eighties, served our country in World War II, had the highest casualty rates of any service in the war. And, yet, when the war was over, the GI Bill did not apply to them. And even later attempts to make up for a past injustice was not done. They missed out on the college education provided by the GI Bill, purchase of homes.

As you know, Mr. Chairman, I have a bill House Resolution 23 called a Belated Thank You to our Merchant Mariners of World War II. A majority of the Congress, over 260, have co-sponsored it. A majority of this Committee has co-sponsored it. And I think they would like to talk to you and your staff about trying to get a vote on that at some point in this Congress.

So I appreciate your courtesy, Mr. Chairman. Am I recognized for the opening statement on this hearing?

And we will have votes and the staff of both Democrats and Republicans will be talking to you and we will try to join you later during the hearing.

Again, Mr. Chairman, your opening—

THE CHAIRMAN. Mr. Filner—

MR. FILNER. Yes, sir.

THE CHAIRMAN. If I could do this by way of procedure. Mr. Farr of California is here and he would like to introduce one of the witnesses here today. Can we yield to Mr. Farr?

MR. FILNER. Please.

THE CHAIRMAN. Can we do that for an introduction?

MR. FILNER. I will be happy to.

THE CHAIRMAN. Mr. Farr.

MR. FARR. Thank you very much, Mr. Chairman and members of the Committee. It is a pleasure for me.

I am a member of the Appropriations Subcommittee with this jurisdiction, the military quality of life and Veterans' Affairs. And we had a similar hearing yesterday. In that hearing, the Chairman was there and I appreciate this effort.

I want to just tell you that out in my district, I represent the former Ft. Ord, which is the largest military base ever closed in the United States, and out of that, the Department of Defense kept a Manpower Development Center there. It is a center where all of the personnel information for all of the people in the military and their families is kept.

And it is available 24/7, and you get calls from all over the world from spouses wondering about healthcare insurance or about issues of family or soldiers or, you know, divorce status or all the kinds of data that one would have. And that center has been leading in helping the Department of Veterans Affairs with their security issues.

And the fellow who has really done the work to keep this center a state-of-the-art, quality center in that is Robert Brandewie who is here as a speaker today. He has developed the Defense Biometric Identify System which has centralized the database. It integrates biometric and other information.

He has also received all kinds of awards and is now being considered as one of the four finalists for the 2006 Service to America Metal to be awarded in September. And it is just a pleasure to have somebody with such high skills and such incredible accomplishments come and share what they are actually doing on the ground to help men and women in uniform.

So I thank you for allowing me to introduce my constituent to you and good luck with your Committee.

THE CHAIRMAN. Thank you very much, Mr. Farr. We appreciate

your work on Appropriations as you work with us to come to these solutions and be of assistance to the VA. So thank you for your quality work.

Members, we have one vote. It is a motion to adjourn. I would like to recess the Committee. When we return, then Mr. Filner will give an opening statement and we will proceed with testimony.

The Committee stands in recess for about seven minutes.

[Recess.]

THE CHAIRMAN. The Committee will come back to order.

Mr. Filner, you are now recognized for an opening statement.

MR. FILNER. Mr. Chairman, since we have kept these people waiting through the vote, I am going to submit my statement for the record. I do agree with what you said and so I do not need to add anything.

I would just like to add one little remark, if I may. Mr. Chairman, Secretary Nicholson said that they are going to correct this problem, but we have to be patient. And I think we know what he means by being patient, as you have been personally working on it. It took the VA at least seven years to address this problem.

And during our May 25th hearing, you directed VA officials to submit a chronology, time lines of events related to the handling of information related to the data loss, and you asked it for about ten days.

I note that over one month has now elapsed since the breach, and we are still being asked to be patient to respond to your request. We might think about directing VA to provide these time lines by the end of close of business today. Maybe we should consider asking that they be prepared independently, have them signed under a perjury clause, witnessed and sealed by the Inspector General.

We should have these time lines not only from the panel that we met with on May 25th, but also from the witnesses scheduled for tomorrow. I think it is time to send a message that we have been patient long enough.

Thank you, Mr. Chairman.

[The statement of Bob Filner appears on p. 50]

THE CHAIRMAN. Mr. Filner, all members that may have opening statements will be submitted for the record. And I thank the gentleman for bringing that issue back to the Chair's attention.

I note that sitting in the audience is the Deputy Secretary, and if you could make sure that someone has that prepared. Any questions on it, please be in touch with the Staff Director. And if you could bring that with you tomorrow and submit it to the Committee. Someone, I am sure, has been working on it.

And I think that is probably the best way to handle that, Mr. Filner. Would that be acceptable?

MR. FILNER. That is fine.

THE CHAIRMAN. All right. Should not be any problem with that,

should there?

DEPUTY SECRETARY MANSFIELD. No.

THE CHAIRMAN. Okay. All right. With this panel, we have an Army veteran, Robert McFarland. He served in the Vietnam War. He was nominated by President George W. Bush to serve as the Assistant Secretary for Information and Technology in the Department of Veterans Affairs on October 15th, 2003, and was confirmed by the Senate on January 22nd, 2004.

Prior to his appointment, he served as Vice President of Government Relations for Dell Computer Corporation. Mr. McFarland left the Department of Veterans Affairs on May 18th of 2006.

We will also hear testimony from Dr. John Gauss who served 32 years in the United States Navy. Following his retirement, Rear Admiral Gauss was nominated by the President and confirmed by the Senate to serve as the Assistant Secretary for Information and Technology and Chief Information Officer for the Department of Veterans Affairs from August 2001 through June 2003.

Rear Admiral Gauss transitioned from government service to the private sector accepting a senior position with Science Application International Corporation in September of 2003. His primary focus at this company was the Olympic C41 Security Project considered critical for safe and successful 2004 Summer Olympic Games in Athens, Greece.

In January of 2005, Admiral Gauss founded Gauss Consulting Services and in February 2006, he joined FGM, Incorporated as the company's President.

We will also hear testimony from Major General Howard. General Howard is the Acting Assistant Secretary for Information and Technology and Acting Chief Information Officer at the Department of Veterans Affairs.

We will also hear from Mr. Brandewie who currently serves as the Director, Defense Manpower Data Center, Field Activity, reporting to the Office of the Secretary of Defense, Personnel and Readiness. He is responsible for the oversight of the largest and most comprehensive automated personal database in DoD, management of a dozen major operational DoD programs, and supervision of a multi- disciplinary staff of approximately 800.

Recently he led the DMDC efforts to redesign the Department's medical benefits and entitlements database for the new TRICARE system, to design and field a comprehensive web authentication capability for the Department of Defense, to develop and field an identification card and biometric- based force protection system now widely deployed throughout the world, and to design and develop and field the common access smart card as the new DoD identification card. Currently more than ten million have been issued.

Pronounce it Bresson?

MR. BRESSON. It is actually Bresson.

THE CHAIRMAN. Bresson. Jim Bresson is the Vice President of Gartner Consulting where he was the managing partner for U.S. Department of Veterans Affairs within Gartner's USA Federal Consulting Practice. He is based in Arlington, Virginia, and his responsibilities for Gartner Consulting involve business development, associate development, and engagement and delivery.

We look forward to your testimony, and we will start with you Dr. Admiral Gauss. Which do you want, Dr. Admiral, Secretary?

ADMIRAL GAUSS. John is fine, sir.

THE CHAIRMAN. All right, John. Proceed.

Do all of you have written testimony?

ADMIRAL GAUSS. Yes, sir.

THE CHAIRMAN. All of you do, even—Mr. McFarland, do you not?

MR. MCFARLAND. No.

THE CHAIRMAN. So Mr. Brandewie, Dr. Gauss, Major General Howard, and Mr. Bresson, all of you have written testimony. It will be submitted for the record. Hearing no objection, so ordered.

You are now recognized, John.

STATEMENTS OF HON. JOHN A. GAUSS, PRESIDENT AND CHIEF OPERATING OFFICER, FGM, INC., (FORMER ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND FORMER CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS); HON. ROBERT MCFARLAND (FORMER ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND FORMER CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS); MG ROBERT T. HOWARD (RET.), SENIOR ADVISOR TO THE DEPUTY SECRETARY SUPERVISOR, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ROBERT J. BRANDEWIE, DIRECTOR, DEFENSE MANPOWER DATA CENTER; JIM BRESSON, VICE PRESIDENT AND MANAGING PARTNER, GARTNER CONSULTING; ACCOMPANIED BY JOE CLARKE, DIRECTOR, GARTNER CONSULTING

STATEMENT OF HON. JOHN A. GAUSS

ADMIRAL GAUSS. Thank you, Mr. Chairman. Good morning to members of the Committee. Thank you for inviting me here today to discuss the important issues related to the Department of Veterans Affairs' information technology reorganization efforts.

I would like to provide the Committee with some background information to help in understanding the thought process that goes into the remarks that follow.

At the time of my confirmation hearing as the VA's Chief Information Officer, the Department was faced with many challenges, including an ever-expanding IT budget, programs that were defined in a stovepipe manner due to the lack of an enterprise architecture, programs that were consistently overrunning budget, behind schedule, failing to meet their performance parameters.

The Department was faced with implementing a comprehensive cyber security program and having to implement an executive oversight process which was a recurring deficiency in many GAO audits.

As a result of the above and as presented in my opening statement before the Senate Veterans' Affairs Committee on 2 August 2001, during my confirmation hearing, I stated that I had five strategic objections:

First, complete the enterprise architecture road map for the future;

Two, integrate the disparate telecommunications networks to improve performance and responsiveness for our veterans;

Three, implement a strong information security program and infrastructure;

Four, create a program and project management process to oversee and help information technology program managers deliver products that meet requirements, are delivered on time, and stay within budget;

And, finally, establish information technology metrics to continuously measure our ability to meet our veterans' needs.

Although implementing a strong information security program is listed as number three in the above list, it was my number one priority. Establishing a comprehensive enterprise architecture and integrating the telecommunications networks will place higher in the order since I believe they are prerequisites to attacking the cyber security problem.

During my 32 years in the Navy, I learned to address organizational issues by using the following simple thought process:

First, define the problem to be solved;

Second, define the optimal yet affordable solution to the problem;

Three, define what work should be accomplished by government and what work should be performed by industry and then organize to implement.

Given the problems and strategic objectives defined above, I concluded three things:

First, all IT programs and IT related activities affecting the three administrations and the central office should be centrally managed at the Department level with funding located in the departments and not the administration's budgets, specifically enterprise architecture, cyber security, telecommunications networks, corporate data centers, any program with the above characteristic that would result from

developing a comprehensive enterprise architecture such as VA-wide registration and eligibility and a central call center, and, finally, all IT programs under the auspices of any VA central office code;

Second, all development activities related to individual administration of IT programs should be managed at the Department level and funded from the Administration budget because they are the ones who have the business requirement for the program;

And, third, the operations and maintenance of in- service IT systems directly related to mission execution within an Administration should be managed by that Administration subject to a comprehensive budget and funding execution approval process with ultimate authority for approving the expenditure of funds residing in the Office of the CIO.

I recognize that the above conclusions are not consistent with current thinking, but I would respectfully ask the Committee to consider the following:

Without a central management of the development activities, how will the Department ever implement a comprehensive, enterprise-wide enterprise architecture to eliminate duplication, to cross-functionally integrate the business processes, and ultimately slow or stop the growth of the Department's IT budget?

I hope this information will help the Committee in its deliberations. Thank you for the opportunity. I stand ready to answer questions.

THE CHAIRMAN. Thank you very much.

Mr. McFarland, you are now recognized.

[The statement of Hon. John A. Gauss appears on p. 59]

STATEMENT OF ROBERT MCFARLAND

MR. MCFARLAND. Thank you, Mr. Chairman.

Although I have no prepared statement, I have had the privilege to appear before this Committee on many occasions over the last two plus years. Our discussions have always been frank, and I have appreciated this Committee's support in my previous efforts to bring the VA's information and technology infrastructure into the 21st century.

I am honored to be here today and would be pleased to answer any questions this Committee may have regarding my experiences while Assistant Secretary and CIO at the Department.

THE CHAIRMAN. You sound like a man that has been at a trout stream.

MR. FILNER. Explain it to us city guys.

THE CHAIRMAN. Explain it to a city guy?

MR. FILNER. Yeah.

THE CHAIRMAN. Well, you know, he worked at the Department for a long time. He took a break. He got jammed while he was there for

a while. He went to a trout stream to gather his mind, and we have pulled him back to Washington, D.C. He is not too excited about being back in Washington, D.C. And he says I will show up, but that does not mean I have to give a statement. And if you want to ask any questions of me, go right ahead.

MR. FILNER. Thank you, sir.

THE CHAIRMAN. So that sounds like a man with a clear mind that has been to a trout stream.

MR. FILNER. All right. Now I get it. Thank you.

THE CHAIRMAN. You got it?

Is that about right, Mr. McFarland?

MR. MCFARLAND. That is pretty close, sir.

THE CHAIRMAN. All right. Thank you.

General Howard, you are now recognized.

STATEMENT OF ROBERT HOWARD

GENERAL HOWARD. Mr. Chairman and members of the Committee, good morning. Thank you for your invitation to discuss the Department of Veterans Affairs' information and technology reorganization plan and the recent data loss incident.

First a short update on the VA IT realignment. The VA IT system model has been developed and approved. The key focus is to transition the IT community to operate within a management system that separates the development and operations and maintenance domains.

VA will establish required business practices and processes that harmonize the oversight and budgetary responsibilities of the Office of the CIO, the functionality of the domains, and business relationships of the IT service provider and the customer for all IT activities across the entire VA.

As background, in an executive decision memo dated October 19th, 2005, the Secretary of the Department of Veterans Affairs approved the concept of a new IT management system for the VA. This decision to move to a new management construct was made to correct long-standing deficiencies in the current decentralized IT management system.

The concept separates the IT community into two domains, an operations and maintenance domain that is the responsibility of the Assistant Secretary for Information and Technology and a smaller application development domain that is the responsibility of the administrations and staff offices. Although the domains are separated, the VA CIO will retain oversight responsibilities for all VA IT projects.

As Secretary Nicholson testified at the House Appropriations Committee hearing yesterday, the long-range plan is to also centralize the

application development domain under the CIO.

The new VA IT management system will clearly enhance the Department's ability to strengthen the protection of sensitive information. With all information security officers reporting to the CIO under this new management system, the CIO will be able to:

One, create and operate the agency-wide information security program;

Two, establish information security policies and procedures and control techniques for the agency which when followed will ensure compliance with all of the above requirements;

Three, to train and oversee personnel with significant responsibilities for information security;

And, finally, assist senior agency officials concerning their information security responsibilities including the analysis process.

The VA IT system model was developed as a framework for the future IT management system. The principal elements of the model include the following:

Definitions of the roles, responsibilities, and initial boundaries between the operations and maintenance domain and the application development domain. And this includes determination of business needs and priorities.

Although the domains are separated, the model prescribes procedures between the domains in order to provide the CIO with oversight and budget responsibilities for all VA IT projects. It also provides the authority, delegation of authority, and governance structure and process for the conduct of all VA IT related business.

The model also contains key IT service delivery business process flows and sample scenarios to illustrate how domain activities are coordinated by these process flows. These flows must be clearly defined to reflect the critical interdependence of business applications and the performance of the IT infrastructure.

Finally, the model contains a recommended "to be" organization for the Office of the CIO designed to balance the tactical needs of operating a complex infrastructure as a shared service with the strategic needs of aligning IT resources to best meet the mission requirements of the Department.

Transitioning now to the recent data loss incident, as you are aware, the Secretary initiated several recent actions to tighten our privacy and data security programs.

On May 24th, the Data Security Assessment and Strengthening of Control Program was established to provide a high priority, and much more focused effort to strengthen our data privacy and security procedures.

The two principal objectives of this program are to first reduce the risk of a reoccurrence of incidents such as the recent data loss and second to remedy the material weakness reported by the Inspector

General.

There are three phases to this effort: Assessment, strengthening of controls, and enforcement. We are almost through the assessment phase and have actions underway in the other two phases as well.

On May 26th, the Secretary issues a directive that requires the top leadership to instruct all VA managers, supervisors, and team leaders of their duty and responsibility to protect sensitive and confidential information.

In this memo, the Secretary also announced that he had convened a task force of VA senior leaders to review all aspects of information security and make recommendations to strengthen our protection of sensitive information.

One of the first tasks of this group is to complete an inventory of all positions requiring access to sensitive VA data and to complete that by the end of June.

This past Monday, we began a Security Awareness Week at all VA facilities. We are emphasizing training and privacy and cyber security for all employees. We require all VA employees, contractors, and volunteers to complete both cyber security and privacy training annually.

Normally employees are required to complete this training by September 30th of each year. However, given the recent incident, the Secretary has directed that this be accomplished by the end of June.

We will be conducting a department-wide inventory of laptops to ensure that they carry the encryption and other cyber security software necessary to ensure remote access users are operating in a safe and secure environment. This effort is on hold, however, due to several class action lawsuits. It will continue once legal clearance is obtained.

Finally we are reviewing all policies, directives, and handbooks related to privacy, cyber security, and records management to ensure they are accurate, clear, and focused. All of these efforts will provide for a more secure environment for sensitive data used in the VA.

Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.

THE CHAIRMAN. Thank you very much.

Mr. Brandewie, you are now recognized.

[The statement of Hon. Robert Howard appears on p. 61]

STATEMENT OF ROBERT BRANDEWIE

MR. BRANDEWIE. Mr. Chairman and members of the Committee, thank you for the opportunity to appear before you today to discuss the data exchanges between the Department of Defense and the Department of Veterans Affairs.

Our center is a central repository of automated human resource

information in the Department of Defense, and we have been actively engaged with the DVA on most of the personnel information flowing between the two departments. These exchanges are very basic to providing an improved experience for the veteran and also for coordination of benefits between the two departments.

It is important to note that these exchanges have been ongoing for more than 25 years. The purpose of the data exchanges between DVA and DoD are twofold: To provide information to the DVA on currently serving and recently separated individuals who are eligible for DVA benefits and services, and to competently administer programs in both agencies that benefit servicemembers, former servicemembers, and their families.

These data exchanges can be categorized as follows: Data for administering educational benefits, active duty and selected Reserve, Montgomery GI Bill; data for administering insurance programs, specifically veterans group life insurance; data for epidemiological studies and for assessing post-war illness; data for coordination of benefits and prevention of fraud, waste, and abuse; and data to estimate veteran population and expedite delivery of benefits.

Data exchanges with the VA, although long-standing, have expanded in breadth in recent years. And an effort to consolidate the exchanges began in earnest about three years ago. Close cooperation and increased exchanges of information have also received encouragement from the Congress and the Administration.

For example, the President's management agenda directed efforts to make the transition from DoD to the DVA seamless, and I quote, `` Transition should be seamless from the veterans' perspective and could be made seamless through data sharing between VA and DoD as well as within VA."

Public Law 108-136 established an interagency Committee known as the DVA DoD Joint Executive Council to direct joint coordination and data sharing efforts between the two departments. DoD believes there is great value to current servicemembers and veterans in the close cooperation evidenced by these data exchanges that has developed between DoD and the Department of Veterans Affairs. However, it is equally important that the exchanges are done with utmost attention to security to ensure no unauthorized disclosure of information.

The DVA has been a partner with us in the implementation of secure transfer between the two agencies. In that regard, we have continued to improve that process and add security to this data transfer process.

My organization did the work to assess the impact of the recent data breach on currently serving active duty, Reserve, and Guard members. We continue to work on mitigation efforts with respect to the compromised information.

In spite of this tragic loss, it is important to reinforce the point there are many benefits to current data exchanges between the two departments. They are done securely and they result in better service and better benefit delivery for servicemembers and veterans.

Mr. Chairman, I thank the Committee for the opportunity to report on data exchanges between DoD and DVA and would welcome the opportunity to answer any questions.

THE CHAIRMAN. Thank you very much.

[The statement of Robert Brandewie appears on p. 67]

THE CHAIRMAN. We have another vote, just one vote. It is a procedural vote. So we are going to have to stand in recess for about seven minutes, and we will return.

[Recess.]

THE CHAIRMAN. All right. The hearing will come back to order.

The Chair now recognizes Mr. Bresson for his statement.

STATEMENT OF JIM BRESSON

MR. BRESSON. Mr. Chairman, Mr. Vice Chairman, and members of the Committee, I appreciate the opportunity to participate in today's hearing regarding the Department of Veterans Affairs' information technology reorganization plan and VA's decision to pursue the federated model.

I am a managing partner within the consulting division at Gartner, the leading provider of research and analysis in the global IT industry. I am accompanied today by my colleague, Joe Clarke, Director with Gartner Consulting, who is the lead subject matter expert in the methodologies we employed in our most recent consulting engagement for the VA.

Unlike many of our competitors, Gartner does not offer IT systems or software implementation services that would compromise our independence and objectivity. It is our objectivity combined with our past performance at the VA that was the basis for Gartner Consulting being selected to convert our originally recommended centralized model to a federated model at VA leadership's direction. I was the lead consultant for this effort.

In December 2005, the Assistant Secretary for IT directed Gartner Consulting to determine the best approach to implement a federated model for VA. Our focus was on ensuring that the VA's federated model would yield a blueprint for implementation that incorporated the seven critical dimensions to achieving a higher performing IT organization at the VA. Those seven dimensions are:

One, organizational structure, the structure in which the IT organization delivers value at a risk level that is tolerable to the Department and best supports its one VA mission;

Two, processes, the critical IT processes, their interfaces, and their dependencies required for IT delivery across the Department;

Three, roles, the IT management practices, responsibilities, and accountabilities required for IT delivery, what VA associates need to do to deliver IT value;

Four, IT services, the necessary IT capabilities that are valued and readily understood by the VA's business community, not just the IT community;

Five, guiding principles, the IT policies that establish focus, governance, and the decision-making fabric within and between VA's IT and business communities;

Six, performance management, the definition of IT performance objectives and success criteria and high-level analysis of IT performance relative to peers in government, insurance, and healthcare delivery;

Seven, culture and norms, the changes required in the underlying culture and norms to effect improved IT management behaviors.

In my written testimony, I have provided details about how Gartner Consulting derived roles and responsibilities and simulated scenarios to illustrate for VA's consideration how the federated approach would work within VA's environment.

It is important to note as we have in our intermittent engagements with the VA that organizational structure alone is not the silver bullet. It is just one dimension of necessary change to the existing IT organization at VA.

There is a tendency for government agencies to want to jump straight to organizational structure alone when seeking to initiate and drive change. Encouraging desirable IT management behavior is less about structure and is more about relentless focus on strategy and execution.

Gartner research and our engagement results indicate that the VA must allow for a balance between line of business autonomy and common enterprise-wide needs. VA's desired end state is not small change. It will require overt, firm, sustained action and persistent messaging supportive of the change from all levels of leadership across the Department.

What will be critical is sustaining the focus of executive leadership in seeing this change through and realizing improved IT performance. Whether VA leadership will achieve the desired end state in an expeditious manner may be less important than whether they are able to successfully institutionalize the federated IT management system.

I firmly believe that VA leadership is taking the right steps forward.

Mr. Chairman, Mr. Vice President, and members of the Committee, 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 Committee may have at this time.

[The statement of Jim Bresson appears on p. 73]

THE CHAIRMAN. Well, I would like to pick up right where you left off. I firmly believe the VA is now taking the right steps. You have to reconcile that. You have to reconcile that with the testimony that Gartner Consulting gave to this Committee and your recommendation for a centralized model that was stiff-armed by the VA.

You are a consultant to the VA; are you not?

MR. BRESSON. We have been a consultant on occasion to the VA. We are—

THE CHAIRMAN. Are you a consultant to the VA right now?

MR. BRESSON. We are currently not under engagement with the VA.

THE CHAIRMAN. Okay. And were you hired in as a consultant to the VA with regard to the federated approach and its implementation?

MR. BRESSON. Yes, we were.

THE CHAIRMAN. Do you anticipate future work with the VA?

MR. BRESSON. I would like to anticipate future work with the VA, yes, sir.

THE CHAIRMAN. And would your future anticipation to work with the VA have anything to do with your last statement before this Committee?

MR. BRESSON. Not at all, sir. Not at all.

THE CHAIRMAN. Then reconcile your testimony, sir.

MR. BRESSON. Okay. I believe, as I said earlier, that organizational structure is one dimension. The work that we did in converting the model that was recommended last spring, 2005 that is, to the federated model dove down deep into processes, roles, services, principles, performance management, and culture and norms.

And in constructing that model, we identified for the VA what path forward they should take in order to make this adhere in their environment. And I believe that from that model they are stepping toward that direction heeding what we advised them to do.

THE CHAIRMAN. Does Gartner Consulting as a company still stand by its recommendation to the United States Congress that the VA centralize, have a centralized model for IT management?

MR. BRESSON. We do stand by that, sir.

THE CHAIRMAN. In your written testimony to the Committee, I note that you have a quote in here, `` Given the poor state of the VA's IT investment management process and the stated demand to drive benefits over a shorter horizon, we recommended the centralization option to maximize the opportunity to create value for our veterans."

You stand by that statement today?

MR. BRESSON. Yes, we do, sir.

THE CHAIRMAN. Okay. Now, Gartner has given this statement, calls it, `` The poor state of VA's IT investment management."

Well, now I am going to turn to Dr. Gauss and Mr. McFarland. Can you explain to me why Gartner Consulting would call it a poor state of investment management when, in fact, both of you were the managers?

ADMIRAL GAUSS. Mr. Chairman, I really have no idea why that finding was uncovered. I can speak to the time between July of 2001 and June of 2003.

When I first became CIO, our capital investment control process for IT was poor. And with a focused effort and working with the Office of Management and Budget, within one year, we turned around our process from a budget submission to OMB of about a five percent first pass acceptance to about a 95 percent first pass acceptance.

And after I departed VA, there was a substantial gap before Mr. McFarland became CIO. And during that interval, I know I do not know what went on at VA and I am not sure whether Mr. McFarland does.

THE CHAIRMAN. Mr. McFarland, what are your thoughts with regard to that statement?

MR. MCFARLAND. Sir, I believe that we continued the enterprise information board environment that Dr. Gauss started which was to review the individual development projects and sustainment projects. But our biggest issue was not making the decisions over which investments were good investments, although where I came from, we dealt with ROI, which is a difficult thing to do in the government because it is not the same as it is in the private sector.

But what we had a problem with was the use of the funds, and this, as you know, is something I was focused on for quite a while, which was to change the budget environment.

So when you use the words poor state of investment management, I think what Gartner was trying to say is that you may pass at an executive level a project spin plan and a project budget, and then the dissemination of that money and the use of that money in many cases which is not being able to be tracked and followed through the chain as it is used out in the field.

And I think that to me was the area where I felt the investment management process was failing, in the budget itself and the expense of the money, because we were never sure that the money was spent on exactly what it had been appropriated for. And to me, that, I think, is what Gartner was trying to say when they said part of the issue of poor investment management process.

THE CHAIRMAN. To Mr. Bresson, I want you to know that we recognize that a movement to cure is more than just about structure. We recognize that. But we also have painfully recognized over the years,

and we have embraced the testimony that Gartner had given to this Committee and the counsel that they gave to the VA prior to their judgment on which option to choose.

The reason we do focus on structure and lines of authority is that as we do the forensics here of trying to put this together in understanding what went wrong, we cannot move to cure until we create the right structure with the proper lines of authority so that we know who has authority to do what, who has the tools to do what.

And so that is kind of why we are focusing on those kinds of things at the moment. We recognize culture and many other things that you also had testified to.

The ROI mentality, Mr. McFarland, that you brought to the VA, we have no objections to that at all because we are looking out at the interest of taxpayers, had to deal with the pains that you did with regard to the core FLS and the vets net.

And there is a reason that we here in Congress wanted the development side under your gentlemen's authorities. And we understand that they fight against that, and we recognize that there are crucibles out there for initiative and that your job is not to say no to that, but just to make sure that it is all compliant under the one architecture.

Gentlemen, we are considering many things in our packages. So what I would like to do here today, we want to do some forensics, we want your opinion on cure. What are your thoughts that if we were to, in our package we are to elevate the position of the CIO to an Under Secretary?

Mr. McFarland?

MR. MCFARLAND. I would think that would be a good move, sir. I believe that in this day and age, the VA like any other agency simply cannot do business for its veterans without an IT infrastructure.

THE CHAIRMAN. And then if we make the CISO a Deputy Secretary right under the CIO as an Under Secretary?

MR. MCFARLAND. You mean an Assistant Secretary, sir?

THE CHAIRMAN. Assistant Secretary, yes.

MR. MCFARLAND. I certainly would applaud those moves because I think that the infrastructure that runs the VA today in its current state is an IT infrastructure and it is important enough that given the past history that those moves would certainly help. It would give the CIO an equal seat at the table with the main administrations to be able to provide the service that keeps the business running.

THE CHAIRMAN. Admiral Gauss?

ADMIRAL GAUSS. Mr. Chairman, I think your idea is an excellent one. And if I may, I have been associated in management positions in the last 14 years of government service where I have had the opportunity to observe how Chief Information Officers can be effective not only at the Department of Veterans Affairs but in other parts of government as well.

Without the Chief Information Officer being elevated to the status of Under Secretary or Under Secretary equivalent, the CIO does not have a seat at the table at any department within government, and the founders or the people who created the Clinger-Cohen Act will continue to be disappointed in results until such a bold action is taken.

I would highly endorse your suggestion, sir.

THE CHAIRMAN. Thank you.

Mr. Filner.

MR. FILNER. Thank you, Mr. Chairman. Thank you for putting together this panel. I learned a lot today.

Mr. Chairman, you said you cannot move to a cure unless certain steps were taken, and I would include in those steps at least a recognition of the problem and get out of a sense of denial.

Every time Mr. Howard referred to what happened on May 3rd, the incident. I do not know if you have been out in the field talking to veterans, but they are scared to death. You got 26 million or more people worried about identity theft.

We have had testimony here that if it was a professional has the data, and there are some circumstances about the theft that may lead to that conclusion, it may be a year before they even know that their identity has been stolen.

So we have a major disaster here. And until you guys start calling it that, I do not think we are going to get the kind of response that we need.

So I hope you folks in the front row there will take that message back to the Secretary, that if he is in a state of denial still, although, I do not know, it took a week to hear the other news, maybe he will not get this message by tomorrow.

Dr. Gauss, you started, your opening sentence was quite an indictment of this situation. Could you just read that for me again or did you have that written out?

ADMIRAL GAUSS. Yes, sir. At the time of my confirmation hearing—

MR. FILNER. No, no. Before that. I think it was the first sentence. You outlined the situation as you saw what was—

ADMIRAL GAUSS. Yes, sir. That was at the time of my confirmation—

MR. FILNER. Oh, okay.

ADMIRAL GAUSS. —the Department was faced with—

MR. FILNER. Okay. Right.

ADMIRAL GAUSS. —an ever-expanding IT budget, programs that were defined in a stovepipe manner due to the lack of an enterprise architecture, programs that were consistently overrunning budget, behind schedule, and failing to meet their performance requirements, was faced with implementing a comprehensive cyber security pro-

gram, and having to institute executive-level oversight process as a result of a recurring theme of GAO reports.

MR. FILNER. I mean, I would like to ask a very generalized set of questions that maybe several of you can respond to. I mean, that is a cultural indictment, and I would like to know if it still exists as you see it, Mr. McFarland? Has it changed? Why hasn't it changed? What did you think of the polyanna statement by Mr. Howard, everything has changed and we are moving forward?

And I might just for Dr. Gauss, I was not at the hearing, but I think at one hearing where Chairman Buyer said to you, would you like to have centralized line control of the system, and I guess you had to say no at that time. I do not know if that was your personal opinion or OMB's opinion because I think they had to approve your statements here.

But if you can go back from that statement, and has anything changed since you have left? Does Mr. Howard's statement sound right to you? I mean, and what needs to be changed for it to come true? Please, and then Mr. McFarland if he can. Get him off the trout stream there.

ADMIRAL GAUSS. Let us see. I am really not qualified to discuss what has happened recently because my knowledge of what has happened is what I have read in the newspaper and in preparing for this hearing, material that I found on the VA web site.

MR. FILNER. But you were there for a couple years.

ADMIRAL GAUSS. Yes, sir.

MR. FILNER. So did it change while you were there?

ADMIRAL GAUSS. During that time—

MR. FILNER. You mentioned one major thing.

ADMIRAL GAUSS. For the record, sir, all of the testimony that I gave in front of this Committee was my testimony. It was the truth. I was not influenced by OMB or my senior—

MR. FILNER. They did not have to be approved?

ADMIRAL GAUSS. I am sure it had to be approved, but I held no punches and I spoke my views.

MR. FILNER. We did have testimony at an earlier hearing of one of, I think, your successors, Mr. Brody, right, who said, because I asked him, he said that he could not say what he wanted to say because it was approved by OMB. So that seemed to be the procedure.

ADMIRAL GAUSS. I stand by today—

MR. FILNER. Okay. Thank you.

ADMIRAL GAUSS. —the testimony that I gave in front of the Subcommittee at the hearings for which I participated.

Now, from a cultural perspective—

MR. FILNER. Did I get that right that you said no to Mr. Buyer when he said would you like to have the centralized control?

ADMIRAL GAUSS. I believe that in my answer, I qualified it along the

terms of what I had in my opening statement, that I felt that the development activity should be centralized. The CIOs should have the authority over all development activities, but that the operations and maintenance of the products that were deployed to the field should still be distributed within the administrations.

And a little bit of the background, we are all an invention of our past. And having served for 32 years in the Navy, I look at the model that is proposed today and it equates to allowing commanding officers to develop their command and control capability, but, yet, to operate it, maintain it, and fix it, you have to go back to the Pentagon. And somehow that just does not seem right based on my experience.

As far as the culture goes, there were cultural impediments at VA that precluded making progress while I was there. Specifically at the executive level, there was commitment to have reform, but there was not commitment to effect the type of change necessary to make that reform.

When you find you are broke, the processes and procedures you operate under are not going to fix you because if they would, you would not be broke in the first place. So change was fundamental, but the attitude was fix it within the current process.

Second, the VA concurrence process is onerous. In my testimony in September of 2002, I talked about a memo the Secretary had signed in August directing the centralization of IT activities. I testified in front of the Subcommittee that we put a team together to build a plan and it would go to the Secretary by November of 2002. That did not happen. It took until May to get it done because the VA concurrence process waters everything down to the lowest common denominator in which people can agree.

I was told one time I could not offer a differing view because nothing goes to the Secretary without the principals concurring.

And, three, the financial management of the programs, the money is distributed into the Administration budget, at least it was during the two years I was there, for such things as enterprise architecture, cyber security, the data networks, all of the infrastructure things needed to run, the machinery needed to run the IT at the Department and for the administrations, and it was left to my office to have to get the money from the administrations in the year of execution.

The budgets should reflect the execution because at the end of the day, the real organization follows the flow of the money. And with the money spread in execution, it is very difficult to get the resources one needs to execute the job.

Mr. Filner. Okay. That was pretty clear.

Mr. McFarland, would you concur or do you have anything to add to that?

Mr. McFarland. I do concur with Dr. Gauss on the state of what he left was pretty much what I found when I got there. I believe the

VA has moved forward in doing some things that will make the job easier.

With the help of this Committee and Congress, there is now a consolidated budget, although I would tell you that I was disappointed that the budget contained only nonpay dollars and not the full budget. I will be frank about that. That does allow better oversight over the spend. There is now under this federated model at least a consolidation of the infrastructure.

And where I might disagree with Dr. Gauss a little bit, I do believe that the infrastructure has to be consolidated because I believe that if you do not consolidate the infrastructure under the CIO, then all you will do is be involved with directives and guidelines over policy of privacy and security.

Without control of that infrastructure, technical control of that infrastructure, you cannot ensure that the environment is safe. So I would disagree. I believe the infrastructure should be consolidated and that not only— all those assets need to be under a single control. The—

MR. FILNER. Mr. Howard, are you heading in that direction or not?

General Howard. Sir, with respect to the operations and maintenance domain, we are. And as I indicated in my testimony—

MR. FILNER. Wait, wait. He just said something very clear. He said control of the infrastructure.

GENERAL HOWARD. Yes, sir.

MR. FILNER. Is that what you are talking about or not?

General Howard. With respect to the operations and maintenance infrastructure, that is correct. The data centers—

MR. FILNER. But he was not restricting it like you are. I mean, he did not have any qualification over infrastructure. What other part of the infrastructure there is? Development?

GENERAL HOWARD. Development is not included in the—

MR. FILNER. Why not?

GENERAL HOWARD. —IT organization that has currently been approved.

MR. FILNER. That is the point, Mr. Howard. I am saying should it be in that?

Mr. McFarland, did you include what he said, operations, maintenance, and development in the consolidated structure—

MR. MCFARLAND. Under the current plan—

MR. FILNER. —infrastructure?

MR. MCFARLAND. Under the current plan—

MR. FILNER. I do not even talk the language you do, so I am trying to get this.

MR. MCFARLAND. I understand. Infrastructure to me does not include development. Infrastructure is the basic assets and people necessary to provide the IT service to the community.

In the current federated model, that infrastructure is supposed to be consolidated under the CIO. And the administrations and staff offices become users of that infrastructure. I strongly believe you cannot allow the infrastructure to be managed by administrations and staff offices.

MR. FILNER. So explain to me the differences in federated model and the centralized model. I mean, what—

MR. MCFARLAND. The difference—

MR. FILNER. — is included in one and not the other?

MR. MCFARLAND. The difference under the Gartner scenarios that were developed is only one issue, that the applications development, the development of new products to serve the needs of veterans in each of the administrations and staff offices, whether it be a financial system or whether it be a medical system, the development of those products, application development, is done in the federated model by the administrations. Everything else is managed by the CIO.

In the centralized model, all of that would be managed by the CIO. And what would happen would be the staff offices and the administrations would provide the specifications and requirements for their needs to the CIO who would then go to the marketplace and develop those products for them.

MR. FILNER. And you agree that that is okay?

MR. MCFARLAND. I am sorry, sir.

MR. FILNER. We got word directly from the Secretary about what Mr. Howard should say, so maybe you should read the note for us, Mr. Howard.

THE CHAIRMAN. Mr. McFarland, to be responsive to the question, I think it would be that do you concur with the centralized model that development should be under authorities of the CIO? I think that is where Mr. Filner was getting to.

MR. MCFARLAND. I have been on record from day one as being preferring the centralized model. I have agreed to support the federated model when I was in office because that was the recommendation of the agency and it was candidly the best I could get.

MR. FILNER. And give me again as concise as you can why— you defined the federated—you gave us a clear explanation, but why would you prefer the centralized? I mean, what did it do that the other did not?

MR. MCFARLAND. I believe you have to have control over development.

MR. FILNER. Well, that is what I asked you at the beginning, and you said no. I asked what did consolidation of infrastructure mean, and you said operation, maintenance, but not development. Now you are saying development should be.

MR. MCFARLAND. Let me define infrastructure for you, sir.

MR. FILNER. Okay.

MR. MCFARLAND. Infrastructure is the assets and people that provide IT services—

MR. FILNER. Okay.

Mr. McFarland. —provide the electrons to anyone who uses those electrons, your e-mail, your whatever, no matter whether you are a doctor, a benefits coordinator, whatever, the users of those workstations. That is the infrastructure.

The development of product is actually the generation of new code—

MR. FILNER. All right.

MR. MCFARLAND. —to run applications.

MR. FILNER. And both should be under the CIO in your preference?

MR. MCFARLAND. It has been my professional—

MR. FILNER. Okay.

MR. MCFARLAND. —opinion that they should be consolidated—

MR. FILNER. Okay.

MR. MCFARLAND. —under one environment.

MR. FILNER. And so they are going in a different direction than that right now?

MR. MCFARLAND. They are using—

MR. FILNER. All right. That is all.

MR. MCFARLAND. —the federated model, yes.

MR. FILNER. Thank you.

Thank you, sir.

THE CHAIRMAN. Mr. Bilirakis, just as a follow-up, if I may.

Mr. Bresson, Gartner Consulting, you are consulting to the leading top 100 companies in the world; are you not?

MR. BRESSON. Yes, sir.

THE CHAIRMAN. Are there any of these companies that you are a consultant to in the world of these companies ever take the development side outside the—to take the development outside the authority of the CIO?

MR. BRESSON. Indeed there are, yes, sir. And I think one of the nuances to the federated model as it may exist in commercial and outside of public sector is that while development may remain outside the CIO's control, in order for those products to run on the infrastructure, they still must, you know, pass through the wickets and be certified to run on that infrastructure. So there is a transfer.

THE CHAIRMAN. Thank you.

Mr. Bilirakis.

MR. BILIRAKIS. Mr. Chairman, virtually everything has kind of been covered on a detailed basis. If this continues on, it is just going to continue to make work for us and take us away from being concerned about healthcare and about claims processing and things of this nature. Somewhere along the line, it has got to be solved.

Let me ask. My impression is that all testimony, I mean, for—it goes all the way back, not just this Administration, the prior Administration and Administration before that. All testimony before coming before Congress has to go to OMB; is that correct? Does anybody know? That is true, right?

GENERAL HOWARD. [Nods head affirmatively.]

MR. MCFARLAND. [Nods head affirmatively.]

MR. BILIRAKIS. Okay. So this is not something that is new.

Dr. Gauss, you prepared your testimony. Of course, obviously, OMB does not tell you what to respond to when you are asked questions from the panel up here. But you prepared your testimony for today, and then there is a process? It went up the line, did it, up through the—

ADMIRAL GAUSS. [Shakes head negatively.]

MR. BILIRAKIS. No? Where does your testimony go?

ADMIRAL GAUSS. As a private citizen—

MR. BILIRAKIS. You are a private citizen, right. All right. I am going to go to General Howard. Forgive me for doing this. Getting a good opportunity for this old Staff Sergeant to talk to a Major General.

GENERAL HOWARD. It has to go through OMB, sir.

MR. BILIRAKIS. Has to go. All right. But does it go up the line through the VA first—

GENERAL HOWARD. Yes, sir.

MR. BILIRAKIS. —before it goes to OMB?

GENERAL HOWARD. Yes, sir, it does. General Counsel- -

MR. BILIRAKIS. Do you like that as a former General officer?

GENERAL HOWARD. Sir, it was probably the same way in the Pentagon, although I cannot remember.

MR. BILIRAKIS. Yeah, I will bet. I will bet.

GENERAL HOWARD. But that is the process.

MR. BILIRAKIS. You know, what is happening here is, you know, we have got a Veterans Administration that I have always had very high regard for. When I came to Congress 24 years ago, there was one committee that I specifically fought for. I guess I did not have to fight too very hard, but the point is I wanted to get a VA Committee, and I did 24 years ago, first day one.

And Mr. Buyer may not know this, but when our side came up with this idea of grading committees, certain committees are considered A committees, B committees, C committees. The rule was that if you had an A committee, you could not serve on any other committee. And the Veterans Committee was considered other than an A committee.

And so Energy and Commerce was considered and still is considered an A committee. And the deal was if you wanted to stay on an A committee, you had to give up any other committees.

I let it be known that I would be glad to give up Energy and Com-

merce if I could keep Veterans Committee. That is how much I feel about this Committee and that is why I get awfully frustrated and angry sometimes when we get partisan here and throw stones at each other, which is something we did not used to do on this Committee. But that is besides the point.

The point here is that activity like this, promises made to Congress on record and whatnot and not kept on what, you know, contract on IT was to be awarded June the 10th and contract work was to be started on June the 15th of this year of 2006 when, in fact, that has not taken place, that is the result of testimony before this Committee back in March of this year.

Other things. We have gone through hearing after hearing. We have had round-table discussions, everything on IT, and still do not see very much progress being made. I mean, that hurts the image of the Veterans Administration.

And, you know, we would like to hear from the veterans, complaints about maybe healthcare, about their claims, or something of that nature. And what we are hearing is they are concerned about privacy and the lack of privacy and their concern about what might happen to their personal situation as a result of what has transpired.

Mr. McFarland, you came aboard with a heck of a background, a tremendous IT background. You were given a certain responsibility. Was your background respected in the VA? Now, you should be free to respond here.

MR. MCFARLAND. Yes, sir. I never got a feeling that my background was not respected. I think I felt I brought a business acumen to the VA—

MR. BILIRAKIS. Yeah.

MR. MCFARLAND. —which I think was—

MR. BILIRAKIS. All right. But—

MR. MCFARLAND. —somewhat new, and I think it was respected certainly in the beginning. I am not sure—

MR. BILIRAKIS. In the beginning. What happened—

MR. MCFARLAND. —if it is respected today.

MR. BILIRAKIS. What happened after the beginning?

MR. MCFARLAND. Well, I think whenever you embark on change, you are going to run into culture. I have said many times I did not believe that a majority of the issues at VA were so much about technology as they were about culture.

MR. BILIRAKIS. Yeah.

MR. MCFARLAND. It is a long-standing history of decentralized management. And when you bring a business acumen that says you want to centralize many of those management functions, I think you run into cultural problems.

But that being said, I do not think anyone disrespected my background. I never had—

MR. BILIRAKIS. Well—

MR. MCFARLAND. —anybody chastise me for it, so—

MR. BILIRAKIS. Yeah. I do not think anybody would have done that, but I am not referring to that obviously. I am referring to— I mean, were you paid attention to? Were you taken seriously in terms of some of the changes as a result of your actual background and experience and that sort of thing?

MR. MCFARLAND. Oh, I think I was taken very seriously, sir, on many occasions. I do not think it was ever an issue of taking me seriously. It was that the problem was the disagreement over the change.

MR. BILIRAKIS. All right. So you were taken seriously, but there were disagreements? Some people disagreed with you?

MR. MCFARLAND. Yeah.

MR. BILIRAKIS. General Howard, you know, here we are. And the Chairman's idea of legislation, basically upgrading the CIO position and whatnot is a good idea. But here we are trying to micro manage. And damn it, we should not be doing that. And, yet, we feel that we almost have to from the questions that have been asked here, detailed-type questions for crying out loud.

We should not have to be concerned with something like that, I do not think. And, yet, we are because we see a process that just is not moving. It is not progressing the way it should be. And then, of course, these errors such as the loss of those files.

General Howard, your testimony had to be cleared, but your responses to us are not cleared, do not have to be cleared.

GENERAL HOWARD. No, sir. That is correct.

MR. BILIRAKIS. All right. Now, you are a General Officer. Are we going to fix this?

I mean, Mr. McFarland mentioned the word culture. He knew darn well that I was going to mention culture because I talked about it constantly during our past hearings. There is a culture there. There is a turf thing there that exists up here, too, and I am the first one to admit that. If I had to say the one thing that bothers me about the Congress is the turf, turf fighting, and committees' jurisdictions and things of that nature.

What do you think? Are we on the right path here? Are we going to fix this? Are we going to be as proud of the VA in terms of IT as we are on our work on healthcare and the Spinal Cord Injury Center, for instance, Haiti Hospital in Tampa?

There was a young lady here with Pfizer who lives down in that area and who volunteers there one day a week. And as I went out to vote, she was boasting to me about the great work that they do.

I mean, there is a lot of pride there. But the pride does not exist as far as IT is concerned. Respond to that.

GENERAL HOWARD. Sir, there is, first of all, no question that this can

be fixed. Obviously we cannot predict the future. But in my mind—

MR. BILIRAKIS. What do you mean by that?

GENERAL HOWARD. You said will we fix it. We can fix it and we are heading in the right direction. There is no question about that.

The issue regarding centralization is still, you know, full centralization, that is, including the development domain, is still on the table. But I think based on the Secretary's testimony yesterday, that also will be centralized. And he went public with that yesterday during the Appropriations hearing. I think that is a very important aspect of it.

Can we do it right away? My personal opinion is we should not. We are already very deep into moving the operations and maintenance and consolidating that.

In the contract you refer to, you are correct. That was delayed due to contracting procedures, but that is ready to be signed. If it is not signed today, it will be in the next few days to bring in the contractor who is going to help us further refine the details of the current approved IT reorganization. But as the Secretary mentioned yesterday, he is going to take the next step.

MR. BILIRAKIS. All right. You said something, you mentioned contract procedures, delays as a result of the contract procedures. Should those procedures in your opinion be changed?

GENERAL HOWARD. Sir, those are typical government procedures. It just takes time to work through that. I did not see anything really out of line. It just took longer than we thought. I mean, we followed all of the procedures. We had written proposals. We had oral presentations and a thorough review.

The last reviews that had to take place were with General Counsel and the Contracting Office. You know, I got an e-mail this morning that indicated those are complete.

So there is no reason why this contract should not be signed. And that will be a very significant piece to what we are discussing today because they will come in, this contractor will come in and help us refine the processes and procedures under which we should operate.

MR. BILIRAKIS. Are we going to pay attention to them? Are we going to—

GENERAL HOWARD. Sir, we are going to pay a lot of attention to them. And the fact of the matter is, you know, we have already detailed 4,600 people to the Office of Information and Technology. And that detail will become permanent on the 1st of October.

Sir, that is in effect as we would refer to in DoD, that is a field operating agency. That is not a staff section. That is a large number of people, and we are now in the process of organizing them, delivering the guidance, an important subset, for example, of the Information Security Offices that exist throughout the VA. There is slightly over 300 of them. They are now under my control.

You know, we are the ones that issue them instructions, that give them the training, that develop their careers, all of that. Bob McFarland did not have that, but we do. And that alone is very helpful in terms of improving our information security.

MR. BILIRAKIS. Well, I am reminded by staff that this was said something like last October that it was going to take place, and here it is what, June, almost July of the next year.

GENERAL HOWARD. Yes, sir. It happened in April, sir. That is—

MR. BILIRAKIS. In April.

GENERAL HOWARD. That is when the detail took place. But to sort of summarize, I am fully confident that we can fix this problem. Clearly it is an organization issue, but it is more than just moving the boxes around.

As Gartner mentioned, processes are very important and probably more important than anything else is the leadership and the emphasis we place upon the whole enterprise.

MR. BILIRAKIS. Yeah. Just my last question. What say you to this culture thing that has been admitted to over a period of time in the VA?

GENERAL HOWARD. Sir, I have been in the VA just a little over a year. I came out of the private sector. There is a culture issue. And one of the reasons for that, I think we all know that we are operating with an agency that is very decentralized. And you cannot fix that overnight. I mean, that has to be done over time. We need to put more emphasis on it.

But, again, under Dr. Kaiser, it was deliberately decentralized and the result of that, quite frankly, was more effective healthcare. I mean, it was, you know, innovation in the field and all of that. And in many ways, that is a good thing. What we probably did not do is maintain sufficient controls over that decentralization.

Even in the Army, you know, you can encourage innovation and to a degree decentralization, but you have regulations and clear directives to make sure that things are followed correctly.

And one comment on directives. The business about are we going to fix this. Sir, one first step, a major first step is to publish very clear directives. I have only been in OI&T a little over a month and clearly that is a problem. Bob McFarland had difficulty with that.

And no longer guidelines and handbooks and all of that. Our policies need to be in very clear directives with signatures on them so that people are very clear about what they—

MR. BILIRAKIS. Yeah. That seems natural. Why did Mr. McFarland have trouble with it and why do you say that it is going to be difficult? I mean, why?

GENERAL HOWARD. Sir, I do not see that difficulty anymore.

MR. BILIRAKIS. All right. Why was it—

GENERAL HOWARD. It took us less than a week to publish 6504. In

fact, the Deputy Secretary was a co- signature on it along with myself. And 6500 is another very critical directive that we are currently working on.

MR. BILIRAKIS. Yeah.

GENERAL HOWARD. And there are more. We cannot rely on memos and guidance that is not signed out and approved at the very high level.

MR. BILIRAKIS. Will enforcement exist?

GENERAL HOWARD. Sir, on the enforcement part, I mentioned in my testimony that we have established an overarching program to address these issues, the Data Security Assessment and Strengthening of Controls Program. This is an overarching program sanctioned by the Deputy Secretary. We have a very detailed list of actions that must occur. In fact, we would be happy to brief this Committee at any time. There are a lot of things that need to be done.

As I mentioned to you, there were three phases to it. The last phase is enforcement. And to give you an example, I think in the area of enforcement, one of the most important things we can do is improve our audit and inspection capability.

As an old Army guy, if you roll into an organization and you do not have a good inspection program, you got a problem right from the very beginning. And we do not have that right now. We have some. We have the IG, of course.

But within OI&T, for example, it is relatively small. It is nowhere near as robust as it needs to be. And along with that capability needs to be the authority to go anywhere within the VA, knock on the door, and walk in and see what is going on.

Sir, I know you are laughing, but we need that and it needs to be robust. And you know what I am talking about. You are talking about unit inspection programs.

MR. BILIRAKIS. I am not sure why the Chair is laughing. I think because he is happy.

But we had testimony what, last week from the counsel that you did not have the authority, the enforcement authority. Am I wrong there or do you have it? Do you feel that you have it?

GENERAL HOWARD. Sir, right now I have certain authority as a result of the approval of the IT organization up to this point. For example, in the area of information security, I own these people. I am responsible for telling them what to do. I have the authority to discipline them.

What I do not have is the authority to discipline somebody in VHA. I do have the authority to lay out the policies and regulations that must be adhered to. And if the VHA folks, for example, do not discipline someone who violates these policies, you know, then it is a matter for the tenth floor, you know, the Secretary level.

Now, I will say that so basically within what has already happened,

I do have some authority. Now, with respect to additional authority, there is a memo being debated right—not debated. It is being finalized and reviewed by the Secretary, regarding further delegation of authority. It has not been signed yet. He may talk to that tomorrow. But there is more to come on that issue.

MR. BILIRAKIS. Well, I know I have taken much more time than I should have. Thank you, General, gentlemen.

Mr. Chairman, we all have suffered through an awful lot of frustration here. I yield back whatever time.

THE CHAIRMAN. Well, Mr. Bilirakis, this is a challenge. It has been a challenge for us for a long time.

And I am smiling whenever I can hear you talk about authority.

Back in 2002, Ms. Carson asked you, Dr. Gauss, a direct question, are you the man in charge. That is exactly how she asked it. And you said, yes, ma'am, it is me. Very close. You may have been in charge, but you did not have a lot of authority in reality.

And that is what also then we learned with your successor, Mr. McFarland. He was in charge. The Secretary even wrote a directive, and then that is undercut by a General Counsel in his interpretation of FISMA that says that you have responsibility, but you do not have authorities.

General, reflecting upon your days in the United States Army, pretty hard for you to have received responsibility to ensure compliance, but then you have no authority to accomplish a mission. You are to take the hill. You are to ensure compliance of having taken the hill, but you have no authority to give orders to anyone.

That is why I use the form heterodox, because it is totally against everything in our society. So my challenge with the Office of the General Counsel, it is how you get to yes. How do you get to yes?

You do not create these odd anomalies that then has a detrimental impact upon an organization. We figure out how we get to work together and pull in the same direction, not to create these divisions and as someone had earlier testified to as decentralizations of mass dispersions, equate to mass dispersions in the VA.

So that is why I am smiling. I am pleased that the VA is moving toward that direction with regard to lines of authority.

I now recognize Ms. Herseth.

MS. HERSETH. Thank you, Mr. Chairman.

Let me just follow-up on the line of questioning of Mr. Bilirakis and some of the comments that the Chairman just made. And I appreciate the testimony that you have offered, written testimony that I had a chance to review and some of your oral testimony today that in the light of the vote, some of us missed.

But I just want to make sure that we have turned a corner and that we will be able to confirm some of this further with the Secretary tomorrow. But the Chairman says, you know, how do we get to yes.

It is sort of like what we say to members of our staff here in Washington or back home serving constituents. You know, it is one thing to move the ball down the field and get to the five yard line, but they all need to get it over the line. It is not just about getting it close. It is getting it there.

And in the questions that Mr. Bilirakis posed to Mr. McFarland about how you were received given your background, your experience when you arrived at the VA, you felt that, you know, you brought this business acumen, it was respect, but there was disagreement then based on the proposals of centralizing the IT function.

And then in response to the question posed to you, General Howard, about once we get the contractor, are you going to pay attention to them. You said, yes, you are going to pay attention to them.

But what if there is disagreement with how they are advising to refine the processes? Have we turned the corner to say now that the Secretary has made the decision to centralize, we have got the contractor that is going to be in place, are we behind that now? It is not about disagreement anymore? It is about simply executing and implementing the recommendations of refining the processes?

GENERAL HOWARD. Ma'am, I cannot say there will never be disagreements. I mean, you are always likely to run into that. But my feeling right now is those have been greatly minimized.

MS. HERSETH. May I interrupt? Even if there is disagreement, though, you are right. There is going to be disagreement. But despite the disagreement, are we going to just rehash the disagreement and—

GENERAL HOWARD. No.

MS. HERSETH. —push back on the contractor about the recommendations or is it, you know, we disagree, but your job was to advise us, recommend, now we are going to implement the recommendations?

GENERAL HOWARD. We have turned the corner. There is no doubt in my mind about this. Just the reassignment of people alone, you know, including the empty spaces that have been given to us upon the insistence of the Deputy Secretary. He says do not just move the people. We want the spaces, too, so that we can flesh out this organization in the correct manner.

So everything that I see from our leadership is heading in the right direction. There is no doubt in my mind about that.

Ms. Herseth. Okay.

GENERAL HOWARD. But to execute is going to require very strong leadership and determination right down until when you finally take the hill, sir, you are right.

MS. HERSETH. And authorities, right, General Howard? So do you feel—

GENERAL HOWARD. And the authorities. And as I mentioned, a very important delegation memo is currently being worked and—

MS. HERSETH. Great. We hope to see that soon and to ask the Secretary about it tomorrow because that was again a line of questioning we pursued last week with the General Counsel who kind of, I felt, was trying to have it both ways by reiterating his interpretation of FISMA, but then talking about certain options the Secretary had to delegate certain authorities.

And it was just really hard to pin him down on whether or not he was trying to allow his interpretation of FISMA to trump what these reserved powers that could be delegated from the Secretary.

So I hope we have turned the corner there, that we are getting very close, that we are moving in the right direction, but not just moving in the right direction and down the field, but that delegation exists to get us to score the goal.

Let me move to a different line of questioning. Mr. Brandewie, we have also in past weeks in different hearings gone into what is happening in other Federal agencies with the relative organization of the CIO.

Are there some weaknesses? Are there strengths that we should be evaluating to assist us with the Department of Veterans Affairs' situation?

I know that the Chairman has asked for a GAO investigation and report on other interpretations of FISMA by other General Counsels and different agencies.

And so in your statement, you note that the DMDC is at the center of most of the human resource information flowing between DoD and the Department of Veterans Affairs. Under the definition in FISMA, is DMDC considered a strategic security system?

MR. BRANDEWIE. No, ma'am, it is not. The data sources for the information that flows to the VA are not classified as national security systems.

MS. HERSETH. Okay. So it does not contain information about security clearances and military job codes?

MR. BRANDEWIE. No, it does not. If I could just comment in a little more detail. The information that goes to the VA starts out very skeletal. I mean, it is just the basic identification information. It grows as events happen in a servicemember's life.

For example, they become eligible for Montgomery GI Bill is a good example. Then we add information on that program and feed it to the VA. So the information that goes from DoD to VA is basic identification and then programmatic information.

MS. HERSETH. Okay.

MR. BRANDEWIE. It is not national security information.

Ms. Herseth. I appreciate your responses and it relieves me of some of the concerns there.

However, let me just ask this question. I know the Chairman is interested whether, you know, based on your responses that it does

not include national security information. But over the course of a servicemember's lifetime as that information grows, you know, how do you feel about data sharing with an agency system plagued by such vulnerabilities as we know the Department of Veterans Affairs' system has been?

MR. BRANDEWIE. Well, I mean, naturally we are concerned. I mean, we are concerned because of the massiveness of the scale. Essentially as came out in the data breach, a vast majority of our active duty and Reserve members' information potentially was compromised in the data breach.

However, in our data use agreements with the VA, we require security evaluations be done on the recipient systems. They have been studious about doing that. I know they are rereviewing a number of the systems right now to make sure that they are, in fact, meeting the security requirements. And so we have to in a partnership sense rely on our partner in the VA to maintain security in the system, but we all remain concerned.

One fix that we have been pursuing actually began under Admiral Gauss is to consolidate the feeds that go from DoD to VA and try and minimize the kind of proliferation of data throughout the agency. And by concentrating that information, I think we can concentrate our efforts to make it more secure and protected.

MS. HERSETH. I agree. But I think a very important first step, especially in light of the concern that as it does get spread out more, you then have the potential of employees within the different administrations— well, just the potential for more possibilities of compromise, I should say.

One last line of questioning, if I might pursue that, Mr. Chairman.

THE CHAIRMAN. Yes, ma'am.

MS. HERSETH. And I think, Admiral Gauss, you answered part of this question when you were talking about the VA concurrence process and that you were told at one point within the chain of command, so to speak, in the VA that you could not go to the Secretary with some of your concerns unless it was consistent, unless it meant these concurrence principles. And, otherwise, if things got watered down to the point that some of your concerns were inconsistent with the minimum threshold of what it was watered down to that it was hard for you to reach the Secretary with those concerns.

So my question is for Mr. McFarland and for you, Admiral. Last week, Bruce Brody, who was a former Associate Deputy Assistant Secretary for cyber and information security at VA, testified before the Committee. And he explained that while he served in that capacity, he was not permitted to speak openly about many of the problems associated with VA's management and information security.

So during each of your tenures as Chief Information Officer for

DVA, were you ever instructed by the Secretary or other senior Department officials to withhold from members of Congress any concerns you held regarding the Department's information system?

ADMIRAL GAUSS. Let me start since Bruce worked for me first before he worked for Bob.

I was never instructed nor did I direct Bruce to withhold information from Congress. What I did, and this is me doing it, is Bruce sometimes could be quite colorful in the presentation of his issues, and sometimes the importance of his issue could be lost in the colorful flavor that he would present them. And I did ask him to tone some things down, but never to obfuscate an issue.

MS. HERSETH. I appreciate the response.

ADMIRAL GAUSS. And if I may on the first part—

MS. HERSETH. Yes.

ADMIRAL GAUSS. —when I talked about the concurrence process, I did not mean to imply that I could not go to see the Secretary. The process, though, required as you lumbered your way through to get a document that could be approved, it required the concurrence.

In fact, I was called once by the former Deputy Secretary, and he said I need you to take your nonconcurrence off. And I said why. It is my view. And he said, well, if it goes the other way, will you support it. And I said of course I will. And that is the only time a dissenting view got documented from my office.

MR. MCFARLAND. I would concur with Admiral Gauss on the issues. I also managed Bruce Brody and I did see some of the colorful presentation, but he was always straightforward and given the ability to speak his mind. And never was I ever either told that I had to water down my opinions or could not speak, nor was I ever told not to submit anything to Congress.

The concurrence process to me, I agree with Admiral Gauss, is troublesome. Unlike what I understand DoD's concurrence to be, at the VA, there is no penalty for not meeting concurrence deadlines. And so what happens is you get the slow roll.

And without having a defined, definitive concurrence deadline such as, I believe, DoD has where if you do not concur or nonconcur, you do not do anything, then you opt out and have no say because one of the reasons you have problems in getting things done quickly is because this concurrence process takes a long time when people simply do not concur, neither nonconcur or concur.

The process allows nonconcurrence. That is not an issue. I believe that we have moved ahead with issues at the VA. Even with nonconcurrence, we have moved ahead. An example would be the federated model. I did not concur with the federated model, but I agreed to support it. So my nonconcurrence on the federated model was well-documented.

The issue is the time frame and this problem of slow roll, which is

what happens, is what causes you the delays in many of these occurrences from happening in the time frame they should happen. And I strongly believe that that time frame should be changed and I have spoken so.

MS. HERSETH. One last question then. Do you feel that the Chairman's proposal to elevate the status and authority of the CIO position would be sufficient to effect the concurrent process or do we also need— again, not that we want to micro manage, but do we also need to somehow specifically address the time frame of the concurrence process or would elevating the position of the CIO with that type of authority make that move on its own? Would it effectuate the change on its own as opposed to independently from another proposal of the Committee?

MR. MCFARLAND. Well, I support the move, the proposed move to Under Secretary status. And I think that will help. I also believe that the VA has at the top level competent management and I believe competent management can deal with this issue.

I do not believe personally that Congress should have to deal with an issue of concurrence in its time lines. People at the VA at executive level are competent. They can deal with this.

MS. HERSETH. I know I have taken up a lot of time, and I appreciate that response. So may I read into your response that with the competent senior leadership at the VA that elevating CIO to an Under Secretary status would allow the competency of senior management in addition to the individual holding the CIO position to address the issue of the concurrence process because if both you and the Admiral are saying that this has been a problem because it has been taking too long, but, yet, you have confidence in senior management at the VA, is it just that one move of elevating the position to Under Secretary status, and will it happen eventually because I also get the sense that you really do not think the Committee should have to do anything on that front, but is there something else that needs to happen to address it effectively?

MR. MCFARLAND. I think it will help greatly because at an Under Secretary level that the CIO will get to sit regularly with Admiral Cooper, Dr. Perlin, Bill Tuork and discuss these issues at that level which should ferret the problems out earlier. That is my opinion.

MS. HERSETH. Thank you.

Thank you, Mr. Chairman.

THE CHAIRMAN. I would like to thank Minority Council. They have brought to this hearing testimony of March 13th, 2002.

It is you and me, Dr. Gauss. You got this one too?

ADMIRAL GAUSS. Is it the verbal? If it is the verbal, I do not have that one.

THE CHAIRMAN. You know, that is all right. Yesterday Chairman Walsh referred to this as groundhog day. And, you know, I listened

to him, and I kind of half chuckled. Reading this, now I almost want to laugh out loud. There are things that we have talked about here. This is back in 2002.

You and I had a little banter going back and forth here and I asked you a specific question. Oh, gosh. We talked about who is in charge. I am in charge. A lot of your questions, I mean, you are the Admiral here. I am in charge. I am responsible. I am in charge of the ship.

But then when we got into specific lines of authority, do you have the specific line authority, and your answer is, no, sir, I do not have direct line authority. I have indirect authority for matters of IT and I have suborganizations within the structure where I deal directly with these people on matters of enterprise architecture and cyber security and that it is an efficiency gained over the past year because I do not have to go to an Under Secretary to get it approved to go to the Deputy Under Secretary in order to get one of the CIOs. I pick up the phone. I call. I direct.

So basically you are saying that I could get it done. I could achieve even though I do not have line authority. I think looking back on all of that, you would probably look at this and say that was pretty hard to accomplish because what we have learned here is that unless we give you the tools, how can you really accomplish that, you know?

I mean, that is kind of where we are. I am not picking on your testimony and your role. What I am trying to do is is I am trying to go back in time, see where we were, where are we today, and how we move to cure.

And there is something else in here. Let me go to this one. We even had a conversation, and this deals with compliance, and we were talking about the lines of authority again. And then I got into the question about the rating of people. And I asked you what input do you have with regard to rating people, and you said I have direct input to the reporting seniors of these folks for what goes into their performance evaluation.

I then say okay. Then with regard to promotions and merit bonuses, do you have an input into that also, and you then say the process at the VA? And I said if you are working with someone in one of those administrations who is messing with you and making life difficult to get implementation to the one VA is what you were talking about at the time, going, do you have the ability to say no to a merit bonus. And you say I do not have that.

The reason I took time to go back in history with regard to this conversation is that since your days at the VA to today, we advance ourselves, the VA has continued to receive this failing grade, yet, we have individuals of whom received bonuses.

Now, going back to this whole question that Mr. Bilirakis brought up about micro management, you are absolutely right. We do not like to do that. We have an oversight responsibility and function.

But if we are going to create a package and part of that package is also going to be on personnel issues, whether it is in specific statutory authority or in report language, if we are to say that with regard to performance reviews, if as a CIO you are to ensure compliance, should IT compliance be one of the criteria of performance reviews or merit bonus?

So I am interested in your thoughts, Dr. Gauss, Mr. McFarland, General Howard.

Admiral Gauss. Mr. Chairman, as far as the recommendation of including those as part of the evaluations, I would agree.

THE CHAIRMAN. All right. Thank you.

Mr. McFarland.

MR. MCFARLAND. I would submit to you that I not only agree. I would submit to you that there is proof that it works because if you remember last time we got an F, one of the major reasons we got an F is because we did not have our 600 major systems certified and accredited.

And when Secretary Principi got very upset about that, we asked for authority to include the potential of bonuses not being paid in the outcome if all of those 600 systems did not get C and A'd within a year. Those 600 systems did get C and A'd in a year and it was because of that potential financial threat.

I am convinced of that because he was very clear with the management team that he would look very harshly on bonuses and people's paychecks would be affected if this did not happen. So I would submit to you that it does work.

THE CHAIRMAN. General Howard.

GENERAL HOWARD. I totally agree, sir. It is a good mechanism that ought to be put in place.

THE CHAIRMAN. All right. Let us envision this for a moment. How would this work under the federated model? You are now an Under Secretary. You have the responsibility under FISMA to ensure compliance. The Secretary has now directed authorities to you. I am anticipating that finally this slow roll approach over Directive 6500 after three years is finally coming and that is what I am hoping for. How do we do it? How do you do this?

GENERAL HOWARD. Sir, the area that it would be difficult is punitive action, you know, any action that must be taken against a person from the person's supervisor. In other words, if Art, for example, worked in another department and violated one of these policies and violated an item—

THE CHAIRMAN. Can you turn that on for me, your microphone on, please.

GENERAL HOWARD. —you know, violated one of these policies, we can make it very clear that he has done so. But the punitive action itself cannot be taken by the CIO. It would have to be taken by his

supervisor.

THE CHAIRMAN. Right. But let us keep it to the question on a performance measure.

GENERAL HOWARD. Right.

THE CHAIRMAN. So I am in one of the stovepipes.

GENERAL HOWARD. Right.

THE CHAIRMAN. So I am now a middle-level manager, just like you, directing a battalion.

GENERAL HOWARD. Right.

THE CHAIRMAN. You have given a directive to your battalion commander that you want certain things to be noted. So all of your officers, they have to make sure that they are compliant with one of your directives. So how do you as now an Under Secretary and CIO, and you now have got CIOs completely under you, right?

GENERAL HOWARD. Right. And I—

THE CHAIRMAN. So how are we going to do that?

GENERAL HOWARD. Those folks belong to me. There is no question about, you know, disciplinary action, any kind of action against folks who directly work for the CIO. If they work somewhere else, you know, clearly violations of anything should be reported to the CIO. You can have that provision.

THE CHAIRMAN. All right. Wait. You are off subject again. Let us go back to the issue on bonuses.

GENERAL HOWARD. On bonuses?

THE CHAIRMAN. On merit, performance, and bonus.

GENERAL HOWARD. And the individual is in one of the stovepipes?

THE CHAIRMAN. Yes.

GENERAL HOWARD. And gets a bonus?

THE CHAIRMAN. Wants a bonus.

GENERAL HOWARD. And should not have gotten—

THE CHAIRMAN. But is not compliant.

GENERAL HOWARD. And should not have gotten the bonus?

THE CHAIRMAN. Uh-huh.

GENERAL HOWARD. The only thing you can do is elevate it to a higher level because, you know, or—

THE CHAIRMAN. Wait. Time out. Let us break this out. One of your CIOs is at one of the medical centers.

GENERAL HOWARD. So he belongs to me.

THE CHAIRMAN. But he is at one of the medical centers.

GENERAL HOWARD. Does not matter. He belongs to me.

THE CHAIRMAN. He is at one of the medical centers and he belongs to you?

GENERAL HOWARD. Yes, sir.

THE CHAIRMAN. He is sitting at the table as any good hospital administrator would do. He has got him at the table there, and that hospital administrator, one of his issues is to be compliant.

And what I am trying to figure out under the federated approach, since the CIO is not going to be in these lines of authority with regard to punitive actions, but if you make it a performance measure, then it is the Secretary through the Under Secretary that has to ensure that certain directives are made and have compliance.

GENERAL HOWARD. Yes.

THE CHAIRMAN. That is our challenge with tomorrow's panel—

GENERAL HOWARD. Sir—

THE CHAIRMAN. —because what is clear today is that with regard to the General Counsel's legal opinion that said unto Bob McFarland that you do not have this authority, then that authority then vested with the Secretary, and directive 6500 just sat out there. Nothing was really acted on with regard to those authorities. It vested with the Deputy and the three Under Secretaries.

And even though you had the responsibility of compliance, authority was not exercised to bring the Department in compliance with FISMA.

GENERAL HOWARD. Sir—

THE CHAIRMAN. I am just letting you know that.

GENERAL HOWARD. Okay, sir.

THE CHAIRMAN. So my challenge here is if we are going to go under the federated approach and we say, fine, we are going to bring it into a performance measure, your CIOs out there can be counsel to that administrator, you know, meeting with them, making sure that they are compliant because here is what is in the pipeline or here is what is going on. That is what he is there for. He is to be the counsel to the administrator. You agree with that?

GENERAL HOWARD. Sir, he also has a black hat on his head, too, that—

THE CHAIRMAN. What does that mean?

GENERAL HOWARD. —needs—he needs to report instances that are not in compliance.

THE CHAIRMAN. And who does he report that to?

GENERAL HOWARD. Up the chain to me.

THE CHAIRMAN. All right. But he also has a responsibility to the hospital administrator, correct?

GENERAL HOWARD. Yes, sir. He sure does as a customer. You know, he is a service provider.

THE CHAIRMAN. Okay.

GENERAL HOWARD. But he also has eyes and ears and he needs to keep them open. And if he uncovers things that are not going on, I expect him to do something about it. Obviously to inform the hospital director, but me too.

I mean, it is like first brigade and second brigade. You know, I cannot give an Article 15 to some guy in first brigade, but I sure can put heat on that brigade commander through the division commander.

And it is particularly a problem in the punitive type of action.

THE CHAIRMAN. So this is going to require—let me turn now to Gartner—under this federated approach, in order for this to work, this is going to require some pretty stern leadership from the Secretary, Deputy Secretary to the Under Secretaries to perfect it.

MR. BRESSON. It does not relinquish leadership at any level, sir. You characterized it as stern. That would probably be a good thing. But the model itself does not preclude that leadership from being exercised, those authorities to be implemented.

THE CHAIRMAN. I appreciated your insights with regard to Ms. Herseth's questions. You did a very good job today with regard to the concurrence and nonconcurrence. That was insightful or us.

And I appreciate the Deputy Secretary being here today, that you are hearing this, and those are things that you struggled with over the years that you have worked. But those time lines, I think, that have been recommended are probably pretty important.

Having that directive sitting out there for three years was probably not a good thing, and we will get a chance to talk about that tomorrow.

With regard to nonpay contractors involved in software development, do you know how many there are?

GENERAL HOWARD. Numbers of contractors, sir, I am not sure. I will have to get that for you.

THE CHAIRMAN. Mr. McFarland, would you have any idea approximately?

MR. MCFARLAND. Contractors are in nonpay, yes. I do not know exactly how many are there. I could give you an educated guess. I would say it is somewhere between 500 to 700, I would guess, throughout the Department. And that is made up of administrations and staff offices. That would be my guess.

THE CHAIRMAN. Now, there is—

GENERAL HOWARD. Sir, if I could pile on. I mentioned that we have phase one of this program we put in place, assessment. We finished the internal part. The next steps is contractors, you know, where are they, what are they doing, et cetera, et cetera.

THE CHAIRMAN. The—

GENERAL HOWARD. When we get through with that, we can give you some feedback.

THE CHAIRMAN. The Secretary gave testimony yesterday to Mr. Walsh's Subcommittee on Appropriations with regard to the concerns about a subcontractor perhaps releasing data if they did not receive a proper payment. The Secretary responded that he was not aware that he had any prime contractors that were offshore.

Now, as I understand, this may be, in fact, technically correct. But what happens if we also put in our package so that we are not jeopardized nor our national security, if we are going to have contractors,

that they may not subcontract with any off-shore entity.

What are your thoughts?

GENERAL HOWARD. Sir, I am not familiar with the details of the incident. I believe you are right. It was a subcontractor that was involved.

THE CHAIRMAN. If you know about that, will you make sure the Secretary is briefed for tomorrow?

GENERAL HOWARD. Yes, sir.

THE CHAIRMAN. All right. Mr. McFarland, your thoughts.

MR. MCFARLAND. I think it is important to know who subcontractors are. There are difficulties in the IT world today. It is an international product. So much of what is put into IT both hardware and software today, much of it does come from various overseas subsidiaries and various overseas environments through contracts.

I think it is wise in the contracting process to understand who your subcontractors are and put in a requirement that requires they notify you if they intend to push any of that work offshore, and then you can make a decision at that point whether you believe that is—I mean, pushing something offshore to Britain, for example, may not be near the issue it would be to pushing something offshore to China. And I think it is a matter of understanding and having a requirement would be good to know what, if any, off-shore requirements come up.

THE CHAIRMAN. All right. I am going to go to Dr. Gauss, but I want you to think about this because I am going to come right back to you, Mr. McFarland, about your counsel to us with regard to what should be included in our package. But I want you to think about it and I am going to come back to you.

Dr. Gauss.

ADMIRAL GAUSS. I would think that in dealing with the purchase of purely commercial products and the support services that go with those commercial products, it would be very difficult to sever off-shore relationships.

That said, any contract that is done for the government where the government is getting specific products and services that meet a specific government need, I think you could impose restrictions that limit off-shore involvement. But there are two separate camps here, I believe.

THE CHAIRMAN. Well, we have experience in this in the Department of Defense with regard to our procurement policies, who is going to build what, who gains access to what, from weapons systems to guidance systems. I mean, you name it.

I hate to create that type of system, but I am very insulted that there is a company out there in another country that would try to blackmail our country, and that is what they tried to do.

And what that does is create a heightened awareness. And you are absolutely right. You do not want to penalize Great Britain or penal-

ize any of our valued allies in the world, but I am pretty concerned.

I am going to come back to you, Mr. McFarland. Take your concept and take it to the next step. What is your best counsel to me?

MR. MCFARLAND. Well, as Dr. Gauss said, there are two distinct domains here. Those are products and services that are bundled, if you will, such as a workstation, a printer, any kind of bundled service where components come from all over the world. You have things called TAA and BAA by American act, those kinds of acts that preclude you from taking product made in certain countries that do not meet those requirements. So you are protected there.

I think your biggest problem is the other domain which is the services domain where you contract with someone for a service, transcription services, you name it. And there you run into the problem.

I think you should require that before any subcontractor, allow any of that work to go off-shore, that he get clearance from the VA so that the VA has an understanding of whether that offshore is Great Britain or if that offshore is China. And I think it would be wise to- -

THE CHAIRMAN. So, number one, would be a notification procedure?

MR. MCFARLAND. Right. And then an approval.

THE CHAIRMAN. And then an approval process, right?

MR. MCFARLAND. Right.

THE CHAIRMAN. Go ahead.

MR. MCFARLAND. I mean, I am not familiar enough with our contracts for services in the VA to know, and I am sure each of them is unique for the service. But those to me ought to be clauses that are boiler plate and that an approval process be required if a subcontractor is an off- shore entity or any of the information is offshore.

THE CHAIRMAN. All right. Here is why I am taking a little time on this particular issue.

MR. BRESSON. Excuse me, Mr. Chairman.

THE CHAIRMAN. Yes.

MR. BRESSON. The only thing I might add with respect to services is it would be significant, yes, to identify the subcontractor as an entity, but quite often knowing the key personnel and their background and/or other attributes about them might also be significant and important to such an action.

THE CHAIRMAN. Thank you for that because the Secretary has brought up several times the issue about, background checks -- that individuals with access to certain data even within the VA have not had background checks.

So what? We are going to highly scrutinize Americans, yet permit some of the services and access to data to be subcontracted to a third-world country with no form of notification or compliance or approval. So I think we need to pause and think about that as we develop our systems. So thank you very much.

So now let me turn to DoD, and that is why I am pretty concerned.

My first question would be, because I do not know the answer to this, when a forensic analysis of the data was done with regard to what was stolen, with regard to active duty Guard and Reserve, were MOSs included?

MR. BRANDEWIE. No, sir.

THE CHAIRMAN. No?

MR. BRANDEWIE. No, sir.

THE CHAIRMAN. Okay. Does the VA within the universe of their data, would they have the MOS?

MR. BRANDEWIE. No. We do not furnish the MOS as part of our data transfer. On separatees, the DOD Form 214, and I am not exactly a hundred percent positive, on separatees, I believe the MOS is included on the DOD Form 214.

That does not come in a data exchange. It comes through a basically paper form and is actually automated by the VA. When it is automated, I am not sure if they include the MOS, but I would assume they do. But it is not part of our automated feed from the Department of Defense to VA.

THE CHAIRMAN. Much of our present War on Terror is operated in the dark world. And I have heightened awareness of our special operators and they sure do not want the world to know who they are and what they have done.

And I am really concerned with regard to protections of data that is out there because I look at this and say, well, yes, this may have happened, but what is next, what could happen.

And I do not want to blow up worst case scenarios, but, Mr. Deputy Secretary, this is an issue I want to explore with you over the next several weeks, and we will bring it up tomorrow on how we develop a system because, you know, as we work here with the Department of Defense, they are not going to be too keen about how do we gto health medical records.

You know, if we cannot give veterans assurances, how can we give our partners assurances? I do not have an expertise or background in procurement law and so I am going to have to turn to experts to help us on how we devise a system to do this.

Let me ask a question about biometrics, user ID numbers. I am also considering placing in our package—this package will be large enough that it will have jurisdictional referrals to other committees. We are going to recommend changes to FISMA.

I am not going to have any of this in the future about lawyers' interpretations. We are going to make this pretty doggone clear. And I have already spoken with Mr. Davis about it, so we are going to make those corrections.

I am also considering saying to the Department of Defense in this legislation and the VA that you cannot use the Social Security number. So let me ask for your thoughts about that.

MR. BRANDEWIE. If could start out—

THE CHAIRMAN. You are going to have to come up with a soldier's ID number or some type of number that both the VA and DoD use that is not the Social Security number.

MR. BRANDEWIE. In passing, sir, I referred to a consolidated feed between DoD and the VA which were to replace the legacy feeds that we do. In that consolidated feed, we feed the VA a new ID number which we give a very odd name to. It is called electronic data interchange personal ID.

It is a made up number. And it is the number we actually trade with the VA in the consolidated feed instead of Social Security number. And it could form the basis for interaction between the two departments without reliance on Social Security number.

Having said that, Social Security number remains an important identifier in establishing identity. Once identity is established, then between agencies and in large- scale computer systems, it would be possible to only use Social Security number simply as an identity anchor and not a way to trade information between systems.

I might add we do that also with the medical community and we have established this number as a patient ID with the medical community, and also pass that over to the VA as well. There are new technologies that are emerging that would allow us to deemphasize Social Security number as a universal identifier.

Having said that, totally banning it from IT systems would create chaos, but it could be deemphasized especially in terms of data interchange. And, again, once identity is established, its importance recedes, and that could be emphasized in legislation.

The Chairman. Our challenge here is that so long as the financial services industries rely upon that Social Security number, therein lies our challenge. So if I take that out of their criteria, you know, I at least can protect our veterans and our military.

What we would have to do is is when they take their oath of enlistment or commission, we are reverting back to the old days where you get your ID number, your soldier number, or whatever.

Do you remember what yours is, Mr. McFarland?

MR. MCFARLAND. Yes, sir.

THE CHAIRMAN. What is it?

MR. MCFARLAND. US54342381.

THE CHAIRMAN. There you go.

You guys knows yours?

GENERAL HOWARD. Yes, sir, 097560.

THE CHAIRMAN. Wow. Well, I am just letting you know that is where I am considering going. And it might create a heartache for you because if you have come up with some other kind of number, we will figure out how we can best do this, and we want to work with DoD to do that because that will also be what we will use with regard to our

patient medical records and that type of thing.

GENERAL HOWARD. Sir, I might add within the VA for employees, we have discussed going to ID numbers for employees.

THE CHAIRMAN. Just to let you know some of the major areas where we are thinking about, and this is not an exclusive list at all, as this Committee and others work together, we are going to look at this issue on performance reviews and criteria. We are going to consider this movement of the CIO to an Under Secretary and elevate the CISO to the Deputy Secretary or Assistant Secretary. I am sorry.

I personally asked the Secretary what personnel changes, if any, does he need with regard to his authorities with regard to disciplinary actions to make sure he can ensure compliance or fire someone.

We are going to look at the issue on the credit monitoring package. I am deeply appreciative to the VA on what they had done in stepping forth to offer that to veterans along with the insurance package. That was a good thing.

I am deeply disturbed with regard to the lawsuit. For the VA to move forward, to take actions to help the veterans and now for a class action lawsuit to prevent you from advertising that assistance, what it does for us is it shows that time is of the essence for us to move our package, and we are going to have to give a directive.

The Secretary shall. And we want to work with you with regard to our language. But when I come in and I use mandatory language instead of discretionary language, what I have done is I have shot a hole through this class action lawsuit out there.

We will also include some FISMA changes and that DoD, VA are not authorized to use Social Security numbers with regard to personal identification. We might direct them to really create a soldier's number, an identification number. It probably would be better to do it in the prospective manner than to say that you shall not or cannot use a Social Security number. I mean, that does not make a lot of sense.

We want to address the issue with regard to the outsourcing and we are also going to bring back our issue on centralization. I have not let it go. I cannot let it go. I respect your opinions. I got to figure out how we can get there.

Let me ask Gartner. I will not keep you here much longer, but let me ask Gartner Consulting. When you turn to one of your major corporations out there and you have now said we need to centralize your IT, how long does that take?

MR. BRESSON. Mr. Chairman, there are a number of factors in that kind of advice, particularly the current business environment, because, as we all know, it is not all about IT meaning that the way decisions are made in the business or in this case in the mission and the business will set the stage for how successful centralizing and/or federating the IT portion of that business.

We do counsel that once the decision is made, centralization, rough order of magnitude, would probably take anywhere between 12 and 36 months, and there are a lot of variables there, the global dispersion of the assets and the people and the organization, the sheer volume of systems and other items that need to be brought under control.

The Chairman. All right. Let me break it down and go right to security. So when the VA designs a security policy, they finally get that done, what kind of training is going to be needed to promulgate that policy to make sure it is properly implemented? What kind of time are we looking at?

Mr. Bresson. I would be guessing, sir.

The Chairman. I mean, you are consulting a lot of companies out there that make changes and all. I mean, three months, six months, nine months?

Mr. Bresson. Right. There is probably a footprint that needs to be established that has a defined period in which it should be established. And then beyond that, there is the continual changes of new personnel coming aboard, potentially other changes in personnel roll, et cetera, that would need to be addressed.

In terms of time—

The Chairman. Let me reask the question because you are very good at dancing now. What is a reasonable time line with regard to implementation of a security policy for an entity such as the VA or a major corporation?

Mr. Bresson. Implementation of a security policy. Well, I am not a security expert, sir, but I would imagine that something implementation-wise starts within a 90-day period and potentially to a 180-day period.

The Chairman. How long did it take DoD?

Mr. Brandewie. To implement a security policy?

The Chairman. Yes.

Mr. Brandewie. I mean, in the basics, it has taken a number of years. I mean, and security is always evolving and changing. I mean, the centralization of the global information grid took probably over two years, you know, and the security policies associated with it. But we are very diverse and decentralized with IT, so I am not sure there is a corollary there for the VA.

The Chairman. Well, kind of because you are very decentralized and so is the VA. And it is not that it is all that bad either.

Mr. Brandewie. No.

The Chairman. And just because it is decentralized does not mean you do not have security policies. They have security policies. It is that it is agency-wide security policy. So it is the development of the agency-wide security policy and its implementation as you centralize that is our challenge, right?

Mr Brandewie. If I could make one comment. I mean, there are

policies all over the place and security policy is certainly one of them. It takes a long time to articulate and work its way through the system.

One thing that DoD has done that has been very effective, I believe, is the establishment of a joint task force for network operations protection, JTFGNO. And they are very fast in terms of identifying a security issue, finding a fix to a security problem, mandating that the fix be implemented, and enforcing the implementation of that fix.

It is like, if you will, a kind of go team that takes the security policy, puts it against the real world threats that are out there, monitors those threats, and then takes action. And that I found to be particularly effective within DoD.

THE CHAIRMAN. So let me ask this about FISMA for a moment. When the FISMA audits have come back and have given the VA very poor ratings over the last four years, as we proceed in this federated model, the responsibility here rests with the Secretary. He acknowledges responsibility.

Who does he delegate this to with regard to compliance based on the FISMA audit? Are you aware, General Howard?

GENERAL HOWARD. Sir, it will be cleared up with this delegation memo I referred to. But as I sit here today, it is my problem, you know, to set the policies and set the actions that need to take place to alleviate a deficiency because the reorganization that will take place, a good number of those will rely with me now.

For example, take the protection of server rooms and things like that. That is now my responsibility with the current direction we are going in the IT reorganization.

I do not know if that answers your question, but—

THE CHAIRMAN. You have a really difficult job. You do. I am not here to beat you up at all because you are saying to this Committee it is me. That is no different than what Admiral Gauss said back in 2002 to Ms. Carson, it is me.

So you can do everything you want. But if you do not get the backing from the Deputy Secretary or the Secretary to make sure things happen to those Under Secretaries, you are going to be back before this Committee. Members of Congress are going to be asking you why once again did you get an "F" in the audit.

GENERAL HOWARD. Sir, the backing is absolutely necessary. You are exactly right. But it is up to me to make it clear as to what should occur. That is my problem. And we have got a lot of work to do in that area.

THE CHAIRMAN. DoD, you received an "F" on your audit, too, did you know, from FISMA?

MR. BRANDEWIE. I believe that is correct.

THE CHAIRMAN. Why did that happen?

MR. BRANDEWIE. I really do not know. I am not familiar with the

detailed reasons for the DOD score.

THE CHAIRMAN. All right. I just thought I would let you know I knew. You thought you were going to get away with it, didn't you?

All right. I want to thank all of you for coming. I have a great deal of respect for you and what you are trying to do here. It is hard for me. I have never been a CEO. I have never run a major organization. It is hard for me, though, in today's time whether it is a government department or agency or whether it is a company or any form of entity, when I have IT involved, why I would not make the CIO my new best friend. I do not understand why that would not happen.

I had an opportunity, just to let you know, McKesson Company out there. Bloomington Hospital just outside of my district, they wanted to modernize their IT. They wanted to do some centralization and do some things. And they brought in McKesson. And the hospital administrator brought in someone from Purdue University, very sharp in information management, and made that CIO his best friend.

And it sent such an incredible signal to the medical director to get on board, that these things are coming, these changes are made, whether it came from the business side of the house; tell me what your recommendations are, what you are looking for. The CIO is going to look at it.

On the medical side of the house, whether it is filmless or that medical technologies, everything had to be compatible and everything had to go through the CIO. And everybody at the board table knew that and everybody was also enthused to talk about how as a team they were all going to work. And they all wanted to know and associate with the CIO. That was a system of pure empowerment, and they were able to perfect changes in a hospital setting rapidly.

So it is challenging for me, General Howard, why you are not the new best friend. I do not know if you are or you are not. But what I am saying is that I recognize you have a very difficult job because you have to be the agent of change. And I do not care if you are going to change the flavor of ice cream at lunch, you are going to have somebody attack the agent of change. And it should never be taken personally when you are the agent of change. All right?

GENERAL HOWARD. Yes, sir. I agree.

THE CHAIRMAN. We want to continue to work with you. Please, if you have recommendations based on the questions, please be in touch with the Committee as we formulate the package.

To Gartner Consulting, thank you very much. You have well earned your pay in your counsel and advice to the VA. It has been very sound, and we appreciate that.

To DOD, you have still got your own work to do, and we will send you back. We appreciate you coming out here today.

This hearing is now concluded.

[Whereupon, at 1:42 p.m., the Committee was adjourned.]

APPENDIX

STATEMENT OF CONGRESSMAN BOB FILNER
before the

HOUSE COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES

June 28, 2006

"IT Architecture"

- **Thank you Mr. Chairman. This is the fourth full Committee hearing on information security and technology we have held since being advised about the lost personal data of veterans.**

- **Each of the previous hearings has addressed the topic of Information Technology (IT) architecture at the VA. Almost without exception, expert witnesses outside of VA have recommended a centralized approach to the agency's IT architecture.**

- **They see advantages in standardization, in flexibility for implementing system-wide changes, for management efficiency, and for enhanced control and safeguarding of VA data.**

- **This view was also supported by a former VA employee and cyber security expert at last week's hearing who testified--in no uncertain terms--that the system of controls and accountability at VA for information security and cyber security is badly broken.**

- **When this former VA cyber security chief was asked why he did not tell this Committee of the myriad of problems he noted when he had previously testified before us in his official capacity, he told us that he was muted--not allowed to comment openly. That, by itself, is a sign of the problem.**

- **Time and again the recommendations of IT experts were ignored. Recommendations were ignored by VA from:**
  - **Independent consultants who found repeated material weaknesses in information security.**
  - **The Government Accountability Office.**
  - **The VA Inspector General.**

- **When new, "IT-savvy" blood entered the VA's information management bloodstream, carrying with it new ideas, a virtual tourniquet was applied by the Administrations and offices in the VA to stop the flow of those new ideas.**

- **And when a proposed policy change on IT was circulated through the VA for concurrence, most responders did not concur with the proposed changes. They seemed to be collectively focused on avoiding accountability rather than on implementing a system-wide methodology for information security.**

- **Mr. Chairman, the key question for us to review at this hearing is: "Which VA IT Organizational Structure would have best prevented VA's "Meltdown" in Information Management?"**

- **I have an answer to that question. We all agree in the House--at least the 408 of us who voted without any opposition to centralize IT management at the VA--that the benefits of a centralized approach outweigh other considerations.**

- **But there is a human element that underlies the VA IT architecture. Superior managers can wrestle success from poorly designed management systems. Conversely, the best management systems can be derailed by bad managers or by willful actions to derail them.**

- **In my opinion, VA does not now possess a satisfactory IT management system, nor is it striving toward implementing a good system in the near future. Couple this with the well documented institutional management failures regarding information security at VA and we are left with a dim future that matches a poor systems choice with poor managers.**

- **Our panel today taps into the perspectives of three individuals who are or were instrumental in shaping some aspect of VA's IT community and who, in the opinion of many observers, were partly the victims of VA's culture of turf control.**

- **Mr. Bresson's company has noted many of the problems VA has faced and recommended solutions. The perspective of his company is important to our assessment.**

- **We will also hear from a principal partner with VA in many policy-driven initiatives, the Department of Defense. Our interest here will be on the long-term impact on existing DoD and VA sharing initiatives that were finally beginning to yield some positive results.**

- **It is my hope that this data breach has not irreparably harmed this critical relationship.**

- **Mr. Chairman, I yield back.**

Opening Statement of
John A. Gauss
Former Assistant Secretary for Information and Technology
And Chief Information Officer
At the Department of Veterans Affairs

Before the
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
U. S. House of Representatives

June 28, 2006

Good morning, Mr. Chairman and members of the Subcommittee. Thank you for inviting me here today to discuss the important issues related to the Information Technology (IT) reorganization efforts at the Department of Veterans Affairs (VA).

I would like to provide the Committee with some background information to help in understanding my thought process regarding VA's IT reorganization.

At the time of my confirmation hearing as the VA's Chief Information Officer (CIO), the Department was faced with:
(1) An ever expanding IT budget;
(2) Programs that were defined in a "stovepipe" manner due to the lack of an Enterprise Architecture;
(3) Programs that were consistently overrunning budget, behind schedule, and failing to meet their performance requirements;
(4) Implementing a comprehensive cyber security program; and,
(5) Having to implement an "executive level" oversight process which was a recurring deficiency identified by the General Accountability Office (GAO).

As a result of the above and as presented in my opening statement before the Senate Veterans' Affairs Committee on 2 August 2001 during my confirmation hearing, I stated that I had five strategic objectives:
(1) Complete the Enterprise Architecture road map to the future;
(2) Integrate disparate telecommunications networks to improve performance and responsiveness for our Veterans;
(3) Implement a strong information security program and infrastructure;
(4) Create a program/project management process to oversee and help the VA information technology program/project managers deliver products that meet requirements, are delivered on time, and stay within budget; and,
(5) Establish information technology metrics to continuously measure our ability to meet our Veterans' needs.

Although implementing a strong information security program is listed as number 3 in the above list, it ***was*** my number one priority. Establishing a comprehensive Enterprise

Architecture and integrating the telecommunications networks were placed higher in the order since I believe they are prerequisites to attacking the number one priority.

During my previous 32 year career in the United States Navy, I learned to address organizational issues by using the following simple thought process:
(1) Define the problem to be solved;
(2) Define the optimal, affordable solution to the problem;
(3) Define what work would be accomplished by government and what work would be performed by industry; then,
(4) Organize to implement.

Given the problems and strategic objectives defined above, I concluded that:
(1) All IT programs and IT-related activities affecting the three Administrations and the VA Central Office should be centrally managed at the Department level with funding located in the Department's and not the Administrations' budgets. Specifically:
(a) Enterprise Architecture;
(b) Cyber Security except facility-specific Information Security Officers (ISOs);
(c) Telecommunications networks;
(d) Corporate data centers;
(e) Any program with the above characteristics that would result from developing a comprehensive Enterprise Architecture, such as VA-wide Registration and Eligibility and a central Call Center; and,
(f) All IT programs under the auspices of any VA Central Office staff code.
(2) All development activities related to individual Administration IT programs should be managed at the Department level with funding from the Administration with the requirement for the program.
(3) The operations and maintenance of in-service IT systems directly related to mission execution within an Administration should be managed by that Administration subject to a comprehensive budget and funding execution approval process with ultimate authority for approving the expenditure of funds residing in the office of the Department's CIO.

I recognize that the above conclusions are not consistent with current thinking, but I would respectfully ask the Committee to consider the following: without central management of the development activities, how will the Department ever implement a comprehensive department-wide Enterprise Architecture to eliminate duplication; cross-functionally integrate VA's IT business processes; and ultimately slow or stop the growth of the department's IT budget?

I hope information I have provided will help the Committee in its deliberations regarding VA's IT reorganization.

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

Statement of
MG Robert T. Howard (Ret)
Senior Advisor to the Deputy Secretary
Supervisor, Office of Information and Technology

Before the
U.S. House of Representatives
Committee on Veterans' Affairs

June 28, 2006

Mr. Chairman and members of the Committee, good morning. Thank you for your invitation to discuss the Department of Veterans Affairs information technology reorganization plan and the recent data loss incident.
I am accompanied today by Mr. Joseph K. Shaffer, Director, VA IT System Model Realignment Office and Mr. Pedro Cadenas, Jr. Associate Deputy Assistant Secretary for Cyber and Information Security. I request that my written testimony be entered into the record.

I would first like to give you an update on the VA IT realignment. The VA IT System Model has been developed and approved. The two principal underpinnings of the VA IT realignment are to ensure: (1) continued world-class service to our veterans, and (2) our continued commitment to patient safety.

The key area of focus is to transition VA's IT community to operate within the VA IT Management System that separates the Development and Operations and Maintenance domains. Hence, VA will establish required business practices and processes that harmonize the oversight and budgetary responsibilities of the Office of the CIO, the functionality of the Domains, and business relationships of the IT service provider and the customer for all IT activities across the entire VA.

As background, in an Executive Decision Memorandum dated October 19, 2005, the Secretary of the Department of Veterans Affairs (Secretary) approved

the concept of a new IT Management System for the VA. This decision to move to the VA IT Management System was made to correct longstanding deficiencies in the current decentralized IT management system. The concept of a new VA IT Management System initially separates the IT community into two domains – an *Operation and Maintenance (O&M) Domain* that is the responsibility of the Assistant Secretary for Information Technology (AS/IT) / (VA CIO) and a much smaller *Application Development Domain* that is the responsibility of the Administrations and Staff Offices. Although the domains are separated, the VA CIO retains oversight responsibilities for all VA IT projects. As Secretary Nicholson testified at the House Appropriations Committee hearing on June 27, 2006, the long-range plan is to bring the Application Development Domain into the larger O&M domain resulting in a single domain for IT.

To achieve greater clarity and understanding of the design and processes of the VA IT Management System, the Secretary directed the development of a Model that would be used to guide the development of a more thorough IT Transition and Implementation Plan. As noted above, the goal is for the Department of Veterans Affairs to complete the transition to this new VA IT Management System on or about July, 2008.

The VA IT System Model will strengthen the protection of all sensitive information As VA's General Counsel Tim McClain testified last week, the Federal Information Security Management Act (FISMA) requires the Secretary to delegate to the CIO sufficient authority to "ensure compliance" by the agency with the above information-security requirements. This must include the authority to (1) create and operate the agency-wide information security program; (2) establish information security policies and procedures and control techniques for the agency, which, when followed, will ensure compliance with all of the above requirements; (3) train and oversee personnel with significant responsibilities for information security; and (4) assist senior agency officials

concerning their information security responsibilities, including the analysis process.

The agency-wide security program directed by FISMA should provide systematic guidance for the conduct of the risk analysis process, security awareness training for all VA personnel, periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, a process for remedial action, procedures for detecting security incidents, and plans for ensuring continuity of operations for information systems. The policies and procedures should interpret, explain, and apply to VA the applicable external standards and provide guidance for the application of these standards to VA operations. The control techniques should permit monitoring of the numerous activities in which programs are required to engage to determine that they are accomplished in accordance with applicable standards and that any appropriate remedial actions are timely undertaken. The program, policies, procedures, and control techniques, and any other actions, should be developed in mutual coordination, cooperation, and collaboration between the CIO and program officials.

FISMA does not necessarily require delegation to the CIO of direct control over agency programs, because such control is not the only means by which the information security-objectives may be accomplished. For example, even without direct control over certain programs, a CIO could endeavor to ensure compliance with governing standards through training and otherwise influencing the behaviors of key program-security personnel. While an agency head certainly may choose to confer certain enforcement powers on the CIO, e.g., the ability to sanction program officials outside the CIO's immediate organization for noncompliance with departmental policies, we do not read FISMA to require it.

The VA IT System Model was developed as a framework for VA's future IT Management System. The principal elements of this *IT System Model* include:

1. Definitions of the roles, responsibilities and initial boundaries between the *Operations and Maintenance (O&M) Domain* that is the responsibility of the AS/IT (CIO) and an *Application Development Domain*, to include determination of business needs and priorities that is the responsibility of the Administrations and Staff Offices. Although the Domains are separated, the Model sets forth essential cohesion between the domains in order to provide the CIO with oversight and budget responsibilities for all VA IT projects.
2. Authority, delegation of authority, and governance structure and process for the conduct of all VA IT-related business;
3. Key IT service delivery business process flows;
4. Sample scenarios to illustrate how Domain activities are coordinated by process flows. These process flows must be clearly defined to reflect the critical interdependence of business applications and the performance of the IT infrastructure; and
5. A recommended "To-Be" organization for the office of the CIO designed to balance the tactical needs of operating a complex infrastructure as a shared service with the strategic needs of aligning IT resources to best meet the mission requirements of the Department.

As you are aware, the Secretary initiated several recent actions to tighten our privacy and data security programs. On May 24 the "Data Security-Assessment and Strengthening of Controls" program was established to provide a high priority and much more focused effort to strengthen our data privacy and security procedures. The two principal objectives of this program are to first, reduce the risk of a recurrence of incidents such as the recent data los, and second, to remedy the material weakness reported by the Inspector General. There are three phases to this effort; Assessment, Strengthening of Controls,

and Enforcement. We are almost through the Assessment Phase and have actions underway in the other two phases as well.

On May 26 the Secretary issued a Directive that requires the top leadership to instruct all VA managers, supervisors, and team leaders of their duty and responsibility to protect sensitive and confidential information. In this memo the Secretary also announced that he had convened a task force of VA senior leaders to review all aspects of information security and make recommendations to strengthen our protection of sensitive information. One of the first tasks of this group is to complete an inventory of all positions requiring access to sensitive VA data by June 30.

We began a Security Awareness Week at all VA facilities (hospitals, clinics, regional offices, and cemeteries) on Monday June 26. Each day managers are expected to focus on one or more elements of information security in meetings.

We are emphasizing training in privacy and cyber security for all employees. We require all VA employees, contractors, and volunteers to complete both Cyber Security and Privacy Training, annually. Both designed to help VA employees understand the importance of protecting sensitive information and make them aware of their responsibilities to protect this information. Normally, employees are required to complete this training by September 30 of each year. However, given the recent incident, the Secretary has directed all employees to complete both courses by June 30.

We will be conducting a Department-wide inventory of laptops to ensure that they carry the encryption and other cyber security software necessary to ensure remote access users are operating in a safe and secure environment.

This effort is on hold, however, due to a recent lawsuit. It will continue once legal clearance is obtained.

Finally, we are reviewing all policies, directives, and handbooks relating to privacy, cyber security and records management to ensure they are accurate, clear and focused.

These efforts will provide for a more secure environment for sensitive data used in VA. Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.

Prepared Statement of

Robert J. Brandewie
Director, Defense Manpower Data Center

Before the House Committee on Veterans' Affairs

Oversight Hearing on the Department of Veterans Affairs Information Technology Infrastructure Reorganization

June 28, 2006

· **publication until released by the Committee**

Chairman Buyer and Members of the Committee, thank you for the opportunity to appear before you today to discuss the data exchanges between the Department of Defense (DoD) and the Department of Veterans Affairs (DVA). I would also like to include an overview of our actions in identifying Active Duty, National Guard, and Reserve members whose information may have been present on a laptop computer stolen from a DVA employee's home and briefly discuss some of the data security measures we employ.

As a prelude to discussing the data exchanges, I would like to note that the Defense Manpower Data Center (DMDC) is the central repository of automated human resource information within DoD. We receive and maintain personnel data on Active Duty and reserve component military members, retired Service members, civilian employees of the Department, some DoD contractors, and many family members. This data is used as the basis for issuance of member and dependent ID cards, eligibility for benefits such as medical care, and to conduct operational programs such as identity management and the Montgomery GI Bill program. Thus, DMDC is at the center of most of the human resource information flowing between DoD and the DVA. It is important to note that other parts of the DoD also exchange information (for example medical records) with DVA, but that the most comprehensive exchanges occur between DMDC and DVA. These exchanges are very basic to providing an improved experience for the veteran and also to coordination of benefits between the two Departments. These exchanges have been going on for more than 25 years.

The purpose of the data exchanges between DVA and DMDC are twofold—to provide information to the DVA on currently serving and recently separated individuals who are eligible for DVA benefits and services, and to competently administer programs in both agencies that benefit Service members, former Service members, and their families. In accordance with the Privacy Act, these data exchanges are disclosed in various Computer Matching Agreements and are in the Federal Register under Systems Notices S322.10 and S322.50. The exchanges can be categorized as follows:

- **Data for administering educational programs:** Data is exchanged on participants in both the Active Duty and Selected Reserve Montgomery GI Bill programs. Data exchanges are also being initiated for Guard and Reserve personnel who served in support of a contingency and for the National Call to Service programs recently established by the Congress.

- **Data for administering insurance programs:** Data is exchanged on medically retired members with service disabilities and recently separated Reservists so they can be notified of their eligibility for Veteran's Group Life Insurance.

- **Data for assessing post-war illnesses:** Data is exchanged on separated Active Duty members and Guard/Reserve members coming off Active Duty who have served in the first Gulf War and in Operations Iraqi Freedom/Enduring Freedom for purposes of post deployment medical assessments.

- **Data for prevention of fraud, waste, and abuse:** Data is exchanged to ensure correct pay amounts and offsets for veterans receiving DVA compensation benefits as well as to prevent the member from inappropriately receiving compensation from DoD and DVA simultaneously.

- **Data to estimate veteran population and expedite delivery of benefits:** Data is provided to DVA on Active Duty enlisted and Guard/Reserve accessions so DVA can establish a skeletal record at time of entry and verify their DoD affiliation. DMDC subsequently provides DVA with additional detailed information at the time a member separates or retires.

Data exchanges with the DVA, although long standing, have been expanded in breadth in recent years and an effort to consolidate the exchanges began in earnest about three years ago. Close cooperation and increased exchanges of information have also received encouragement from the Congress and the Administration. Public Law 107-347 established the Office of Electronic Government in the Office of Management and Budget (OMB). OMB oversees the President's Management Agenda and had an agenda initiative in 2002 to ". . . improve coordination of health care and eliminate potentially duplicative budgeting by sharing data between VA and DoD." Additionally, the President's Management Agenda directed efforts to make the transition from DoD to the DVA seamless – " Transition should be seamless from the veteran's perspective and could be made seamless through data sharing between VA and DoD,

as well as within VA" (page 70). Public Law 108-136 established an interagency committee known as the DVA-DoD Joint Executive Council to direct joint coordination and data sharing efforts between the two Departments. As a result, DoD and DVA have been working an initiative to obtain full interoperability between appropriate DVA and DoD automated systems to enhance the transfer of data and the delivery of benefits. At the current time, some information is flowing machine-to-machine between DMDC and the DVA's One VA initiative known as the VA/DoD Identity Repository (VADIR). All data exchanges are scheduled to be consolidated and near real-time in 2008.

DoD believes that there is great value to current Service members and veterans in the close cooperation, evidenced by these data exchanges, that has developed between DoD and the Department of Veterans' Affairs. However, it is equally important that the exchanges are done with the utmost attention to security to ensure no unauthorized disclosure of information. Current DoD policy requires that Privacy Act and other sensitive but unclassified information be protected while being transmitted. DoD and DVA have taken a number of steps to ensure that the information we exchange remains safe from unauthorized disclosure. In keeping with DoD policy, in June 2003 DMDC established a policy that all data exchanges that contain privacy protected information would be done using secure technologies. These technologies include data encryption, the use of Virtual Private Networks (VPN), and the use of commercial secure transfer services like Connect:Direct. This policy would apply both to information transfers within the Department and between sister agencies. The DVA was a partner in the implementation of secure transfer and we have continued to add security to our transfer process. Most recently both agencies migrated to a new version of Connect:Direct - Secure+. This product adds data encryption services to its existing secure transfer technology.

I will now turn and discuss our actions resulting from the theft of data on a laptop computer from a DVA employees' home. On June 1, DMDC was requested to match the Social Security Numbers (SSN) of individuals that may have been present on the stolen computer against current Active Duty and Reserve and Guard personnel files.

The stolen data may have included data extracted from the DVA's Beneficiary Identification and Records Locator Subsystem or BIRLS file. We knew that the accession data we provide to DVA was included on the BIRLS database and began working with DVA Headquarters and their Austin, TX center. On June 2, Austin sent us 19.6 million records—those with SSNs—from the compromised BIRLS extract over a secure connection. Over the weekend of June 3-4, we matched SSNs from the 19.6 million BIRLS extract records against our master database of about 27 million records and found a large number of Active Duty, National Guard, and Reserve members in the BIRLS extract.

On June 5, we validated our work by matching the two large datasets once again and early on June 6 confirmed the results. The numbers were provided to the leadership of DoD and to DVA on June 6 and SSN level detailed records were provided to each of the Military Services on June 8. We also received from the DVA's Austin center about 6.8 million records from the BIRLS extract file that did not have SSNs and have matched a few of them to Active Duty, Guard and Reserve members. In addition, we used the data provided by VA to identify other members of the DoD community (civilian employees, retirees, etc.) potentially impacted by the data loss. We also examined the impact on dependents of DoD members.

Over the next several days, we worked with DVA to refine the list of SSNs that were stolen. They indicated that some SSNs on the BIRLS extract were not compromised and some SSNs not on BIRLS were. They provided these new datasets to us and we refined the list of individuals whose data was stolen. The final numbers show about approximately 1.1 million currently serving Active Duty, 415, 000 Guard, and 633,000 Reserve members were potentially impacted. Of these, about 146,000 Active Duty, 34,000 Guardsmen, and 25,000 Reservists are currently serving in Operation Enduring Freedom or Operation Iraqi Freedom.

We continue to work closely with the VA on mitigation efforts with respect to the compromised information. Our leadership in the Office of the Under Secretary of

Defense (Personnel and Readiness) has given their full support and we have offered the resources of the DMDC where they can be helpful. In spite of this tragic loss, it is important to reinforce the point that there are many benefits to the current data exchanges between the two Departments, they are done securely, and they result in better service and benefit delivery for Service members and veterans.

Mr. Chairman I thank the committee for the opportunity to report on data exchanges between the DoD and the DVA and would welcome the opportunity to answer any questions.

Written Testimony
Jim Bresson
Vice President and Managing Partner, Gartner Consulting

Mr. Chairman, Mr. Vice Chairman, and Members of the Committee:

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

I am a Managing Partner within the consulting division at Gartner, the leading provider of research and analysis on the global IT industry. Unlike many of our competitors, Gartner does not offer IT systems or software 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, and I am frequently partnered directly with Senior Executive Service and General Officer leaders aiming to transform their IT organizations. During the past six years I have supported several large federal government departments and agencies faced with the challenges of:

- Enterprising their mission support applications, IT infrastructure and services;
- Improving their program performance management; and
- Meeting shared services and/or constituent/citizen service expectations.

I am accompanied by my colleague, Joe Clarke, who is an expert in the methodologies we employed during our most recent engagement with VA. I suspect Mr. Clarke may be able to help us answer any questions seeking specific details that might arise in the course of our dialogue this morning.

Background

My colleague, Michael Pedersen, previously provided testimony to this committee last September 14, 2005. His testimony at that time responded to the Committee's request for information regarding Gartner Consulting's study delivered last spring 2005, and its recommendations on the reorganization of VA's IT infrastructure.

To recap the highlights of Gartner Consulting's previous testimony, the Committee may recall that we believe changing the VA's IT 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

Gartner is a trademark of Gartner, Inc. or its affiliates
28 June 2006
© 2006 Gartner, Inc. and/or its affiliates
All rights reserved

7. Culture and Norms — the changes required in the underlying culture and norms to effect behavior change.

We provided elaboration on each of these dimensions; and it is our professional opinion that VA's overall IT get well strategy must address each of these dimensions.

For the first dimension - Organizational Structure - we identified two models as having 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.

Additionally, we presented our assessment of the benefits and risks related to each model. Subsequently, we provided rationale for our recommendation that VA pursue the Centralized model option:

> *"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."*

We regret that subsequent – and current – dialogue appears only to focus on this singular dimension, possibly to the exclusion of the other dimensions. **Gartner Consulting reaffirms our professional opinion that VA's overall IT get well strategy must address <u>each of these dimensions</u>.**

Significant Events Since Our Previous Testimony

Subsequent to our delivery of engagement results and recommendations to the VA last spring 2005, which concluded Gartner Consulting's engagement with VA, the Secretary of the VA (SECVA) issued an Executive Decision Memorandum (EDM) in October 2005. That EDM approved the concept of a Federated IT Management System for the VA and charged the Assistant Secretary for IT with the development of a Federated Model to be used as the foundation for development of a more detailed implementation plan and execution details.

In December 2005, VA awarded a competitive contract to Technatomy Corporation (Technatomy), a Service Disabled Veteran-Owned Small Business, to convert the existing centralized model previously provided by Gartner Consulting (then as subcontractor to Topgallant Partners) to a federated model. Technatomy partnered with Gartner Consulting as its sub contractor to convert the centralized model to a federated model in accordance with the contract award. Additionally, VA's award to Technatomy sought support for the development of a Statement of Work, with traceability to the Federated Model, as the basis for a future solicitation seeking a third party IT Realignment implementation plan services provider

The Technatomy/Gartner Consulting team performed the desired conversion to the federated model and delivered its results to VA in February 2006. This team subsequently supported development of the components for the aforementioned future solicitation package, and concluded our engagement with VA in March 2006.

I was the lead consultant for the model conversion effort, and I formed a team of Gartner Consulting subject matter experts to perform this conversion. In close collaboration with our Technatomy program manager, I directed the team's activities to fulfill the contract objectives and to deliver VA's desired results.

Gartner is a trademark of Gartner, Inc. or its affiliates.

© 2006 Gartner, Inc. and/or its affiliates.
All rights reserved.

The balance of my testimony provides a description of our model conversion approach and task execution. This information is drawn directly from the detailed project deliverable submitted to the VA, and was presented to the Assistant Secretary for IT and the Deputy Assistant Secretary for IT. Subsequently, at the request of the Deputy Secretary (DEPSECVA), this information was presented for discussion with him, joined by the VA Administrations' Undersecretaries and the Assistant Secretaries representing the Staff Offices.

Principles of the Federated Model

Within the Operations & Maintenance Domain the VA Office of the Chief Information Officer (OCIO) has primary authority over processes. The Administrations, Staff Offices and Staff Organizations are required to perform supporting roles in many of the processes. The supporting roles are usually related to specific business needs.

VA OCIO retains control over the Development Domain for OneVA Enterprise business applications. In addition, VA OCIO may control business application development for the Administrations and Staff Offices or Organizations that desire to take advantage of the economies of scale associated with that centralized development capability.

Those applications which are business unit specific (e.g., VistA) remain under the limited control of that particular Administration, Staff Office or Staff Organization. In some cases, the business unit has relinquished the development responsibility to the VA OCIO.

Even when Business Application Management has been delegated to an Administration, Staff Office or Staff Organization, the VA OCIO still retains oversight responsibilities in accordance with the Clinger-Cohen Act.

Our Approach to the VA's Federated IT Model

In response to the VA's contract requirements and heeding the DEPSECVA's direction to Gartner to determine the best approach to implement a federated model for VA, the Technatomy/Gartner Consulting team leveraged previous Topgallant Partners/Gartner Consulting deliverables and focused our model conversion effort on the interactions between the VA CIO and the Administrations, the Staff Offices, and the Staff Organizations (for IT operation and maintenance and CIO oversight activities).

Based on the conclusions of the previous engagement, this conversion team understood that within the VA's current environment role specialization, centralized functions, common methodology, reusability, and standardization are viewed as risky because these methods decrease the perceived power any one individual has over his or her own work. Consequently, we applied several of Gartner's frameworks in an effort to rely on industry standard best practices, Gartner Research, Gartner, Inc. and MIT Sloan Center for Information Systems Research (Broadbent and Weill), and minimize perceived loss of control by individual actors, including:

- IT Process Reference Architecture
- Performance-Based Management
- IT Human Capital Management.
- IT Job Families and Role Design
- IT Process Governance

The new Federated Model also presents an optimum design for the Office of the CIO and its subordinate organizations aimed at delineating the mission, responsibilities, authorities and accountabilities of each organization, and the business practices and processes that eliminate duplication, streamline operations and promote organizational efficiencies.

The relationship between the operational and management responsibilities of the VA CIO and the application development responsibilities of the Administrations, the Staff Offices, and Staff Organizations were defined by the process flows that require exchanges of information in order to deliver consistent, repeatable services and effective IT controls, and by the governance roles and responsibilities shared

Gartner is a trademark of Gartner, Inc. or its affiliates
28 June 2006
© 2006 Gartner, Inc. and/or its affiliates
All rights reserved.

between these organizations. Simply stated, **process is the linchpin to delivering consistent, repeatable services and effective IT controls**.

Linking Development with Operation & Maintenance

The Gartner definitions of the Development and Operation & Maintenance domains highlight the need for coordinated activities between developers and operations.

In a Federated Model activities are coordinated by process flows that must be clearly defined to reflect the critical interdependence of business applications and the performance of the IT infrastructure.

Both domains must be involved early in the application life cycle to plan for and ensure high performance and service quality after an application goes into production.

IT Process Flows

The federated model has been selected by many organizations for the delivery of IT services. The most typical variation of the model involves designating shared services that will be centrally managed to optimize service levels and efficiency

The VA has decided to structure its federated model using two domains: Development and Operations and Maintenance. Definitions of both domains have been developed.

Interaction between the domains must be coordinated throughout the life cycle to ensure that IT solutions are developed and delivered in a controlled fashion. This coordination is accomplished by specifying the processes that will be used to manage the delivery of IT services. The processes have been grouped into five areas:

- Enterprise Management
- Business Management
- Business Application Management
- Infrastructure Operations
- Service Support

A detailed framework has been developed to define the processes and activities that must be coordinated between the Development and Operations and Maintenance Domains. That process framework leverages the best practices of the IT industry and establishes the parameters within which IT services will be managed at the VA.

Process Flows Throughout the System Development Life Cycle

Both domains, Development and Operation & Maintenance, play critical roles throughout the System Development Life Cycle (SDLC) and defining those responsibilities depends on the processes involved. The following four functional areas each have differing levels of responsibility for both domains:

- Enterprise Management – Processes required to provide enterprise-wide standards for IT services, including:
  - Security Management
  - Project Management
  - Quality Management
  - Enterprise Architecture Management
  - Strategic Planning
  - Corporate Performance Management.
- Business Management – Processes for business relationship management and financial management of IT resources, including:
  - Business Relationship Management
  - Service Level Management
  - Financial Management
  - Contract Management
  - Business Continuity Management
  - Contractor Management.

Gartner is a trademark of Gartner, Inc. or its affiliates
28 June 2006
© 2006 Gartner, Inc and/or its affiliates.
All rights reserved.

- Business Application Management – Development of applications to meet business requirements, including:
  - Business Needs Management
  - Requirement Definition Management
  - Software Lifecycle Management.
  - Test Management
  - Implementation Management
- IT Operations – Processes associated with both Infrastructure Operations and Service Support, including:
  - Infrastructure Planning
  - Infrastructure & Applications Management
  - Capacity Management
  - SLA Administration
  - Performance Management
  - Production Control
  - Database Management
  - Disk and Tape Management
  - Facilities Management
  - Change Management
  - Configuration Management
  - Inventory Management
  - Incident Management
  - Problem Management
  - Service Request management
  - Release Management.

Sample Scenarios

The Technatomy/Gartner Consulting team developed three separate scenarios to illustrate the day to day operation of the federated model in the future VA environment.

The three scenarios were (a) a minor enhancement to an application, (b) the introduction of new functionality, and (c) a major enhancement. Each scenario shows the required coordination and interaction between the two VA domains (Development and Operations and Maintenance) throughout the life cycles of these modifications.

IT activities performed within these scenarios include Service Support processes (including incident management, problem management, and change management), Enterprise Management processes (including project management, quality management, and security management), Business Application Management processes (including software lifecycle management, O&M support, test support, and test management), Infrastructure Operations processes (including infrastructure planning, facilities management, and database management), and a critical loop back to Service Support processes.

Generally, as the magnitude of the enhancement increases, additional processes and/or actors in the system are involved.

The scenarios also illustrate the similarities among the three types of changes. Many of the same process steps must be performed regardless of the size of the required modification.

VA OCIO Organizational Structure

The Technatomy/Gartner Consulting team developed an OCIO organizational design that aligns with the process flows required for a federated model.

The OCIO organizational design balances the tactical needs of operating a complex infrastructure as a shared service and the strategic needs of aligning IT resources to best meet the mission requirements of the Department.

The description of the mission of the organizational element as well as the key attributes have been developed for each component of the VA OCIO.

Gartner is a trademark of Gartner, Inc or its affiliates.
28 June 2006
© 2006 Gartner, Inc. and/or its affiliates.
All rights reserved.

The OCIO organizational design represents a desired End State based on best practices in the industry and government. It is recognized that a near term transition from current business practices to End State is necessary.

VA IT Job Families

A Job Family is a group of similar skills, knowledge, and abilities/behaviors that focuses on the role a person plays in providing services.

IT job families have been defined based on Gartner research into IT related jobs in both industry and government.

Based upon the process flows and the organizational design it is possible to define the IT job families that are appropriate for each element of the VA OCIO design.

Based on the defined interaction between the VA OCIO and the Administrations, Staff Offices, and Staff Organizations it is possible to define the IT job families that are appropriate of the VA offices.

General characteristics, included competencies, and typical roles for each of the IT job families have been included in the appendix to the report.

IT Process Governance

A critical success factor for any process framework is a clearly defined governance structure that differentiates between advisory and management responsibilities.

Governance concerns:

- What decisions are made
- Who has input or decision rights
- How IT decisions are made
- Why are the decisions made

The delivered Federated Information Technology System Model specifies input rights and decision rights for each activity.

The benefits of effective governance of the Federated Information Technology System Model relate directly to accomplishing the mission of the Department and can form the basis for effective performance management metrics.

Mr. Chairman, Mr. Vice Chairman, and members of the Committee, 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 Committee may have at this time.

Gartner is a trademark of Gartner, Inc or its affiliates.

© 2006 Gartner, Inc and/or its affiliates.
All rights reserved.