ROBERT T. HOWARD ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF

ROBERT T. HOWARD
ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
United States Senate
September 19, 2007
**

Thank you, Mr. Chairman. I would like to thank you for the opportunity to testify on the current status of the VA Office of Information & Technology's (OIT) reorganization and it's impact on the delivery of healthcare and benefits; the effect of enhanced VA IT security policies and procedures on healthcare and benefits delivery; the status of asset management/inventory control for IT systems; the legacy system transition; joint in-patient record systems; and unresolved problems identified during the realignment. These are all very important issues that need to be addressed. To assist in discussing these issues today, I am accompanied by:

- Dr. Paul Tibbits, my Deputy Chief Information Officer for Enterprise Development,
• Mr. Ray Sullivan, my Director of Field Operations

First, I would like to thank you Mr. Chairman for being the catalyst for establishing my top priorities as Assistant Secretary for the Office of Information and Technology. They were developed in response to a nomination post-hearing question presented by you back in September of last year. At the time of your question the paper was blank so I thank you for prompting me to develop what has turned out to be very helpful and extremely important priority statements.

These priorities are guiding the realignment process we see taking place today. There are seven of them. Briefly, they include (1) establishing a well-led, high performing, IT organization that delivers responsive IT support to the three Administrations and Central Office staff sections; (2) standardizing IT infrastructure and IT business processes throughout VA; (3) establishing programs that make VA's IT system more interoperable and compatible;
(4) effectively managing the VA IT appropriation to ensure sustainment and modernization of our IT infrastructure and more focused application development to meet increasing and changing requirements of our business units;
(5) strengthening information security controls within VA and among our contractors in order to substantially reduce the risk of unauthorized exposure of veteran or VA employee sensitive personal information; (6) creating an environment of vigilance and awareness to the risks of compromising veteran or employee sensitive personal information within the VA by integrating security awareness into daily activities; and (7) remedying the Department's longstanding IT

material weaknesses relating to a general lack of security controls. I assure you that we are working hard to give these priorities the required attention.

As you know, the Secretary approved the department's new organization structure in 2007, and we've set a goal to complete the realignment by July 2008. We have transferred over 6,000 employees to the Office of Information and Technology. This, along with the centralized IT appropriation and delegation of authority for FISMA provides a unique opportunity to significantly improve IT activities within VA. Another critical element in that regard is the full commitment from VA's leadership to make this reorganization successful.

I have provided an organization chart for your reference throughout the hearing. In addition to five additional deputies, we have an IT Oversight and Compliance capability and a Quality and Performance office. We also have implemented a new IT governance plan which establishes the processes, responsibilities and authorities required to manage VA's IT resources. The GAO recently released a report on our realignment progress and correctly identified that there is more work to be done to have a successful transition from a decentralized to a centralized organization. We have already begun implementing some of their recommendations

Clearly an important question associated with this realignment is how has it impacted the delivery of healthcare and benefits to our veterans. In my opinion, there has been no significant change in these two areas-which was a key objective of this reorganization - to do no harm. This is not to say we have not had problems - we have. But we have also experienced improvements in our ability to gain knowledge over IT activities that were not very visible in the past, in IT funding details across the VA, and in our ability to protect the sensitive information of our veterans.

An area in which information protection has dramatically improved is incident response. VA has encrypted over 18,000 laptop computers, and has implemented procedures for issuing encrypted portable data storage devices. This month, the Department is procuring software to address the encryption of data at rest. And just last week we awarded a contract for an extensive port monitoring capability which will help us better control what devices can access our network. At the same time, VA continues to increase self-reporting security and privacy violations and incidents. This trend is a direct, positive outcome of the significant amount of policy, guidance, and training conducted on information protection over the past year and a half.

Since the May 2006 data breach, the VA staff is now more aware of the importance of protecting our veterans' and employees' information and identities. While we do have a way to go here, I have definitely seen improvement. The Department has also undertaken a concerted effort to reduce the use of social security numbers and to review and eliminate a significant amount of personally identifiable information VA currently holds. To that end, VA has drafted two documents outlining plans to achieve both these goals. These plans were developed in accordance with OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" and will be included in this year's FISMA report. Regarding the FISMA report, not only will we submit one this year, (we got an incomplete last year), but we have, for the first time, completed testing of over 10,000 security controls on our 603 computer systems.

We are also addressing some critical problem areas. As you know, the House Veterans Affairs Oversight & Investigations Committee recently held a hearing on VA's IT asset management based on a GAO report (report 07-505) which found inadequate controls and risk associated with theft, loss, and misappropriation of IT equipment at selected VA locations. In that report, GAO found many problems regarding the IT asset management environment and included a number of important recommendations - with which we agree and are implementing. We have completed a handbook on the Control of Information Technology Equipment within the VA which includes each of the recommendations made by GAO in its report. These documents are now being finalized within the Department, but we have already implemented the procedures they describe. They will provide clear direction on all aspects of IT asset management.

For the past six months, tightening IT inventory control throughout VA has been the focus of a cross-functional Tiger Team. Types of equipment to be inventoried are black berries, thumb drives, cell phones, etc. In addition, VA has issued a memorandum requiring each VA facility to complete, by the end of December of this year, a wall-to-wall inventory of all IT equipment assets, including sensitive items, regardless of cost. Reporting requirements have been established at the Facility, Regional and Field Operations levels to ensure that issues are identified and addressed early in the process. By way of support, we have established an IT Inventory Control Knowledge Center that is accessible by all VA personnel. This website provides references, templates, definitions, frequently asked questions and a link to contact the Tiger Team directly. Also, the Office of Oversight and Compliance is working with Tiger Team members to develop a compliance checklist that will be used for scheduled and unscheduled audits regarding IT assets. This initial inventory will help provide a VA IT asset baseline-something that has not existed before.

We have also made progress in the evolution of our healthcare and benefits systems and in improving ties with DoD. The work with DoD has been most helpful in the area of data sharing and data standardization. We are moving our healthcare system from a hospital-centric model to a patient-centric approach. This approach will ultimately allow veterans and their care providers to access seamless health records and information at any time, regardless of location. This modernization will utilize a central IT architecture and a six-phase transition plan to be completed by 2015.

The existing portfolio of VBA applications are based on various legacy technologies, most of which are not web-based. These legacy applications are more expensive in that they require more intensive support since they rely on outdated software. To remedy this, VBA has established an application architecture blueprint to be used for all applications. A pilot is being performed for the Benefits Delivery Network (BDN) Re-host program to migrate the legacy system to a more modern browser-based environment.

In closing, I want to assure you Mr. Chairman that we will remain focused in our efforts to improve all aspects of the Information Technology environment in the VA and to make sure that we do not negatively impact the delivery of healthcare or benefits in the process but instead begin to see steady improvements in modernizing both our healthcare and benefits IT environments. Thank you for your time and the opportunity to speak on this issue. We would be happy to answer any questions you may have.