House Veterans Affairs Committee
June 29, 2006

Hon. Gordon H. Mansfield
Deputy Secretary of Veterans Affairs
****
6/27/2006 4:34 PM

Mr. Chairman and Members of the Committee. Thank you for this opportunity to appear before the House Committee on Veterans Affairs.

The Secretary has acted decisively to determine the scope of the loss of data, ascertain its impact and act affirmatively to address what we must do to protect our veterans. He has directed changes that will affect the culture of this department and has moved information security to the forefront of our consciousness.

This loss was tragic on many levels, but it is important to note that the data that was stolen was a copy of other data that is still in VA's possession i.e. it was not a loss to the VA.

As has been noted in previous hearings, it is useful to discuss our efforts in a few basic parts: (1) what we have done; (2) what we are doing; (3) what needs to be done; and (4) how we will measure our progress. The Secretary has stressed to senior staff that, our goal, is to have the VA be the *Gold Standard* in the realm of cyber and information security, just as it has become in the realm of electronic medical records and the delivery of healthcare to veterans.

What we have done

Following the theft of data from a VA employee's home, we retained forensic experts to determine the extent of potential loss. Once the magnitude of the loss was more fully understood, we have been working non-stop to take steps as appropriate – going forward – to protect our veterans.

As previously announced, the Secretary has:

- Implemented a series of personnel changes in the Office of Policy and Planning, where the breach occurred. Recently-retired Admiral Patrick Dunne has been nominated by the President to be Assistant Secretary for Policy and Planning. With his confirmation, he will bring the much needed leadership to that office. Admiral Dunne is working now at VA as a consultant.

- Has retained Richard Romley as an outside, independent advisor to the Secretary. He has significant experience in data theft, governmental reorganization and critical issue development. As a former prosecutor, Rick has a reputation for independence and a unique ability to get to the bottom of issues.

- Has expedited completion of Cyber Security Awareness Training and Privacy Awareness Training for all VA employees. He has directed that all employees have this training prior to the end of June.

- He has directed that VA facilities across the country – every hospital, Community-Based Outpatient Clinic (CBOC), regional office, national cemetery, field office and VA's Central Office – observe Security Awareness Week which began Monday, June 26th. Throughout this week, each office will focus on different aspects of cyber and information security, how those pertain to their particular operation, and how to assure that security is an integral part of the work place ethic.

- VA's initial response to the data loss was to mail over 17.5 million letters advising individuals of this data loss, and providing them with a toll free number which will outline proactive steps they can take to protect themselves. This call center immediately provided the capacity to handle up to an additional 260,000 calls a day. The volume of calls has been less than we expected.

What we are doing – Specific Actions

At a recent press conference, the Secretary announced that VA would be providing free credit monitoring to all affected veterans who sought that service. That service will also include an insurance component to help minimize any personal out of pocket expenses, should a veteran's identity be compromised as a result of this loss. We were preparing to issue a request for proposals to vendors capable of providing this service. Last Friday, the Federal District Court in Kentucky hearing one of the class action lawsuits emanating from this data theft, issued a Temporary Restraining Order barring the government from publicizing its free credit monitoring offer to veterans whose personal data was stolen.

The Secretary has also directed that every laptop computer in VA undergo a security review to ensure that all security and virus software is current, including the immediate removal of any unauthorized information or software and the application of appropriate encryption programs. But, because of the pending lawsuits, this directive has been placed on hold until we obtain guidance from the courts.

In addition, we have been in discussions with corporations which provide unique data breach analysis to see if data is being exploited and we anticipate entering into a contract shortly for this service.

We are making an effort to be responsive to concerns, expressed at a recent hearing, that we provide "detection, protection and insurance," essentially a credit protection and resolution package, for those possibly affected. It is appropriate that we do this.

The Secretary has directed that VA conduct an inventory of all positions requiring access to sensitive VA data by August 31, 2006, to ensure that only those employees who need such access to do their jobs have it. And we will be developing the procedures necessary to assure that employees have an appropriate level of background check in place, and that those be updated on a regular basis. For example, the employee from whom data was stolen had not had a background investigation for 32 years.

As the chief operating officer of the Department;

- I have overseen issuance of IT Directive 06-1, *Data Security-Assessment and Strengthening of Controls o*n May 24, 2006. This directs all three VA administrations and staff offices to review existing internal methods of storing, transmitting and protecting sensitive data. It also calls for a review of current procedures and VA-wide actions to date through a series of briefings attended by key departmental officials during the months of May and June.
- I have reviewed Directive 07-10. This is as system of determining what time of background check and information access is necessary per occupation title.
- I have overseen the issuance of VA Directive 6504 on June 12, 2006. This directive provided policy regarding transmission, transportation and use of, and access to, VA data outside VA facilities.
- Along with internal actions, I communicated the Department's actions with various Members of Congress and their staffs-to include coming here to discuss matters with committee staff.

What we are doing – Major IT Reorganization within VA

In October 2005 the Secretary issued a directive to implement the reorganization of IT within VA. Pursuant to that reorganization, more than 4,610 IT professionals engaged in operations and maintenance of the Department's IT infrastructure, plus 560 unencumbered positions, have been detailed to the Office of

Information and Technology, under the direction of the Chief Information Officer. As of the beginning of the new Fiscal Year on October 1, 2006, those details will become permanent, thereby establishing a new career field within OIT.

In this IT reorganization, all IT professionals are being consolidated into the Office of Information and Technology, except for certain Development Domain personnel in VHA and VBA. These developers will also be brought under the control of the CIO as well.

They will look to the CIO for:

1. Budget Direction/ and OMB exhibit 300
2. Security Requirements
3. System Standards; and
4. Enterprise Architecture Requirements

Other major milestones include the establishment of the position of Chief Financial Officer with budget authority in the Office of Information and Technology. This new office is being established to give the CIO control over all Departmental IT funds.

Security has been centralized under the CIO. All Department Information Security Officers (ISOs) have been detailed to the CIO

This situation has highlighted for us the fact that we have not had the right policies, procedures, guidelines, regulations and directives in place – with the teeth to enforce them – to assure that those nominally responsible for security could effectively do their job. This is why the Department has acted aggressively in implementing stronger administrative procedures.

For example, the IT operation today has evolved over time and has included the services of many talented and dedicated professionals. Their efforts are paying off. For example, in terms of cyber security, VA IT systems are:

1. Certified

2. Accredited, and
3. External independent gateways have been reduced.

We will continue to implement IG recommendations as warranted.

What we are doing – IT Assessment

The range of IT programs administered by the Department on behalf of our veteran clientele is extensive. As a result, the array of hardware and software, where it is located, the number of systems, the number of persons having access to data, how that access is granted or denied, how the data is utilized and by whom, what background checks are needed – all have grown tremendously over the years. These are areas that require out immediate review, and, where necessary, remediation.

This theft of VA data has been a wake up call to all of us—at VA and in government in general. IG reports in the past years have highlighted specific weaknesses, but as an institution, VA did not respond to those with the sense of urgency that, in retrospect, was called for. With benefit of hindsight, that need for urgency is overwhelmingly apparent today. We recognize that we must change the culture of the Department, and we have embarked on doing just that.

We have also directed that previously authorized work procedures which allowed employees to transport hard copies of claims folders to alternative work sites be stopped. It is a government-wide practice to encourage telework or telecommuting, especially in the Washington metropolitan area. Yet we must assure that our policies and procedures implementing this are such that sensitive data relating to our veterans is properly protected. Our Acting Undersecretary for Benefits is to review and revise his own guidance to his staff in this area to ensure the protection of veterans' vital records and sensitive data prior to resuming this practice, if at all.

What we are doing – Regulations and Guidelines

We are working to assure that we have clear guidance for all VA employees in place, and that they are aware of what is required of them – and of the consequences, should they fail to adhere to that guidance, which sets forth the guidelines for information security and the enforcement mechanisms pertaining to that. This document is designed to eliminate any confusion as to what is expected of Departmental employees concerning security of data.

Measurement of Success

How will we measure our success in this endeavor?

One measure of success is to correct deficiencies noted by the IG in the past.

Additionally, we will improve our FISMA compliance. As I noted, in the past we received an "F" on the FISMA scorecard. That is unacceptable, and we must do better in the future.

And we will continue to communicate with VA employees that which is expected of them to comply with information and data security.

What needs to be done – Legislation

The Health Insurance Portability and Accountability Act (HIPAA) governs all aspects of the privacy of sensitive information pertaining to an individual's health. HIPAA provides for criminal penalties of up to 20 years imprisonment and a fine of up to $250,000 for intentional misuse of health information for private gain.

There is no comparable law pertaining to the misuse of other non-health, sensitive, personal information, and I echo the Secretary's call that the Congress should enact such a law. Someone intent on fraudulently using personal information may think twice if he or she focuses on severe penalties that could be encountered for such a crime.

Conclusion

Mr. Chairman, the fixes we have outlined won't be easy, and it won't be overnight, but I am absolutely convinced that we can do it. We have as goal to become the "Gold standard" just as it has become the 'model' for health care in the United States.

Mr. Chairman, that concludes my testimony.

# # #