The Honorable R. James Nicholson, Secretary, Department of Veterans Affairs, Washington, D.C. Accompanied by: Mr. Robert Howard, Senior Advisor to the Deputy Secretary, Department of Veterans Affairs, Washington, D.C.; The Honorable Tim McClain, General Counsel, Department of Veterans Affairs, Washington, D.C.; The Honorable Robert Henke, Assistant Secretary for Management, Department of Veterans Affairs, Washington, DC

Written Statement of
The Hon. R. James Nicholson
Secretary of the Department of Veterans Affairs
Senate Veterans' Affairs Committee
July 20, 2006
**

Mr. Chairman and Members of the Committee.

Thank you for the opportunity to appear before you to follow up on what occurred within the Department of Veterans Affairs since the unfortunate theft of computer equipment containing VA data from the home of a VA employee on May 3rd. I appeared before you at a hearing on May 25th to tell you of what I knew about this situation at that time. Since then, much has happened.

On Thursday, June 29, 2006, I announced that federal law enforcement authorities had recovered the stolen laptop and external hard drive. The FBI's forensic examination of the recovered laptop and hard drive is complete. The FBI has a high degree of confidence -- based on the results of the forensic tests and other information gathered during the investigation that the data contained on that equipment was not accessed or compromised.

This is good news for our veterans and active duty military personnel and should alleviate any concerns they may have. But, identity theft is the fastest growing white-collar crime in this country, and it is important that we remain vigilant. For that reason, we will be retaining the services of a company that specializes in data breach analysis to monitor this situation.

I know the members of this Committee have digested the VA Inspector General's report on events related to the data breach.

I concur with the recommendations contained in the Inspector General's report, and am fully committed to seeing them implemented in the shortest possible time. Last October I approved a major restructuring of information security within the Department, centralizing almost all of it under the Chief Information Officer. This process was, and of course, still is underway and will greatly facilitate control, training, responsibility and accountability. This consolidation of IT has been accelerated as a result of this incident. There have been several changes that have already been implemented, and, as we continue this effort, we can make VA the ?Gold Standard? in the area of information security. VA has made great strides forward in the area of health care and today is the recognized leader in health records and safety and is setting the standards for others to follow. I am committed to doing the same in the area of information security.

We are formulating an action plan that is a multi-phased effort which includes actions in the technical area such as encryption processes and tools; actions in the management area such as a complete overhaul of policies and directives; and actions focused on operational areas such as procedures and tools for monitoring the extraction of sensitive information.

On June 28, 2006 I issued a memorandum delegating to the VA Chief Information Officer (CIO) all authority and responsibilities given to me by the Federal Information Security Management Act (FISMA.) This delegation does not relieve me of the ultimate responsibility but it does empower the CIO with the authority he needs.

This delegation restructures responsibilities and authorities for information security at the VA, bringing them together in one individual. It also is the first step in bringing about the cultural changes within VA generally, and more particularly, within IT at VA, that must occur. I have made it clear to all senior managers in the Department that information security, cyber security and the reorganization of the Office of Information Technology (OIT) are top priorities. These senior leaders know that every employee must be committed to ensure the security of veterans' personal information. Performance evaluations and executive bonuses will reflect the leaders' and employees' level of commitment.

When I commit to becoming the ?Gold Standard,? I mean VA must be the best in the federal government in protecting personal and health information, training and educating our employees to achieve that goal. The culture must put the custody of veterans' personal information first ? over and above expediency. I expect nothing less.

The IG Report has highlighted serious deficiencies. We have a plan for transformation. I realize, however, the recommendations contained in this report are just a start. Achieving our goal of leadership will require much more.

I have reached outside our ranks and enlisted the assistance of leading experts in the field of data security to assist us in defining our path. With their guidance and VA resources, we will become the system for all other agencies to emulate.

Training in the area of information and cyber security will be a vital component of our transformation. To ensure quality and consistency in such a broad-based training program, I have directed the establishment of a new Office of Cyber & Information Security Training within the Office of Information Technology.

This office will be responsible for developing and implementing a training program which will begin with new employee orientation and continue through such programs as Leadership VA, the SES Candidate Development Program and the Senior Leadership Academy. I expect a continual emphasis on information security throughout an employee's career.

Excellence in information security will take the full commitment of VA's senior leadership, both political appointees and career senior executives. It will take time, but my sense of urgency is clear.

Measurable progress will require a steady and consistent message for ? and from ? all who work for this agency.

Industry experts will help our own IT professionals develop program changes and validate our timelines. Employees will be held accountable for safeguarding the sensitive information entrusted to us by veterans and beneficiaries. Even now we are conducting an inventory to determine appropriate access needs for everyone within VA. And we will be instituting background checks appropriate to those access levels.

In fact, it is our people that will make all of this happen. There is nothing more important than having people with training and character, who assume the responsibility to implement the changes needed.

Mr. Chairman, unfortunately a very bad thing happened. A monumentally awful thing. I am outraged by it and the slow response of some of our Department. But I am the responsible person, and it is to me that you are entitled to look to see that this is fixed. It won't be easy, and it won't be overnight, but I am absolutely convinced that we can do it. As I've said, I think we can turn VA into the model for information security, just as it has become the model for health care in the United States, as most recently attested to in an article in Business Week magazine dated July 17th.

Mr. Chairman, that concludes my testimony. I would be pleased to answer any questions that the Committee may have.