Statement of
The Honorable R. James Nicholson
Secretary of Veterans Affairs

Before the
Committee on Government Reform
U.S. House of Representatives

June 8, 2006
******

Mr. Chairman, Ranking Member Waxman, and members of the Committee.

Thank you for your invitation to appear before you this morning to provide you with a report and assessment of current events at the Department of Veterans Affairs. In that context, I will also present an overview of VA privacy and security policies and procedures, along with the Department's views on the adequacy of current legislation, regulations and policies governing privacy, information security and data breach notification.

The facts surrounding the recent data breach at VA that now rightfully draw the spotlight of Congressional oversight to government-wide information security policies and procedures are well known to you. I will briefly recap them before reviewing with you the actions that VA has taken in response, and what we have learned—and are learning—as a result.

A VA analyst took home electronic data files from VA. He was not authorized to do so. On May 3rd, that employee's home was broken into in what appears to local law enforcement to have been a routine breaking and entering. His laptop computer and hard drive containing the VA data were stolen. Initial analysis performed by both VA and its Inspector General indicated that these data contained identifying information, including names and dates of birth, for up to 26.5 million veterans and some of their spouses. In addition, that information, plus social security numbers, was available for some 19.6 million of those veterans. Also possibly included were some numerical

disability ratings and the diagnostic codes which identify the disabilities for which the veteran is being compensated. It is important to note that none of the data included the VA's electronic medical records.

As part of our ongoing effort to better determine what information was compromised, in addition to deploying our own internal technical experts, VA hired its own independent forensic experts, Internet Security Services, to analyze data on some 17 disks that were in the possession of the analyst. On June 1st, we learned that there was some information pertaining to active duty, Guard and Reserve troops among the individuals whose data had been compromised. On June 5th, we learned through ongoing analysis, and through discussions with the Department of Defense, that private information – the names, social security numbers and dates of birth – of as many as 1.1 million active-duty personnel from all the armed forces, along with 430,000 members of the National Guard, and 645,000 members of the Reserve force, may have been included. We are working with the Department of Defense to match data and verify, to the greatest extent possible, those potentially affected. Individualized notification letters are being sent to all those whose personal information may have been included among the stolen data. We are working with the Internal Revenue Service and the Social Security Administration to assure that we have their most current addresses.

As I stated in my testimony before both the House and Senate Committees on Veterans' Affairs last month, I am outraged at the theft of this data and the fact an employee would put it at risk by taking it home in violation of VA policies. I am also gravely concerned about the timing of the Department's response once the burglary became known. Full-scale investigations into this matter remain ongoing. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. We remain hopeful that this was a common theft, and that no use will be made of the VA data.

However, because we are committed to keeping our veterans and service members informed, VA, working with our Federal government colleagues, established call centers (800-FED-INFO) and a dedicated website (www.firstgov.gov) on May 22nd to provide answers to any concerned veteran, service member, or family member. These are updated as additional information becomes available to us regarding this data theft and what it might imply. Those tools will remain active for as long as they remain necessary for communicating with all affected persons.

From the moment I was informed, VA began taking all possible steps to protect and inform our veterans. Last week, I announced a series of personnel changes in VA's Office of Policy and Planning, the division in which the breach occurred. I have detailed current Assistant General Counsel for Management and Operations, Paul Hutter, to provide leadership to this office while the recent nomination of Patrick W. Dunne as Assistant Secretary for Policy and Planning is considered by the United States Senate. Mr. Hutter replaced the Acting Assistant Secretary for Policy and Planning, a long-time career employee, who has been placed on administrative leave. In addition, the Deputy Assistant Secretary for Policy resigned effective Friday, June 2, 2006.

I assure you that my commitment to changing the way we do business at VA is not limited to personnel actions. Moving forward, and emphasizing our commitment to improving our information security procedures, on May 31, 2006, I named former Maricopa County (Phoenix, AZ) District Attorney Richard M. Romley as my new Special Advisor for Information Security, reporting directly to me.

Mr. Romley will evaluate the current state of VA's information security procedures and processes, and will make recommendations for improvement in VA's information security systems. Rick Romley is a well-respected prosecutor and combat veteran who will bring a critical outsider's perspective to this effort. Mr. Romley shares my commitment to cutting through the bureaucracy to provide the results our nation's veterans and service members deserve and expect.

I have initiated several actions to determine how to best strengthen our privacy and data security programs. On May 24, 2006, we launched the *Data Security-Assessment and Strengthening of Controls* program, a high priority, focused plan to strengthen our data privacy and security procedures. This program will minimize the risk of a re-occurrence of incidents similar to this recent breach, and seeks to remedy material weakness that could place sensitive information at risk.

On May 26, 2006, I issued a directive to my top leadership to reinforce in each VA manager, supervisor, or team leader their duty and responsibility to protect sensitive and confidential information. In this memo, I instructed all employees to complete privacy and cyber security training by June 30, 2006. Further, I have convened a task force of VA's senior leadership to review all aspects of information security and to make recommendations that will strengthen our safeguarding of sensitive information. As an initial step, I charged this Task Force to complete an inventory of all positions requiring access to sensitive VA data by June 30, 2006. In conjunction with this, we will conduct a review of sensitivity levels and ensure that personnel at all levels have the appropriate and current National Agency Check and Inquiry (NACI), Minimum Background Investigation (MBI), or Background Investigation (BI) investigations and that these are documented in their respective personnel records.

On June 6, 2006, two days ago, I issued VA IT Directive 06-2, *Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations.* This Directive recommits both the Department, and our employees, to protecting the personal data of all individuals, including veterans, dependents and employees, while informing all concerned parties that failure to comply with VA policy may violate Federal law and could result in administrative, civil or criminal penalties. It further provides direction on proper notification procedures should a breach occur, and directs all VA senior management officials to ensure that employees under their supervision fully comply.

Also on June 6th, I issued a separate directive that the Under Secretary for Benefits suspend the practice of permitting Veterans Benefits Administration (VBA) employees to remove claims files from their regular work stations in order to adjudicate claims from alternative work locations (i.e. their homes.) This suspension will remain in place until I am satisfied VBA has in place adequate policies and procedures, and the necessary physical means to safeguard those files from theft, loss, or other unauthorized disclosure.

These initiatives will culminate across VA nationwide during the week of June 26, 2006, when VA facilities across the country – every hospital, CBOC, regional office, national cemetery, field office and VA's Central Office – will "stand down" for Security Awareness Week. Managers throughout VA will review information security and reinforce privacy obligations and responsibilities with their staff. I have also ordered that every laptop in VA undergo a security review to ensure that all security and virus software is current. The review will include removal of any unauthorized information or software. Importantly, I have ordered that no personal laptop or computer equipment be allowed access to VA's Virtual Private Network (VPN) or be used for official business. VPN settings will be changed every 30 days, forcing laptop users to return the laptop to VA for updating and security screening. We are in the process of conducting an inventory of all positions in VA with access to VPN or to any sensitive information.

You asked that I review VA's data security policies and procedures. The Department has several policies, procedures, and guidelines that govern the privacy and security of sensitive information.

VA Directive 6502, dated June 30, 2003, *Privacy Program*, establishes a Department-wide program for the protection of the privacy of veterans, their dependents and beneficiaries, as well as the privacy of all VA employees. This directive provides for the safeguarding and security of all privacy-protected data stored or transmitted in VA information systems for which VA is responsible, as well as those systems shared with, or operated by, other Federal agencies, contractors, or outside organizations.

Specific policies and procedures for the approval of alternative workplace arrangements, or telework, are governed by VA Directive 5011, dated September 22, 2005, *Hours of Duty and Leave*. This directive requires the completion of the User's Remote Computing Security Agreement between the Supervisor and the employee. The employee must complete a safety checklist and notify his organization's Information Security Officer (ISO) of the telework arrangement. The organization sponsoring telework must also ensure that adequate technological security protections are in place on all electronic devices issued to telework participants.

The FY 2001 Department of Transportation and Related Agencies Appropriations Act, Public Law 106-346, Section 359, states that, "Each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the extent possible without diminished employee performance." Under that law telecommuting is defined as "any arrangement in which an employee regularly performs officially assigned duties at home or other work sites geographically convenient to the residence of the employee," and an eligible employee is "any satisfactorily performing employee of the agency whose job may typically be performed at least one day per week at an alternative workplace." Telework is not unique to VA, and is, in fact, an alternative work arrangement promoted by federal government policy. The Office of Personnel Management (OPM) encourages telework as a means of making reasonable accommodation to persons with disabilities and as a critical factor in the implementation of continuity of operations plans.

One existing Security Guideline, *Security Guideline for Single-User Remote Access*, describes appropriate security measures for mobile or fixed computers used to process, store, or transmit information or connect to VA IT systems when such computers are housed in an alternate work location. It identifies and recommends the minimally acceptable security controls when VA personnel use anything other than a direct connected, VA-controlled local area network (LAN) connection to perform VA information processing. Examples include people that are on travel, telecommuting or working from alternate work locations. This document requires that any data not stored on our systems be encrypted and password protected. I have directed the Office of

Information & Technology to publish this guideline as a VA Directive. This document sets the standards for access, use, and information security, including physical security, incident reporting and responsibilities.

Finally, we will continue to require all VA employees and contractors to complete annually both Cyber Security Awareness Training and Privacy Awareness Training. This training is designed to help VA employees understand the importance of protecting sensitive information and making them aware of their responsibilities in this regard. Normally, employees are required to complete this training by September 30th of each year. However, as I noted earlier, given the recent data breach at VA, I directed all employees to complete both courses by June 30, 2006.

As any Federal agency, VA's privacy and security policies and procedures implement all pertinent laws, regulations, Executive Orders. These laws include the Privacy Act, the Health Information Portability and Accountability Act, the Federal Information Security Management Act, and the Information Technology Management Reform Act. We establish our policies and procedures to implement Federal Information Processing Standards Publications developed by the National Institute of Standards and Technology, the Office of Personnel Management, the Office of Management and Budget and any other oversight agency in these program areas. I believe that we should have policies and legislation, government wide, that would enable us to discipline employees and, possibly bring criminal actions, against those who willfully disregard the safeguards needed to protect veterans and other sensitive data.

I am committed to working with Congress to create a plan for the federal government to improve this situation, and at the same time, I have asked the President's ID Theft Task Force to assist us in developing this policy.

There are many lessons to be learned from the recent data breach at VA. I do know, as I have stated previously, that the time to determine that a loss had occurred

and to assure that proper individuals within the chain of command were notified was too protracted. There was also a breakdown in communications in the notification process once the incident occurred.

Mr. Chairman, in his testimony this morning, Clay Johnson, III, Deputy Director for Management of the Office of Management and Budget, stated that

> "the recent incident makes painfully obvious a long-known security risk – a single trusted individual can mistakenly or intentionally, and very quickly, undo all of the sophisticated and expensive controls designed to safeguard our information and systems from attack."

This has been a painful lesson for us at VA, and I am committed to assuring that we have the people, adequately trained, policies and procedures in place to assure that this could not happen again. Moreover, I am strongly committed to ensuring that VA seize on this moment to change the status quo, to break the "as is" model of doing business, and to make VA an exemplary federal agency in the area of information security and privacy protection, just as it has become in the area of health care.

A significant change in the way VA manages its information technology infrastructure was already well underway before this incident. In October, 2005 I issued a directive reorganizing IT at VA through the centralization of many functions, to include cyber and information security and privacy. As we continue to centralize the control of our IT systems, our ability to meet our information security and privacy obligations will be greatly enhanced. We will stay focused on the problems until they are fixed, and we will take direct and immediate action to address and alleviate affected people's concerns. With greater control, comes greater accountability. Mr. Chairman, I remain cognizant that we are accountable not only to Congress, but also to our nation's veterans and our men and women who are wearing the uniform today. It is my pledge to you that I am, and will remain, guided in my leadership of VA by what is best for our veterans.

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