OPENING STATEMENT
Senator Daniel K. Akaka
Committee on Veterans' Affairs
Committee on Homeland Security and Governmental Affairs
Joint Hearing on VA Data Theft

May 25, 2006

Thank you Chairman Craig and Chairman Collins for working together to call this very important and timely joint hearing. As the Ranking Member on the Veterans' Affairs Committee and a senior member on the Homeland Security and Governmental Affairs Committee, I am privileged to sit on the two committees that have oversight on this issue. Having both Committees investigating this matter will allow us to address the specifics of the incident involving VA data and work to craft safeguards for the entire government.

Let me be clear – the specific incident that brings us here today happens to involve VA and VA data. It could just as easily have involved other departments and agencies. It may be wise to have other departments and agencies examine their policies on classified and confidential data and the proper use and security for such data.

Shortly after the news of this incident broke, I spoke with VA Inspector General George Opfer. He told me his office launched a full investigation into the matter that will examine all the facts. I eagerly await his findings as the investigation will provide independent information for Congress to assess this situation. I also wrote to Secretary Nicholson with a number of questions. I look forward to his response today.

I am especially concerned with the manner in which VA handled this investigation. Although the breach occurred more than three weeks ago, Congress and the public were only notified of the incident this week. Regardless of whether identity theft actually occurs as a result of this incident, anytime the government loses a database of personal information, privacy is compromised. We must do all we can do to prevent this from ever happening again.

The security mechanisms at VA are not working if a mid-level VA employee was able to walk out of the building with a massive amount of personal information. It seems to me that data of this magnitude and importance should be in the hands of very few VA employees and should be guarded with the utmost security. Thus far, VA has said the employee was not authorized to take the information home. I am troubled as to how an employee who is not authorized to take home the private information of more than twenty-six million veterans was still able to do just that.

VA failed to take several steps to safeguard this information. For example, VA could have scrambled Social Security numbers based upon an encryption formula, whereby access to files that translate scrambled Social Security numbers is only possible with special authorization.

This procedure was not followed in this instance, and we need to know why.

It is important to note how we came to learn about the loss of the data. The VA employee whose computer equipment was stolen disclosed this to VA. If the employee had chosen not to report the theft immediately, VA and the public could possibly still be in the dark about the incident.

As I said earlier, while today's hearing is focusing on the information security practices at VA, I believe the data breach is indicative of broader information security and privacy problems throughout the government. I understand the problems that agencies face, as I have been working on federal data collection and privacy for a number of years.

At my request, the Government Accountability Office conducted several investigations on federal data mining activities and found that federal agencies are not following all key privacy and information security practices. Last week, I introduced legislation to strengthen the investigative authority and independence of the Chief Privacy Officer at the Department of Homeland Security. I believe we need to make sure that all agencies have a strong privacy official to ensure that what happened at VA will not happen again.

Last year, the Office of Management and Budget directed each agency to designate a senior privacy official. However, issues remain as to whether these individuals are focused on matters other than privacy, which may cause a conflict of interest; the training received by and the expertise of these individuals; and the enforcement authority of the privacy officers in each agency. Having policies and safeguards in place will not work if agencies are not following the law. The incident at VA demonstrates the need to review the Privacy Act.

I believe it is appropriate at this time, Chairman Collins, for our Committee to undertake this review as soon as possible. The applicability of the Act in this increasingly electronic age, combined with limited remedial action, necessitates that we take a closer look, and make sure that the personal information that the government collects is properly maintained.

I intend to work with all appropriate parties to provide real solutions to these glaring problems, not just in VA but across all government agencies and departments. It is unfortunate that, as the Nation prepares to honor those who paid the ultimate sacrifice in defense of our freedom, our government has breached the trust of its heroes. Our veterans deserve much better. Thank you.