

**Statement of  
Congressman John T. Salazar  
Representing the Third Congressional District  
Of Colorado  
Before the Veterans' Affairs Committee  
United States House of Representatives  
Washington, DC  
July 18, 2006**

Chairman Buyer, Acting Ranking Member Filner, I thank you for the opportunity to come before the House Committee on Veterans' Affairs to testify with regard to certain provisions of the Veterans Identity and Credit Protection Act of 2006. I wish there was no need for this bill, but the simple fact is that on May 3 of this year, personal computer equipment containing the personal information of some 26.5 million veterans and 2.2 million active duty and reserve component service members and their spouses was stolen from the home of a VA employee.

This theft, while alarming on its own merit, brought to light a deep and more troubling tragedy regarding cyber security and communications at the Department of Veterans' Affairs. In the two months since the theft of this computer equipment, this committee has held five oversight hearings in which we heard from current and former VA employees, private sector experts on IT security, academics, and the Secretary himself. These hearings opened the Committee's eyes to numerous problems that have already been discussed.

The purpose of my testimony is to discuss provisions of the bill related to new notification requirements for the Secretary. I, like many of my colleagues in this committee, was outraged when I learned that there was a 19 day gap between the date of the theft and the day Congress and the public was notified. In response to the theft of this

data and the revelation that such delays in notification occurred, I introduced HR 5588. This comprehensive bill, much of which is adopted in the bill before the Committee today, addresses the notification structure and requirements within the Department should another data breach occur.

There are several subtle differences between this bill and HR 5588 so I will address the similarities of the two bills.

Both HR 5588 and the Veterans Identity and Credit Protection Act of 2006 codify in federal statute the manner in which the Secretary of Veterans' Affairs is to notify both Congress and affected individuals involved in a data breach. By outlining the manner, content and timeframe under which the notification of a data breach takes place, it is my hope we can prevent a repeat of the 19 day delay we witnessed in May.

Under the provisions of both bills, this committee and our counterparts in the Senate are to receive notice of any breach "without unreasonable delay following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system." More importantly, however, HR 5588 proscribes the way in which the Secretary is to notify affected individuals. Each individual whose information has been compromised shall be notified in writing without unreasonable delay and that notification will include the following:

- A description of the personal information that was acquired during the breach;
- A telephone number the individual may use at no cost to make inquiries about the breach;

- Toll free contact numbers for the major credit reporting agencies;
- Toll free telephone number and website address for the Federal Trade Commission; and
- Information regarding the right of an individual to place a fraud alert, obtain a security freeze, and receive credit monitoring where applicable.

There are relatively few differences between HR 5588 and the Veterans Identity and Credit Protection Act in this section of the bill. Mr. Chairman, I hope to work with you in the next two days to address some of these minor differences and come to agreement on any amendments that may need to be made.

Mr. Chairman, I would like to conclude by thanking you and Acting Ranking Member Filner for holding this hearing today as well as the previous five oversight hearings. I feel this committee can work in a bipartisan manner to pass a finely crafted, comprehensive piece of legislation that I think will serve our veterans well. The bill makes much needed changes to the VA culture of indifference which we heard so much about during our oversight hearings. By ensuring that VA officials have both resources and authority to implement IT security, it is my hope we can prevent future breaches of data especially those on the magnitude of the one we saw this year. In addition to those changes, I am happy that this bill affords veterans whose identities may be compromised the opportunity to seek appropriate remedies to protect their identity including the use of fraud alerts and credit freezes.

Mr. Chairman, I thank you for inviting me to testify before the committee today. Your work and dedication to fixing the bureaucratic inefficiencies and problems within VA as well as your commitment to protecting veterans is very much appreciated.