

May 26, 2006

Dear Friend:

On May 3rd, the home of a U.S. Department of Veterans Affairs (VA) data analyst was burglarized and among the items stolen was a laptop potentially containing the names, social security numbers, dates of birth, disability ratings, and diagnostic codes for 26.5 million veterans, nearly every veteran in America. This absolute breakdown in basic security may result in millions of veterans finding themselves vulnerable to identity theft.

I am strongly recommending to veterans that they monitor their credit reports, bank statements, credit cards statements, health records, financial records, and any other area which may be threatened. The Federal Trade Commission (FTC) has created a website that outlines what steps veterans might take to monitor their individual information. That website can be reached at <http://www.ftc.gov/veterans>. Additionally, the VA has set-up a phone number to assist veterans in learning more about what has occurred and how to approach the situation. You may call 1-800-333-4636, Monday through Saturday from 8 a.m. to 9 p.m. (EDT). More information can also be found at <http://tomudall.house.gov/display2.cfm?id=11870&type=Issues>.

Yesterday, both the House Veterans Affairs Committee (HVAC) and the Senate Veterans Affairs Committee (SVAC) held hearings on the incident and brought Secretary Nicholson forward to testify. In his testimony the Secretary said, "I am the person ultimately responsible." Unfortunately, the simple theft of this material, egregious enough as it is, pales in comparison to the lackluster, bureaucratic manner in which the VA responded. Although the burglary occurred on May 3rd, VA Secretary Nicholson was not made aware of the incident until May 16th, the FBI and Secret Service were not alerted until May 17th, and Congress, millions of veterans, and the general public were not told of the incident until May 22nd. To handle this massive loss of personal, private veterans' information as an "internal matter," as the VA did until two weeks after the incident, constitutes nothing less than irresponsibility of the highest order. To read my statement from yesterday's hearing please visit <http://tomudall.house.gov/pdf/5-25-06%20VA%20theft.pdf>.

The VA Inspector General's office is expected to complete a thorough criminal investigation into the incident as well as a review of all VA regulations and guidelines regarding data use, internal security, and management process. Once this review is completed, I fully expect the HVAC to hold hearings to ensure the VA understands the absolute seriousness of this matter, and that Congress enact new requirements for the VA that will prevent similar episodes for occurring.

"Deter identity thieves by safeguarding your information." This basic commandment of protecting one's identity was ignored by the VA, to the potential great detriment of 26.5 million veterans. This is not how sensitive information ought to be

handled, it is not how the VA should be “serving those who have served,” and it is a complete reflection on the VA’s inability to enact level-headed security on the most important of information. “You cannot secure what you cannot manage,” one information technology specialist testified at yesterday’s hearing, and I completely agree with that sentiment.

Complete change is needed at the VA in how they handle and protect veterans’ information, and I will continue to strongly push for such change to be enacted. Until that time, I encourage all veterans to take preventive, proactive approaches protecting their identity, and to utilize all tools available to them. My office stands ready to assist, and I will fight in Congress to make sure this monumental mistake is not borne on the shoulders of our veterans.

Very truly yours,

Tom Udall
Member of Congress