

JACKIE WALORSKI
2ND DISTRICT, INDIANA

COMMITTEE ON ARMED SERVICES

COMMITTEE ON BUDGET

COMMITTEE ON VETERANS' AFFAIRS

Congress of the United States
House of Representatives
Washington, DC 20515-1402

419 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3915

202 LINCOLNWAY EAST
SUITE 101
MISHAWAKA, IN 46544
(574) 204-2645

December 15, 2014

The Honorable Robert McDonald
Secretary
U. S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Secretary McDonald:

I am requesting information regarding the ongoing response of the U.S. Department of Veterans Affairs (VA) to the continued fallout resulting from the eBenefits website privacy and security breach.

It has come to my attention that a Veteran in Southwest Florida had his account through the VA hacked twice within two months. Individuals broke into Frank Taylor's account and created a fake online profile through the eBenefits system in order to steal his disability compensation. As you already know, earlier this year thousands of Veterans had their personally identifiable information (PII), including medical and financial information, divulged online through the eBenefits portal. Despite VA's multiple assurances that its systems are secure, security incidents continue to occur on a regular basis.

Mr. Taylor received absolutely no notification that there were changes made to his account. The fact that eBenefits does not check a Veteran's information within his or her existing account, and is unable to tell if there is a discrepancy between an account already registered through the VA and an account setup online is unacceptable. Please respond to the following questions along with evidentiary documentation by no later than close of business on Friday, January 9, 2015:

1. How is VA enhancing reporting procedures which identify potential security breaches, and improving notification to Veterans when changes are made to their accounts?
2. Someone allegedly setup an eBenefits account for Mr. Taylor, although he never setup an account himself. How does VA reconcile the information of Veterans receiving benefits who have never electronically registered with eBenefits, with the information of those already registered in the system?
3. Mr. Taylor had his eBenefits account deactivated October 17, so it would not be hacked again. However, after the deactivation of his account he continued to not receive his

money because account was breached a second time. How will VA ensure that victims who have been hacked once will not be hacked again?

4. How many eBenefits accounts have been deactivated and how many have fraud alerts placed on them in order to prevent future attacks?

It is clear that the agency's information systems, including the eBenefits portal, continue to be afflicted by persistent information security weaknesses. Recognizing the importance of securing Veterans' personal information, and minimizing further instances of identity theft or other fraudulent activity, my colleagues on the House Veterans' Affairs Committee and I expect VA to take all steps necessary to strengthen the security and privacy of the eBenefits portal.

On behalf of the Veterans in my district and across the nation who are awaiting compensation they will not receive due to fake online profiles, I implore you to address the remaining security problems associated with the eBenefits portal.

Sincerely,



Jackie Walorski
Member of Congress