

**STATEMENT OF
THE HONORABLE JACKIE WALORSKI
INDIANA'S SECOND DISTRICT
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES**

April 21, 2015

Thank you Mr. Chairman.

I appreciate working with you and my fellow colleagues on the committee on this vital piece of legislation. I urge my colleagues to support my amendment in the nature of a substitute to H.R. 1017, the Veterans Information Security Improvement Act of 2015. The amendment makes some technical changes to the legislation, which includes additional definition provisions for “digital signatures” and “digital rights management”, as well as requiring in VA’s implementation reports an explanation on the progress made concerning information security-related recommendations by GAO and the IG. It will also require VA’s information System Security Plan to include detailed documentation and full integration into VA’s enterprise architecture strategy.

There is currently a systemic problem within VA's security systems that pose a serious threat to our veterans and our national security. Within VA's 420,000 computers, there are 5 vulnerabilities on at least 95% of those computers. In addition, VA employs tens of thousands of outdated operating systems. One of the more troubling stories comes from an OIG report that was released last week. The report stated in regards to VA contract employees being allowed to access the VA's network from foreign countries that "VA information security employees still reacted with indifference, little sense of urgency, or responsibility concerning a possible cyber threat." This report only gets worse, an employee who traveled to China not only accessed the VA's network, he was also allowed to log into his VA assigned computer in the US, which the VA security system could not recognize that he was connecting from China. Finally, the individual left the device he was using in China. The report concluded that since VA did not have a specific policy on prohibiting access from foreign countries to VA's network, Office of Information Technology (OIT) employee's would not prohibit it. Consequently, VA employees and contractors

were allowed unfettered access from foreign countries, such as cyber-threat countries like China. I am deeply troubled that VA has known the severity of these security risks for years, yet it continues to down play and disregard the problem.

For too long VA has ignored the longstanding problems within its IT systems. My bill, H.R. 1017 prescribes specific actions and tasks VA should take to address their vast information security weaknesses. Specifically, it directs VA to, reclaim, secure, and safeguard VA's network, defend workstations from critical security vulnerabilities, and upgrade or phase out outdated operating systems. This plan is taken from common federal and industry best practices. Such specificity is essential in mitigating known information weaknesses at VA, since VA either ignores or misapplies the current IT requirements. Again, I urge my colleagues to support the amendment and I yield back my time.