

GAO finds Information Technology at Veterans Affairs is Still Far from Secure

Posted At : September 21, 2007 3:17 PM | Posted By : Chris Campbell

Related Categories: Information Security, Federal

In a review of the progress the Veterans Affairs has made in improving its Information Security, the General Accounting Office (GAO) released a report; *Sustained Management Commitment and Oversight are Vital to Resolving Longstanding Weaknesses at the Department of Veterans Affairs*. The report concludes that despite efforts to implement initiatives to strengthen its IT security VA remains vulnerable.

As far back as 2005, VA began restructuring its management organization in order to provide better oversight and financial controls when purchasing IT systems. Other improvement efforts include developing an information protection program, improving the agency's incident management ability, and the establishment of an office for IT oversight and compliance. Following the theft of a VA laptop from an employee's home that included personal information on over 26 million active military and retired personnel, VA began an agency-wide effort to add encryption software to required laptops across the agency. However, efforts to secure its IT security have fallen short in many regards and as a result, VA's IT security remains vulnerable.

According to GAO, areas of concern that continue to stall the improvement of security across the VA include the fact that:

-
- since June 2006, the position of chief information security officer has remained empty. This has left IT security initiatives without an internal advocate making it more difficult to push some initiatives through;
- despite the restructuring of the IT office that has taken place the responsibility for managing and implementing security programs remains decentralized. Additionally, the process guiding coordination of security between VA's officials has never been formally documented;
- VA's Office of IT Oversight and Compliance does not possess an established criteria on which it performs its examinations, thus facilities across the VA may be evaluated with different standards;
- even though VA has been advocating the use of encrypted thumb drives and adding encryption software to laptops, the agency has not established a policy to define which devices require encryption; and
- within its procedures for incident response, VA has not defined the manner in which it facilities can seek advice from other agencies in handling incidents.