On May 3, 2006, a career civil servant at the Department of Veterans Affairs (VA) violated official policy by taking computer disks containing personally identifiable information (PII) about 26.5 million veterans home with him. The disks were stolen from his home. Two weeks after officials learned of the theft, the VA disclosed the incident to the public and set up a Website and an 800-number to provide veterans and with information and a channel for reporting possible identity theft.

The USA.gov Website put up a page called "Latest Information on Veterans Affairs Data Security" with answers to frequently-asked questions; the VA itself also continued issuing press releases (using keyword “data” in the search field at provides a reasonable chronology).

In early June 2006, the VA announced that the stolen data might include PII about up to 1.1M active-duty troops, 430,000 members of the National Guard and 645,000 members of the reserves. Reactions from a coalition of veterans groups was immediate: they launched a class-action lawsuit demanding full disclosure of exactly who was affected by the theft and seeking $1000 in damages for each victim.

The VA struggled to cope with the bad publicity and potential legal liability resulting from the May theft. On May 26, 2006, Secretary of VA R. James Nicholson issued a Directive to all VA supervisors in which he wrote, “Having access to such sensitive information brings with it a grave responsibility. It requires that we protect Federal property and information, and that it shall not be used for other than authorized activities and only in authorized locations. As managers, supervisors, and team leaders it is your responsibility to ensure that your staff is aware of and adheres to all Federal and VA policies and guidelines governing privacy protected material. I also expect each and every one of you to know what sensitive and confidential data your subordinates, including contractors, have access to and how, when and where that data is used, especially in those cases where it is used or accessed off-site.”

On May 30, 2006, the VA fired the analyst “response for data loss” and announced changes in the administration of information security in the organization. The press release made no mention of who was responsible for allowing anybody to store unencrypted PII on VA computers or media.

Coincidentally, at the end of May, the Government Accountability Office (GAO) issued a report: “GAO-06-612: Homeland Security: Guidance and Standards are Needed for Measuring the
The report specifically named the VA as requiring “guidance and standards for measuring performance in federal government facility protection.”

On June 21, 2006, the VA announced that it would provide free credit monitoring for everyone affected by the data theft in May.

But worse was yet to come. More in the saga next time.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at mekabay@gmail.com; Web site at http://www.mekabay.com/index.htm.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.