In this brief series of articles, I’ve been recounting the tale of data losses at the Department of Veterans Affairs (VA). This will close the subject for now.

On Friday, February 2, 2007, Secretary of Veterans Affairs Jim Nicholson announced that a VA employee in the VA medical center in Birmingham, AL had reported an external hard drive as missing on January 22nd. According to Rep Spencer Bachus (R-AL), the backup hard drive contained personally identifiable information (PII) on up to 48,000 veterans – and despite VA regulations promulgated in 2006, as many as 20,000 of those records were not encrypted.<http://news.com.com/2100-1029_3-6156386.html> A week later, the VA admitted that the hard drive actually contained PII about 535,000 patients and 1.3 million doctors.<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011218> It was that loss that led to the letter I quoted in the first article of this series.<http://www.networkworld.com/newsletters/sec/2007/0611sec1.html>

A few weeks later, the Government Accountability Office (GAO) released the closest thing to an exasperated blast of exasperation I think government workers are capable of: in testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans’ Affairs, House of Representatives on February 28, 2007, GAO Director of Information Security Issues Gregory C. Wilshusen presented a report entitled “Veterans Affairs Needs to Address Long-Standing Weaknesses.”<http://www.gao.gov/new.items/d07532t.pdf> The summary on page 2 of the PDF file include this commentary:

“For many years, GAO has raised significant concerns about VA’s information security—particularly its lack of a comprehensive information security program, which is vital to safeguarding government information. The figure below details information security weaknesses that GAO identified from 1998 to 2005. As shown, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring that changes to computer software were authorized and timely; or (5) providing continuity of computerized systems and operations. The department’s IG has also reported recurring weaknesses throughout VA in such areas as access controls, physical security, and segregation of incompatible duties. In response, the department has taken actions to address these weaknesses, but these have not been sufficient to establish a comprehensive information security programs. As a result, sensitive information has remained vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. Without an established and implemented security program, the department will continue to have major challenges in protecting its systems and information from security breaches.”

In early March 2007, the VA reacted to the January 22nd loss of the portable hard drive. Chief Information Officer (CIO) Robert Howard promulgated a policy restricting the use of portable data storage devices. Only flash drives smaller than 2 GB – and only those issued by the VA’s
CIO office itself – would be permitted on the VA network or computers. Encryption would be
used throughout the system, just like the assurance issued in August 2006 about spending $3.7M
on encryption tools.<

In addition, the CIO announced sweeping changes in security administration, with promotion of five deputy CIOs to the rank of assistant secretaries for the following functions: application development, information security, operations and maintenance, resource management and strategic planning.

The latest news I want to mention is the blinding revelation that has come upon federal agencies as of late May 2007: they will stop storing Social Security Numbers and other PII wherever possible.<

I tell you, it amazes me sometimes to see the speed with which people can respond to
information about security.

[By the way, the Latin title of today’s essay means, “Let it stand for what it is worth.”]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto: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.