**Veterans Affairs Data Theft (http://epic.org/privacy/vatheft/)**

* **Department of Veterans Affairs Reports Massive Data Theft.** The Department of Veterans Affairs announced today that an agency employee took home records on 26.5 million veterans that were subsequently stolen by a burglar. The data included names, Social Security Numbers (SSNs), and date of birth, as well as some disability ratings. The FBI and the VA Inspector General's Office have launched "full-scale investigations." Information for those who are concerned about identity theft is available from the Federal Trade Commission. (May 22)
* **Scope of Veterans Affairs Data Theft Widens.** The personal information of about 1.1 million active-duty military personnel, 430,000 members of the National Guard, and 645,000 members of the Reserves was stolen in the recent theft of computer data from the Department of Veterans Affairs, the agency announced Tuesday. The agency previously said ([pdf](http://www.usa.gov/veteransinfo_letter.pdf)) that all 26.5 million people affected by the data theft were veterans and their spouses. The data include SSNs and disability ratings. Privacy Rights Clearinghouse offers ID theft prevention tips. (Jun. 7)
* **Stolen Veterans Affairs Laptop and Hard Drive Are Found.** The stolen laptop computer and hard drive containing sensitive data for up to 26.5 million veterans, their spouses, and active-duty military personnel have been found, according to Veterans Affairs Secretary Jim Nicholson. This comes as newly discovered documents showing that Veterans Affairs had given permission in 2002 for the analyst, from whom the equipment was stolen, to work from home with data that included millions of SSNs, disability ratings, and other personal information. Agency officials previously said the analyst was fired because he violated agency procedure by taking the data home. (Jun. 29)

**Background**

An information security breach by a Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million people. The agency has estimated that it will cost between $100 million to $500 million to prevent and cover possible losses from the data theft. Though the theft occurred on May 3, 2006, the agency waited until May 22 to inform those who were affected. The delay was just one of many failures by Veterans Affairs in this incident.

On May 3, 2006, a data analyst at Veterans Affairs took home a laptop and an external hard drive containing unencrypted information on 26.5 million people. The computer equipment was stolen in a burglary of the analyst's home in Montgomery County, Md., and he immediately reported the theft to both Maryland police and his supervisors at Veterans Affairs. The analyst admitted that he had been routinely taking home such sensitive data for three years. Though the analyst's supervisors knew of the theft, Veterans Affairs Secretary R. James Nicholson was not told of the data theft until May 16. The next day, Secretary Nicholson informed the FBI, who began working with Montgomery County police to investigate the burglary.

On May 22, Veterans Affairs issued a statement about the theft, explaining the data stolen included the names, SSNs, date of birth, and some disability ratings for 26.5 million veterans and spouses, but did not include financial information or electronic health records. Subsequent investigation showed that the scope of the data breach was beyond the initial assessment. At a Congressional hearing on May 25, Secretary Nicholson admitted that, though the agency had said the data stolen did not include health records, it did include disability ratings that provided medical information on 2.6 million people.

On June 3, Veterans Affairs announced that the personal information of about 50,000 active-duty personnel were included in the data stolen. Another announcement followed on June 6, explaining that the 26.5 million people affected by the data theft included "1.1 million military members on active duty, 430,000 members of the National Guard, and 645,000 members of the Reserves." The FBI and Montgomery County police continue to investigate the theft.

The massive theft of data from Veterans Affairs is one of many that have been revealed in the last year and a half.

On June 29, an unidentified person turned in the stolen laptop computer and hard drive. This news came as newly discovered documents showed that Veterans Affairs had given permission in 2002 for the analyst, from whom the equipment was stolen, to work from home with data that included millions of SSNs, disability ratings and other personal information. Agency officials previously said the analyst was fired because he violated agency procedure by taking the data home.

**Congressional Investigation**

**VA Ignores Cybersecurity Warnings**

## Government auditors tell House panel that they can't force VA officials to comply with their recommendations.

### Grant Gross, IDG News Service

Wednesday, June 14, 2006 03:00 PM PDT

U.S. lawmakers on Wednesday questioned why the U.S. Department of Veterans Affairs continues to suffer from cybersecurity problems despite multiple warnings from government auditors.

Members of the House Veterans' Affairs Committee asked government auditors why the VA has not acted on repeated cybersecurity recommendations. The hearing follows the VA's announcement last month that personal data of 26.5 million U.S. military veterans and spouses was stolen from the home of a VA data analyst, who had the information stored on a personal laptop computer and an external hard drive. He was not authorized to take that information home. The VA has said that the computer equipment and not the data was the target of whoever stole it.

## 'Pathetic' Response

Some veterans received notices of the data theft by mail this week, close to six weeks after the May 3 break-in. Representative Bob Filner (D-California) called the VA's response to the data theft "pathetic."

"If it were possible to approach the theft of veterans' and service members' records without emotions ... this situation might be even an interesting case study of lax policies, failed leadership, and organizational arrogance," Filner said.

VA Secretary R. James Nicholson announced that last month he had demoted two agency supervisors who failed to tell him of the data theft, immediately. The analyst who took home the data against agency policy will also be fired, Nicholson has said. As recently as last week, the VA has said there is no indication the stolen information has been used in identity theft schemes.

The committee will hear from Nicholson later this month.

## Bureaucracy Hampers Cybersecurity Efforts

Auditors with the U.S. Government Accountability Office and the office of the Inspector General of Veteran affairs said at Wednesday's hearing that they have no authority to force the VA to comply with their recommendations. In addition, the VA does not give its chief information officer authority to implement the recommendations without approval from three undersecretaries in the agency, said Michael Stale, the VA's assistant inspector general for audits.

"They have a long way to go to mitigate their vulnerabilities and have a comprehensive IT security program," he said.

The GAO has issued multiple reports about VA cybersecurity problems since 2000, and the VA has received a failing grade in four of the past five years on an annual cybersecurity review by the House Government Reform Committee.

The agency seems to focus on individual medical centers or regional centers in fixing identified problems, instead of fixing those problems agency wide, Staley said. "The responses we get back to those recommendations are, 'We've take action at site A,'" he said. "Then the next year we ... go to site B, and we see the same conditions exist."

Committee Chairman Steve Buyer (R-Indiana) asked Staley and GAO auditors who was responsible if VA officials ignored cybersecurity warnings. Auditors are working with the White House Office of Management and Budget to work on cybersecurity problems across the U.S. government, said Linda Koontz, GAO's director of information management issues.

"We need to figure out what are the lines of authority," Buyer said.

The VA's decentralized management, with its three divisions largely responsible for their own IT security, has contributed to cybersecurity problems, Buyer said. "VA's internal controls in data security have been grossly inadequate for years," he added.