



WikiLeaks Document Release

<http://wikileaks.org/wiki/CRS-RL33612>

February 2, 2009

Congressional Research Service

Report RL33612

*Department of Veterans Affairs: Information Security and
Information Technology Management Reorganization*

Sidath Viranga Panangala, Domestic Social Policy Division

August 14, 2006

Abstract. On July 20, 2006, the House Committee on Veterans' Affairs marked up and ordered to be reported out of committee by voice vote the Veterans Identity and Credit Security Act of 2006 (H.R. 5835). H.R. 5835, as amended, would, among other things, create a new position of Under Secretary for Information Services in the Department of Veterans Affairs (VA) who would also serve as the Chief Information Officer (CIO) of the department. The bill would also provide credit protection services and fraud resolution services to veterans in the event of a data security breach at the VA. Moreover, H.R. 5835 would establish scholarship and student loan repayment programs at the VA as a tool for recruiting and retaining cybersecurity personnel. The bill is awaiting report to the full House.

WikiLeaks

CRS Report for Congress

Received through the CRS Web

Department of Veterans Affairs: Information Security and Information Technology Management Reorganization

August 14, 2006

Sidath Viranga Panangala
Analyst in Social Legislation
Domestic Social Policy Division

<http://wikileaks.org/wiki/CRS-RL33612>

Department of Veterans Affairs: Information Security and Information Technology Management Reorganization

Summary

On May 3, 2006, the home of a Department of Veterans Affairs (VA) data analyst was burglarized, resulting in the theft of a laptop computer and an external data storage device that was reported to contain personal information on more than 26 million veterans and United States military personnel. The VA Secretary testified that he was not informed of the incident until May 16, 2006, almost two weeks after the data had been stolen. VA publicly announced the theft on May 22. On June 29, VA announced that the stolen laptop computer and external hard drive had been recovered intact and that, based on a forensic examination conducted by the Federal Bureau of Investigation (FBI), the files on the external hard drive had not been compromised.

Following this data theft, and in light of several ongoing information security and information technology management issues at the VA, several legislative proposals were introduced in Congress. On July 18, 2006, the House Committee on Veterans' Affairs held a hearing to review these proposals, including its own draft bill. On July 19, Chairman Buyer introduced the committee's draft proposal as the Veterans Identity and Credit Security Act of 2006 (H.R. 5835). On July 20, the full committee marked up H.R. 5835 and ordered the measure reported out of committee by voice vote. H.R. 5835, as amended, would, among other things, create a new position of Under Secretary for Information Services in the VA who would also serve as the Chief Information Officer (CIO) of the department. The bill would also provide credit protection services and fraud resolution services to veterans in the event of a data security breach at the VA. Moreover, H.R. 5835, as amended, would establish a scholarship program at the VA for recruitment of personnel who are pursuing a doctoral degree in cybersecurity.

This report supersedes CRS Report RS22460, *Theft of Veterans' Personal Information, and Department of Veterans Affairs Information Technology Reorganization: Issues for Congress*, by Sidath Viranga Panangala and Alison M. Smith.

This report will be updated as events warrant.

Contents

Most Recent Developments	1
Background	1
Information Security Issues at the VA	3
VA Information Technology Reorganization	5
Legislative Proposals on Data Security	7
Veterans Identity and Credit Security Act of 2006	8

Department of Veterans Affairs: Information Security and Information Technology Management Reorganization

Most Recent Developments

On July 20, 2006, the House Committee on Veterans' Affairs marked up and ordered to be reported out of committee by voice vote the Veterans Identity and Credit Security Act of 2006 (H.R. 5835). H.R. 5835, as amended, would, among other things, create a new position of Under Secretary for Information Services in the Department of Veterans Affairs (VA) who would also serve as the Chief Information Officer (CIO) of the department. The bill would also provide credit protection services and fraud resolution services to veterans in the event of a data security breach at the VA. Moreover, H.R. 5835 would establish scholarship and student loan repayment programs at the VA as a tool for recruiting and retaining cybersecurity personnel. The bill is awaiting report to the full House.

Background

On May 3, 2006, the home of a VA data analyst was burglarized, and among the items stolen were the employee's personal laptop computer and an external data storage device. According to the VA, the information stored on this equipment included the names, birthdates, and Social Security numbers of approximately 26.5 million veterans and their spouses, and as many as 1.1 million active-duty military personnel, 430,000 National Guard members, and 645,000 reserve personnel. The data theft also included some numerical disability ratings and the diagnostic codes that identify veterans' disability.¹ The analyst was authorized to have access to sensitive data in the performance of his duties, and had been routinely taking such data home since 2003.²

¹ U.S. Department of Veterans Affairs, Office of the Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans* (Report No:06-02238-163), July 11, 2006, p.1, available at [<http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf>], visited July 11, 2006. Ann Scott Tyson and Christopher Lee, "Data Theft Affected Most in Military; National Security Concerns Raised," *Washington Post*, June 7, 2006, Final Edition, p. A01.

² Testimony of Inspector General of the Department of Veterans Affairs, George J. Opfer, in the U.S. Congress, House Committee on Veterans' Affairs, hearing on the *Recent Security Breach at the Department of Veterans Affairs, in which 26.5 million Veterans Records were Stolen from the Home of a VA Employee*, 109th Congress, second session, May 25, 2006.

On June 29, during a hearing of the House Veterans' Affairs Committee, the Secretary of Veterans Affairs announced that the laptop computer and external data storage device that were stolen from the VA data analyst had been recovered intact and that, according to computer forensic examinations performed by the Federal Bureau of Investigation (FBI), the data files were not accessed or compromised. VA issued a statement on July 14 stating that "the FBI indicated to VA that it has a high degree of confidence, based on the results of the forensic tests and other information gathered during the investigation, that the sensitive files were not accessed or compromised."³ VA also announced that it would no longer provide one year of free credit monitoring to veterans whose personal information may have been compromised due to this theft, but would continue to conduct data breach analyses looking across multiple industries to detect patterns of misuse related to the data loss.⁴ At the same time, the Administration withdrew its request for \$160.5 million of additional funding for VA to provide credit monitoring services for veterans and military personnel affected by the theft and security breach. In its letter to Congress, the Administration stated that "on the basis of the FBI's analysis, credit monitoring services and the associated funding will no longer be necessary."⁵

Since the May 3 data theft, VA has informed both the House and Senate Veterans' Affairs Committees about several additional data breaches. On May 18, 2006, VA began notifying veterans at the state veterans' nursing home in Silver Bay, Minnesota, regarding the loss of their individually identifiable information (e.g., names, birthdates, Social Security numbers, and addresses). During the same month, it was also reported that a data tape containing about 16,000 VA legal case records had been lost from the Indiana VA regional counsel's office. These records potentially contained identifiable data of veterans and their dependents. Most recently, on August 7, VA announced that a subcontractor, hired to assist in insurance collections at VA medical centers (VAMCs) in Pittsburgh and Philadelphia, had lost a desktop computer containing personal information on some veterans. According to the VA, the desktop contained information on approximately 5,000 patients treated at the Philadelphia VAMC, approximately 11,000 patients treated at the Pittsburgh VAMC, and approximately 2,000 deceased patients.⁶ VA is also investigating the possibility that the computer may have contained information on approximately another 20,000 people who received care through the Pittsburgh VAMC.⁷

³ U.S. Department of Veterans Affairs, "FBI Highly Confident Recovered Data Has Not Been Accessed or Compromised," press release, July 14, 2006.

⁴ U.S. Department of Veterans Affairs, "VA to Conduct Data Breach Analysis; Individual Credit Monitoring No Longer Necessary," press release, July 17, 2006.

⁵ Office and Management and Budget (OMB) letter available at [http://www.whitehouse.gov/omb/budget/amendments/supplemental8a_7_18_06.pdf], visited on July 18, 2006.

⁶ U.S. Department of Veterans Affairs, Office of Public Affairs, "Subcontractor Notifies VA of Missing Computer with Vet Files; VA, Law Enforcement Authorities Investigating," press release, Aug. 7, 2006, p. 1.

⁷ Ibid.

In response to these data breaches, the VA has taken several measures to address its information system security vulnerabilities. Noted below are some key actions taken thus far:

- the Secretary's memorandum to VA employees requiring them to complete cybersecurity and privacy awareness training;
- issuance of VA IT Directive 06-2, which requires supervisory approval before the removal of confidential and Privacy Act-protected information from a worksite;
- issuance of VA Directive 6504, restricting the transmission, transportation of, and access to VA data outside VA facilities; and
- the Secretary's memorandum delegating authority to the Assistant Secretary of Information Technology for enforcement of information policies and practices.⁸

This report provides a brief overview of information security issues at the VA and recent attempts by Congress to reorganize the management of information security and technology at the department. It also provides a brief analysis of the Veterans Identity and Credit Security Act of 2006 (H.R. 5835), as amended.

Information Security Issues at the VA

Recent data breaches at the VA come at a time when the department's information systems are under increased scrutiny. In the past several years, both the Government Accountability Office (GAO) and the VA's Office of Inspector General (OIG) have highlighted the VA's computer security vulnerabilities. In September 1998, GAO reported that computer security weaknesses placed critical VA operations such as financial management, health care delivery, and benefits payments at risk of misuse and disruption.⁹ In 1999, GAO reported that the VA's success in improving computer security largely depended on strong commitment and the dedication of adequate resources to the information security program plan.¹⁰ In September 2000, GAO reported that serious computer security problems persisted throughout the VA because the agency had not fully implemented an integrated security management program, nor had the Veterans Health Administration (VHA) effectively managed

⁸ For a complete list of activities, see U.S. Department of Veterans Affairs, Office of the Inspector General, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*. (Report No. 06-02238-163) July 11, 2006, pp. 62-64, available at [<http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf>], visited Aug. 7, 2006.

⁹ U.S. Government Accountability Office, *Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure*, GAO/AIMD-98-175, Sept. 23, 1998.

¹⁰ U.S. Government Accountability Office, *Information Systems: The Status of Computer Security at the Department of Veterans Affairs*, GAO/AIMD-00-5, Oct. 4, 1999.

computer security at its medical facilities.¹¹ Furthermore, in testimony before the House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, GAO stated that "VA continues to report pervasive and serious information security weaknesses. Thus far, its actions toward establishing a comprehensive computer security management program have not been sufficient to ensure that the department can protect its computer systems, networks, and sensitive veterans health care and benefits data from unnecessary exposure to vulnerabilities and risks."¹² In its annual audit reports on VA's information security program, the OIG found that VA's computer system remains vulnerable to unauthorized access and misuse of sensitive information and data. In March 2005, VA's OIG reported that it had "identified significant information security vulnerabilities that place VA at considerable risk of denial of service attacks, disruption of mission-critical systems, fraudulent benefits payments, fraudulent receipt of health care benefits, unauthorized access to sensitive data, and improper disclosure of sensitive data."¹³

In its testimony before the Senate Veterans' Affairs Committee on July 20, 2006, the OIG stated that "VA policies, procedures, and practices do not adequately safeguard personal or proprietary information used by VA employees and contractors." Furthermore, the OIG "found a patchwork of policies that were difficult to locate and fragmented. None of the policies prohibited the removal of protected information from the worksite or storing protected information on a personally-owned computer, and did not provide safeguards for electronic data stored on portable media or a personal computer."¹⁴ While VA has attempted to fix data security vulnerabilities in selected sites identified by the OIG, the agency has not fully instituted the recommendations made by GAO and the OIG throughout its system.¹⁵

¹¹ U.S. Government Accountability Office, *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration*, GAO/AIMD-00-232, Sept. 8, 2000.

¹² U.S. Government Accountability Office, *VA Information Technology Progress Made, but Continued Management Attention Is Key to Achieving Results*, GAO-02-369T, Mar. 13, 2002.

¹³ U.S. Department of Veterans Affairs, Office of the Inspector General, *Audit of the Department of Veterans Affairs Information Security Program* (Report No. 04-00772-122), not publicly available. This was quoted in the U.S. Department of Veterans Affairs, Office of the Inspector General, *Major Management Challenges Fiscal Year 2005* (Report No. 06-00480-26), Nov. 15, 2005, available at [<http://www.va.gov/oig/53/reports/VAOIG-06-00480-26.pdf>], visited June 13, 2006.

¹⁴ Testimony of Inspector General of the Department of Veterans Affairs, George J. Opfer, in the U.S. Congress, Senate Committee on Veterans' Affairs, hearing on *VA Data Privacy Breach: Twenty-Six Million People Deserve Assurance of Future Security*, 109th Congress, second session, July 20, 2006.

¹⁵ Testimony of Assistant Inspector General for Audit, Department of Veterans Affairs, Michael Staley, and testimony of Director of Information Management Issues, U.S. Government Accountability Office, Linda Koontz, in the U.S. Congress, House Committee on Veterans' Affairs, hearing on the *Recent Security Breach at the Department of Veterans Affairs, in which 26.5 million Veterans Records were Stolen from the Home of a VA* (continued...)

VA Information Technology Reorganization

During the past few years, the House and Senate Veterans' Affairs Committees have drawn attention to shortcomings in the management of VA's information technology (IT) projects, most recently the failure of a pilot implementation of the Core Financial and Logistical System (CoreFLS) — integrated financial and logistics systems management software — at the Bay Pines Medical Center in Florida.¹⁶

In the wake of the CoreFLS failure, the VA's Assistant Secretary for Information Technology, in December 2004, contracted with the Gartner Group to conduct an organizational assessment of VA IT. The study, delivered in May 2005, proposed several options to reorganize the development and management of VA IT programs.

The first option was to keep the existing IT management structure in which VA IT resources are operated and managed within a highly decentralized management structure. The Department's CIO manages a central office staff of approximately 350 employees and a direct budget of approximately \$50 million per year. While the CIO is charged with overall responsibility for the successful management of all VA IT resources, the CIO has no direct management control or organizational authority over any of these resources. The Department's CIO provides policy guidance, budgetary review, and general oversight via indirect supervision of the CIOs of each of the VA's three administrations — the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA).

The second option proposed was the "regional option." Under this option, VA would be divided into three to five geographically based subdivisions. Within each of these, a Deputy CIO would control all IT assets and would be responsible for all service delivery within that region. These Deputy CIOs would report directly to the VA CIO.

The third option recommended by the Gartner study was the "administration-centric option." Under this option, VA would be divided by administration — into the VHA, VBA, and NCA — and a Deputy CIO for each administration would control all IT assets and be responsible for all service delivery within that administration. These Deputy CIOs would report directly to the VA CIO.

The fourth option proposed was the "federated option." Under this option, VA would divide operational responsibilities and IT systems development responsibilities into separate domains. All IT operational service delivery personnel and the budget associated with their support would come under the direct supervision of a national organization that reports directly to the CIO's office. This organization would be charged with delivering all IT-related operational services to all elements of the VA

¹⁵ (...continued)

Employee, 109th Congress, second session, June 14, 2006.

¹⁶ Opening statement of Senator Larry Craig, in the U.S. Congress, Senate Committee on Veterans Affairs, hearing on *The Management of Information Technology Resources by the Department of Veterans Affairs*, 109th Congress, first session, Oct. 20, 2005.

based upon a negotiated and formally agreed-upon set of specific standard IT services delivered according to a clearly understood and documented set of service-level agreement standards. Under a federated approach, IT systems development and management responsibility would remain with the three administrations. The VA CIO would maintain overall responsibility for the successful management of these resources and continue to provide IT budget oversight, policy, and program management direction for the Department.

The last option recommended was the “centralized option.” Under this option, all VA IT personnel resources, assets, and budget would be under the direct supervision of the VA’s CIO. In general, this centralized IT organization would be charged with delivering all IT-related operational and systems development services to all elements of the VA based upon a negotiated and formally agreed-upon set of specific standard IT services.¹⁷

Following a briefing on the Gartner report, VA senior management, in October 2005, adopted the federated model as the best model to reorganize the management of VA IT. As stated earlier, under the federated model, the VA would separate operational responsibilities and IT systems development responsibilities into separate domains. All IT operational service delivery personnel and the budget associated with their support, including all non-medical IT equipment, maintenance, and contractor support would come under the direct supervision of the CIO. According to the VA, this organizational model will provide all IT-related operational services to all elements of the VA, based upon a negotiated and formally agreed-upon set of specific standard IT services. The delivery of services would be according to a clearly understood and documented set of service-level agreement standards.¹⁸

However, frustrated by repeated failures in the VA’s IT management, the House Veterans’ Affairs Committee (HVAC) felt that it needed to legislate to transform VA IT management. Therefore, at the same time the VA was adopting a federated model, HVAC reported the Department of Veterans Affairs Information Technology Management Improvement Act of 2005 (H.R. 4061, H.Rept. 109-256) to reorganize the management of VA IT programs. The bill mandated that the VA adopt a centralized model for IT development and management. It was the view of HVAC that the VA should maintain a centralized IT management system to maintain control of all IT-related assets, and that a federated model would not optimize IT support and service delivery throughout the VA.¹⁹ H.R. 4061 passed the full House on November 2, 2005. There has been no Senate action on this bill.

¹⁷ Testimony of Deputy Secretary of Veterans Affairs, Gordon H. Mansfield, in the U.S. Congress House Committee on Veterans’ Affairs, hearing on the *VA IT Infrastructure Reorganization and the Role of the CIO*, Sept. 14, 2005.

¹⁸ Testimony of Deputy Secretary of Veterans Affairs, Gordon H. Mansfield, in the U.S. Congress, Senate Committee on Veterans’ Affairs, hearing on the *Management of Information Technology Resources by the Department of Veterans Affairs*, Oct. 20, 2005.

¹⁹ U.S. Congress, House Committee on Veterans’ Affairs, *Department of Veterans Affairs Information Technology Management Improvement Act of 2005*, report to accompany H.R. 4061, 109th Congress, first session, H.Rept. 109-256, p. 5.

The House and Senate Appropriations Committees have also expressed concern about the management of the VA's IT program. In its report (S.Rept. 109-105) to accompany the FY2006 Military Construction and Veterans Affairs Appropriations bill (H.R. 2528), the Senate Appropriations Committee stated its concern "that without a single office ultimately responsible for the Department's numerous automation efforts, the vast sums appropriated for this area might not be obligated in the most efficient manner."²⁰ Moreover, the conference agreement on the FY2006 Military Construction, Military Quality of Life and Veterans Affairs Appropriations Act (H.Rept. 109-305, P.L.109-144) included a provision withholding funding for the new HealthVet-VistA project until the VA receives approval from the House and Senate Appropriations Committees on its expenditure plan for the project.²¹

Legislative Proposals on Data Security

Since VA announced the loss of data, a number of legislative proposals have been introduced in both the House and Senate to address some of the issues arising from the data theft. These bills have been referred to the House and Senate Committees on Veterans' Affairs. H.R. 5520, which was referred to the House Judiciary Committee, would establish the Office of Veterans Identity Protection Claims to adjudicate claims for those persons who have suffered losses due to the theft. The House Judiciary Committee approved H.R. 5520 by voice vote on June 21. The committee also approved an amendment to the bill that would authorize \$2 million annually from fiscal years 2007-2011 to investigate and prosecute individuals involved in the security breach, and would allow veterans and active-duty service members to file claims for up to two years for reimbursement due to losses resulting from the security breach. H.R. 5577 would establish the Office of Identity Protection to prevent and mitigate misuse of stolen personal information. H.R. 5487 and H.R. 5588 would require the VA Secretary to establish safeguards to protect sensitive personal information against unauthorized access, and to outline security breach notification procedures. H.R. 5455, H.R. 5464, H.R. 5577, and S. 2970 include a notification clause. H.R. 5490 would require the Secretary to establish a national database of veterans who apply for or receive benefits. H.R. 5467, H.R. 5490, H.R. 5577, S. 3176, and S. 3486 would impose penalties or liabilities for the unauthorized access to or disclosure of personal information.

Many of the bills would provide affected individuals with credit-monitoring services. S. 3176 and S. 3486 would require the Federal Trade Commission, in consultation with the VA Secretary, to develop and implement a financial counseling program. Other bills (H.R. 5455, H.R. 5464, H.R. 5487, H.R. 5577, H.R. 5588, and S. 2970) would also provide free credit monitoring services and/or credit reports.

²⁰ U.S. Congress, Conference Committees, *Military Quality of Life and Veterans Affairs Appropriations Act, 2006*, conference report to accompany H.R. 2528, 109th Congress, first session, H.Rept. 109-305, p.56.

²¹ HealthVet-VistA is the VA's next-generation health information system, which will eventually replace the current Veterans Health Information Systems and Technology Architecture (VistA), which is the automated patient record system.

Veterans Identity and Credit Security Act of 2006

On July 18, 2006, the House Committee on Veterans' Affairs held a hearing to review several of these legislative proposals. At the hearing, the committee heard testimony on the following bills: the Veterans' ID Theft Protection Act of 2006 (H.R. 5487); the Veterans Identity Protection Act of 2006 (H.R. 5577); the Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006 (H.R. 5588); the Veterans Identity Protection Act (H.R. 5464); and the Comprehensive Credit Services for Veterans Act of 2006 (H.R. 5783). The committee also heard testimony on a draft proposal drawn up by the committee. On July 19, Chairman Buyer introduced the committee's draft proposal as the Veterans Identity and Credit Security Act of 2006 (H.R. 5835). On July 20, the full committee marked up H.R. 5835 and ordered the measure to be reported out of committee by voice vote.

H.R. 5835, as amended, would create a new position of Under Secretary for Information Services who would also serve as the CIO of the VA, and would maintain control of all IT-related assets of the department, including budgets and personnel. The bill would require the VA to provide free credit protection services to those whose personal, sensitive information is lost, stolen, or otherwise compromised while in the possession of the VA. If the measure is implemented, VA would have to inform all affected individuals about any data breach, and VA would have to contract with credit reporting agencies to provide fraud alert services, and provide credit security freezes to affected individuals who request it. Moreover, under H.R. 5835, if the Secretary determines — based on an independent risk analysis — that a reasonable risk exists for the potential misuse of sensitive information involved in a data breach, VA is required to provide additional notification to affected individuals informing them about credit protection services.

The Veterans Identity and Credit Security Act of 2006 includes a provision that would establish a scholarship program that would increase VA's ability to recruit and retain qualified cybersecurity professionals. Under this proposed program, VA would pay tuition, fees, and a monthly stipend of \$1,500 to persons who are pursuing a doctoral degree in computer science and electrical and computer engineering. Furthermore, H.R. 5835 would authorize a student loan repayment program as a recruitment mechanism to attract qualified individuals with doctoral degrees in computer science and electrical and computer engineering. Under this program, the department would pay up to \$16,500 a year for five years to eligible employees to repay loans related to their doctoral degrees in the above-mentioned fields.

The Congressional Budget Office (CBO) estimates that implementing H.R. 5835, as reported, would cost \$5 million in FY2007 and approximately \$50 million over the FY2007-FY2011 period. Furthermore, CBO estimates that if VA were to experience another data breach similar to the data theft that occurred on May 3, 2006, the cost could be as much as \$1 billion.²²

²² U.S. Congressional Budget Office, Cost Estimate, H.R. 5835, Veterans Identity and Credit Security Act of 2006, July 28, 2006, p.1.