Order Code RS22460
June 22, 2006

Theft of Veterans' Personal Information, and Department of Veterans Affairs Information Technology Reorganization: Issues for Congress

Sidath Viranga Panangala
Analyst in Social Legislation
Domestic Social Policy Division

Alison M. Smith
Legislative Attorney
American Law Division

Summary

The Department of Veterans Affairs (VA) recently reported a security breach in its cybersecurity system that resulted in the loss of veterans' personal information, including names, birthdates, and Social Security numbers. According to the VA, at this time there have been no reports of identity theft resulting from the loss of the data, and the agency has announced that it will provide one year of free credit monitoring to veterans whose information was stolen. This loss of data has raised several important issues for Congress, including providing immediate relief to veterans that may be affected by the breach of data, as well as reorganization of the VA information technology (IT) system so that such incidents may be avoided in the future. This report will be updated as events warrant.

Background

On May 3, 2006, the home of a Department of Veterans Affairs (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 employee 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] According to the VA, at this time there have been no reports of identity theft resulting from the loss of the data. On June 7, 2006, the VA issued DIRECTIVE 6504 *Restrictions on Transmission, Transportation and Use Of, and Access To, VA Data Outside VA Facilities.* This directive established a new policy that, among other things, restricts VA employees from transmitting, transporting, and accessing agency data while working in locations outside VA facilities.[3] On June 21, the VA announced that it will provide one year of free credit monitoring to veterans whose personal information may have been compromised due to this theft.

Last month's VA data theft comes at a time when the agency'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.[4] 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.[5] 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 computer security at its medical facilities.[6] 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

---

[1] Testimony of the Inspector General of the Department of Veterans Affairs, George J. Opfer, and testimony of the Secretary of Veterans Affairs, James Nicholson, 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 Cong., 2nd sess., May 25, 2006. Ann Scott Tyson and Christopher Lee, "Data Theft Affected Most in Military; National Security Concerns Raised" *Washington Post*, June 7, 2006, Final Edition, A Section, 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 Cong., 2nd sess., May 25, 2006.

[3] Available at [http://www.va.gov/pubs/directives/Information-Resources-Management-(IRM)/6504dir06.htm], visited June 19, 2006.

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

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

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

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."[7] 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."[8] 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.[9]

The remainder of this report provides a brief chronology of events that took place from the time the VA data analyst discovered the burglary to the time the theft was announced publicly by the VA, a summary of data security legislation that has been introduced in Congress, a discussion of some long-term issues for Congress, and a brief discussion of VA information technology (IT) reorganization issues as they relate to improving the VA cybersecurity system.

Chronology of Events

On May 3, 2006, the home of a VA employee was burglarized. The employee discovered the theft upon returning home that afternoon and immediately notified VA's Deputy Assistant Secretary (DAS) for Policy. On May 4, the DAS met with the Information and Privacy Security Officer (ISO) in the office of policy and with the Acting Director of the Data and Management Service to discuss issues related to the data theft and to review notification procedures. On May 5, the ISO notified the Acting Assistant Secretary (AAS) for Policy and Planning about the data theft. The AAS asked the ISO to prepare a memo that identified and catalogued the specific data files that had been compromised and the number and type of specific identifiers that may have been lost. On May 9, AAS informed VA's Chief of Staff about the potential loss of veterans' personal information. The Chief of Staff asked AAS to prepare a memorandum on the loss of data. On May 10, the Chief of Staff informed the Deputy Secretary about the incident. That

---

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

[8] 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.

[9] 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 Employee*, 109th Cong., 2nd sess., June 14, 2006.

same day, an information security officer from the VA OIG's office was attending a regularly scheduled ISO monthly meeting. During that meeting, one of the ISOs mentioned that a VA employee had lost data that had been stolen from his residence. That officer reported to his supervisor, and the next day it was reported to OIG's Office of Investigations. The Chief of Staff informed Secretary Nicholson about the theft on May 16. That same day, Secretary Nicholson informed the White House, and on May 22, almost three weeks after the burglary, VA publicly announced the data theft.[10]

Legislative Proposals on Data Security

A number of legislative proposals have been introduced in both the House and Senate to address some of the issues arising from this 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.

Issues for Congress

The theft of veterans' personal information raises important questions for Congress. First, what is the long-term cost of providing credit monitoring and other services for veterans whose personal information may be used fraudulently? Initial estimates range

---

[10] Based on testimony of James Nicholson, R. Allen Pittman, Robert J. Henke, Pedro Cadenas Jr., Dennis M. Duffy, Tim S. McClain, George J. Opfer, Jon Wooditch, and Michael Staley 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 Cong., 2nd sess., May 25, 2006.

from $100 million to $500 million.[11] It has also been reported that since the data theft, VA has spent about $1 million for printing and about $6 million for postage to mail letters to veterans informing them of the data theft.[12] Moreover, about $200,000 a day is spent to operate a call center for veterans seeking information. Second, what are the potential legal implications that could arise as a result of veterans suing the government? Five veterans' service organizations have filed a class-action lawsuit against the VA over the theft of the personal data. The suit seeks $1,000 in damages for each of the 26.5 million veterans. The House Veterans' Affairs Committee has broached the idea of a special claims adjudication process that would speed resolution of claims made by veterans who suspect that they were victims of identity theft. Beyond the immediate need to provide relief to veterans who may be affected by this theft, Congress may also opt to address the broader issue of information technology management and long-standing information security vulnerabilities at the VA and other federal agencies.

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) — an integrated financial and logistics systems management software — at the Bay Pines Medical Center in Florida.[13]

In 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. Following a briefing on the Gartner report, VA senior management, in October 2005, adopted the federated model presented in that report as the best model to reorganize the management of the VA IT. It should be noted that since July 1990, the VA has had a decentralized system of IT development and management. Each of the three administrations within the VA — VHA, the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA) — developed and managed its own IT functions.

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

---

[11] Testimony of Secretary of Veterans Affairs James Nicholson to a question posed by Congressman Cliff Stearns 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 Cong., 2nd sess., May 25, 2006.

[12] Daniel Pulliam, "VA Spends More Than $14 Million Handling Data Breach," *Government Executive,* available at [http://www.govexec.com/dailyfed/0606/062006p1.htm], visited June 21, 2006.

[13] 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 1st sess.*, Oct. 20, 2005.

supervision of the Chief Information Officer (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.[14]

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 would mandate 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.[15] H.R. 4061 passed the full House on November 2, 2005. There has been no Senate action on this bill.

The House and Senate Appropriations Committees have also expressed concern about the management of the VA's IT program. According to the Senate 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."[16] 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 HealtheVet-VistA project until the VA receives approval from the House and Senate Appropriations Committees on its expenditure plan for the project.[17]

---

[14] 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.

[15] 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 Cong., 1st sess., H.Rept. 109-256, p. 5.

[16] U.S. Congress, Conference Committees, *Military Quality of Life and Veterans Affairs Appropriations Act, 2006*, conference report to accompany H.R. 2528, 109th Cong., 1st sess., H.Rept. 109-305, p.56.

[17] HealtheVet-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.