



Department of Veterans Affairs Office of Inspector General

Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans

**To Report Suspected Wrongdoing in VA Programs and Operations
Call the OIG Hotline – (800) 488-8244**

Contents

	Page
Executive Summary	i
Introduction	1
Purpose	1
Background.....	1
Scope and Methodology	2
Results and Conclusions	3
Issue 1: Whether the Employee Had an Official Need to Access the Data That Was Stolen, Whether He Was Authorized to Take It Home, and Whether It Was Properly Safeguarded	3
Issue 2: Whether the Response of Managers and Senior Executives in the Office of Policy, Planning, and Preparedness to the Notification of the Stolen Data Was Appropriate and Timely	10
Issue 3: Whether the Secretary’s Immediate Staff Demonstrated a Lack of Urgency in Notifying the Secretary	17
Issue 4: Whether Information Security Officials Effectively Triggered Appropriate Notifications and an Investigation of the Stolen Data	22
Issue 5: Whether VA Policies Safeguard VA Information	27
Issue 6: Whether Audits and Reviews of VA’s Information Management Security Program Controls Continue to Identify Vulnerabilities.....	43
Appendixes	
A. Secretary’s Comments	52
B. Report Distribution.....	68

Executive Summary

Introduction

On May 3, 2006, the home of a VA employee was burglarized resulting in the theft of a personally-owned laptop computer and an external hard drive, which was reported to contain personal information on approximately 26 million veterans and United States military personnel. The VA Secretary was not informed of the incident until May 16, 2006, almost 2 weeks after the data was stolen. The Congress and veterans were not notified until May 22, 2006.

The Office of Inspector General (OIG) initiated this review to determine: (1) whether the employee had an official need to access the data that was stolen, whether he was authorized to take it home, and whether it was properly safeguarded; (2) whether proper notifications of the stolen data were made, and whether those notifications were pursued in an appropriate and timely manner; (3) whether VA had policies and procedures in place to safeguard personal and proprietary information maintained by VA; and (4) whether VA had sufficiently addressed long-standing OIG reported information security weaknesses. The Senate and House veterans' affairs committees, as well as several other members of Congress, have expressed considerable interest in this review.

The burglary was reported to the local police. When the employee discovered that the computer equipment was among the items stolen, he immediately notified VA management in the Office of Policy, Planning, and Preparedness, including Security and Law Enforcement personnel. The employee advised all of them that the stolen personal computer equipment contained VA data.

Results

Employee Not Authorized to Take VA Data Home

Because the employee was responsible for planning and designing analytical projects and supporting surveys involving all aspects of VA policies and programs, he was authorized access to, and use of, VA databases. The employee explained that much of the data that he had stored on the stolen external hard drive was for his "fascination project" that he self-initiated and worked on at home during his own time.

Because of past criticism on the reliability of the National Survey of Veterans, his project focused on identifying approximately 7,000 veterans who participated in the 2001 survey, in order to compare the accuracy of their responses with information VA already had on file. He began the project in 2003, but could not recall spending time working on it during 2006.

To conduct this project, the employee took home vast amounts of VA data and loaded it on an external hard drive. The stolen laptop did not contain VA data. The employee reported that the external hard drive that was stolen likely included large record extracts from the Beneficiary Identification and Records Locator Subsystem (BIRLS) that contained records on approximately 26 million living veterans. The extract contained veterans' social security numbers, full names, birth dates, service numbers, and combined degree of disability. He also reported that the stolen hard drive likely contained an extract of the August 2005 Compensation and Pension (C&P) file, containing personal identifiers of over 2.8 million living veterans.

While the employee had authorization to access and use large VA databases containing veterans' personal identifiers in the performance of his official duties, his supervisors and managers were not aware that he was working on the project, and acknowledged that if they had, they would not have authorized him to take such large amounts of VA data home. In fact, one manager could not justify taking such a large amount of data home under any circumstances.

By storing the files on his personal external hard drive and leaving it unattended, the employee failed to properly safeguard the data and unnecessarily exposed it to risks greater than those existing in the workplace. While the employee stored the laptop and the external hard drive in separate areas of the house, he acknowledged that he took security of the data for granted.

The loss of VA data was possible because the employee used extremely poor judgment when he decided to take personal information pertaining to millions of veterans out of the office and store it in his house, without encrypting or password protecting the data. This serious error in judgment is one for which the employee is personally accountable. The Department has already proposed administrative action.

An Assistant United States Attorney has declined prosecution of the employee for any criminal activity on his part relating to taking VA data to his home. The OIG, in coordination with the Federal Bureau of Investigation (FBI) and the Montgomery County Police Department in Maryland, are continuing to pursue the criminal investigation into the burglary. On June 28, 2006, the stolen laptop computer and external hard drive were recovered intact. Based on all the facts gathered thus far during the investigation, as well as the results of computer forensics examinations, the FBI and OIG are highly confident that the files on the external hard drive were not compromised after the burglary.

Processing the Notification of the Stolen Data Was Not Appropriate or Timely

Despite Mr. Michael McLendon, Deputy Assistant Secretary for Policy, being notified of the theft and loss of VA data on May 3, 2006, it was not until May 5, 2006, that the Information Security Officer (ISO) for OPP&P interviewed the employee to determine more facts about the loss. The ISO reported that the employee was so flustered he decided not to discuss the matter; rather he had directed the employee to write down

what data was lost. The employee's written account of the lost data was essentially an identification of database extracts with little quantified information concerning the significance or magnitude of the incident. This is important because this document served as the basis for all further notifications in VA up to, and including, the Deputy Secretary.

Mr. McLendon received the report of the stolen data from the OPP&P ISO on May 5, 2006. Instead of providing the report to higher management, Mr. McLendon advised his supervisor, Mr. Dennis Duffy, Acting Assistant Secretary for Policy, Planning, and Preparedness, of his intent to rewrite the report because it was inadequate and did not appropriately address the event. He submitted his revised report to Mr. Duffy on May 8, 2006.

Our review of Mr. McLendon's revisions determined that his changes were an attempt to mitigate the risk of misuse of the stolen data. He focused on adding information that most of the critical data was stored in files protected by a statistical software program, making it difficult to access. This, however, was not the case because we were able to display and print portions of the formatted data without using the software program. Mr. McLendon made these revisions without consulting the programming expert on his staff or with the employee who reported the stolen data. Mr. Duffy provided the report to Mr. Thomas Bowman, VA Chief of Staff, on May 10, 2006. Mr. Duffy also did not attempt to determine the magnitude of the stolen data nor did he talk to the employee.

Mr. McLendon did not inform his direct supervisor, Mr. Duffy, when he learned of the incident on May 3, 2006. Mr. Duffy advised us that he did not learn of the theft until Friday morning, May 5, 2006, when he spoke with the OPP&P ISO, in what Mr. Duffy described as a rather "casual hallway meeting."

Mr. Duffy did not discuss the matter initially with Mr. McLendon, noting that there had been a long and very strained relationship with him. Mr. Duffy said that Mr. McLendon had a very strong belief that, as a political appointee, he reported in some fashion to the Secretary and that there was no need for a "careerist" to supervise him. Mr. McLendon characterized the office as one of the most dysfunctional organizations in VA, and that it was one of the most hostile work environments he ever worked in.

Mr. Duffy said he just did not perceive this as a crisis. In hindsight, he added that his greatest regret is that he "failed to recognize the magnitude of the whole thing." Both Mr. Duffy and Mr. McLendon bear responsibility for the impact that their strained relationship, which both acknowledged, may have had on the operations of the office in handling the aftermath of the incident.

We also concluded that Mr. John Baffa, Deputy Assistant Secretary for Security and Law Enforcement, who was notified of the incident on May 4, 2006, also failed to take appropriate action to determine the magnitude and significance of the stolen VA data.

Mr. Duffy notified Mr. Bowman of the data theft on May 9, 2006, and followed up with the report the next day. Shortly thereafter, Mr. Bowman provided it to Mr. Jack Thompson, Deputy General Counsel, and asked him to provide an assessment of the agency's duties and responsibilities to notify individuals whose identifying information was compromised. On May 10, 2006, Mr. Bowman informed Mr. Gordon Mansfield, Deputy Secretary, of the burglary and the stolen VA data.

It was not until the morning of May 16, 2006, after the Chief of Staff was informed by the Inspector General that the stolen data most likely contained records with personal identifiers on approximately 26 million records, that Mr. Bowman notified the Secretary of the theft and magnitude of the lost data.

The delay in notifying the Secretary was spent waiting for legal advice from the Office of General Counsel (OGC). This 6-day delay can be attributed to a lack of urgency on the part of those requesting this advice and those responsible for providing the response. This is not to say that everyone who was notified of the incident failed to recognize the importance of this matter, but no one clearly identified it as a high priority item and no one followed up on the status of the request until after the May 16, 2006, call from the Inspector General.

Although Mr. Bowman acknowledged he knew the VA data stolen could affect the records of millions of veterans, he demonstrated no urgency in notifying the Secretary. He notified the Deputy Secretary the day after he learned of the loss. While the Deputy Secretary does not recall discussing the magnitude of the number of veterans affected by the theft, he too decided not to raise the issue to the Secretary until they knew more information on what VA's legal responsibilities were and more about the magnitude of the problem. Once again, no one attempted to contact the employee who reported the theft to determine the magnitude of the lost data. The OIG was able to determine the extent of the stolen data after one interview with the employee on May 15, 2006.

Information Security Officials Acted with Indifference and Little Sense of Urgency

On May 5, 2006, the OPP&P ISO forwarded information concerning the theft of the data to the District ISO, who is responsible for coordinating ISO activities among VA Central Office staff offices. He also submitted it to the Security Operations Center (SOC), Office of Information and Technology, which has responsibility for assessing and resolving reported information security incidents. However, the OPP&P ISO's incident report had significant errors and omissions, and information security officials did not adequately attempt to identify the magnitude of the incident or elevate it until overtaken by the events on May 16, 2006.

At nearly every step, VA information security officials with responsibility for receiving, assessing, investigating, or notifying higher level officials of the data loss reacted with indifference and little sense of urgency or responsibility. At no time did the District ISO or SOC attempt to interview the employee who reported the data stolen to clarify

omissions in the OPP&P ISO's report or to gain a better understanding of the scope and severity of the potential data loss. While the District ISO elevated the matter to Mr. Johnny Davis, Acting Associate Deputy Assistant Secretary for Cyber Security Operations, this occurred as another "hallway conversation," and he was not provided any details on the nature of the missing data. No further notifications were made up the chain-of-command.

Twelve days after receiving the original incident report, the SOC had made no meaningful progress in assessing the magnitude of the event and, ironically, had passed responsibility to gather information on the incident back to the OPP&P ISO to review it as a possible privacy violation, an area outside the jurisdiction of the SOC. The OPP&P ISO also serves as the Privacy Officer.

Policies and Procedures Do Not Adequately Protect Personal or Proprietary Data

The potential disclosure of Privacy Act protected information resulting from the theft of an employee's personal hard drive raised the issue of whether VA policies adequately safeguard information that is not stored on a VA automated system. Based on our review of VA policies that existed at the time of the incident; policies that have been issued since the incident; and interviews with VA employees Chief Information Officers, Privacy Officers, and ISOs; we concluded that VA policies, procedures, and practices do not adequately safeguard personal or proprietary information used by VA employees and contractors.

We 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.

The loss of protected information not stored on a VA automated system highlighted a gap between VA policies implementing information laws and those implementing information security laws. We found that policies implementing information laws focus on identifying what information is to be protected and the conditions for disclosure; whereas, policies implementing information security laws focus on protecting VA automated systems from unauthorized intrusions and viruses. As a result, VA did not have policies in place at the time of the incident to safeguard protected information not stored on a VA automated system.

Although policies implemented by the Secretary since the incident are a positive step, we determined that more needs to be done to ensure protected information is adequately safeguarded. We found that VA's mandated Cyber Security and Privacy Awareness training are not sufficient to ensure that VA and contract employees are familiar with the applicable laws, regulations, and policies. We also found that position sensitivity levels designations for VA and contract employees are either not done or are not accurate. In addition, we found that VA contracts do not contain terms and conditions to adequately safeguard protected information provided to contractors.

We determined that VA needs to enhance its policies for identifying and reporting incidents involving information violations and information security violations to ensure that incidents are promptly and thoroughly investigated; the magnitude of the potential loss is properly evaluated; and that VA management, appropriate law enforcement entities, and individuals and entities potentially affected by the incident are notified in a timely manner.

Information Security Control Weaknesses Remain Uncorrected

For the past several years, we have reported vulnerabilities with information technology security controls in our Consolidated Financial Statements audit reports, Federal Information Security Management Act audit reports, and Combined Assessment Program reports. The recurring themes in these reports support the need for a centralized approach to achieve standardization, remediation of identified weaknesses, and a clear chain-of-command and accountability structure for information security. Each year, we continue to identify repeat deficiencies and repeat recommendations that remain unimplemented. These recommendations, among other issues, highlight the need to address security vulnerabilities of unauthorized access and misuse of sensitive data, the accuracy of position sensitivity levels, timeliness of background investigations, and cyber security and privacy awareness training. We have also reported information technology security as a Major Management Challenge for the Department each year for the past 6 years.

Recommendations

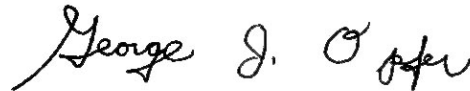
We recommend that the Secretary:

- Take whatever administrative action deemed appropriate concerning the individuals involved in the inappropriate and untimely handling of the notification of stolen VA data involving the personal identifiers of millions of veterans.
- Establish one clear, concise VA policy on safeguarding protected information when stored or not stored in VA automated systems, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.
- Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.
- Ensure that all position descriptions are evaluated and have proper sensitivity level designations, that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and automated systems, and that all required background checks are completed in a timely manner.

- Establish VA-wide policy for contracts for services that requires access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored, or processed on non-VA automated systems is safeguarded.
- Establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

Comments

The Secretary agreed with the findings and recommendations and provided acceptable improvement plans. See Appendix A for the Secretary's response and implementation plans for each recommendation. For the Secretary's complete response, including the attachments, please refer to the enclosed computer disk. We will follow up on the implementation of the recommendations until they are completed.



GEORGE J. OPFER
Inspector General

Introduction

Purpose

The VA Office of Inspector General (OIG) investigated the circumstances surrounding the theft of VA records containing veterans' and other individuals' personal identifiers, which were electronically stored in an employee's personal computer external hard drive maintained at the employee's residence. The purpose of this investigation was to determine the following:

- Whether the employee had an official need to access the data that was stolen, whether he was authorized to take it home, and whether it was properly safeguarded.
- Whether proper notifications of the stolen data were made, and whether those notifications were pursued in an appropriate and timely manner.
- Whether VA had adequate policies and procedures in place to safeguard personal and proprietary information maintained by VA.
- Whether VA has sufficiently addressed long-standing OIG reported information security weaknesses.

Background

On Wednesday, May 3, 2006, the home of a VA Information Technology Specialist, hereafter referred to as "the employee," was burglarized resulting in the theft of a personally-owned laptop computer and an external hard drive, which was reported to contain personal information on approximately 26 million veterans and United States military personnel.

The burglary was discovered by the employee's wife on the afternoon of May 3, 2006, who immediately reported it to the local police. When the employee arrived home on the day of the burglary shortly after 5:00 p.m. and discovered that the computer equipment was among the items stolen, he immediately notified Office of Policy, Planning, and Preparedness (OPP&P) management. He also notified the VA Office of Security and Law Enforcement, which is part of the OPP&P organization. The employee advised all of them that the stolen personal computer equipment contained VA data.

The VA Secretary was not informed of the incident until May 16, 2006, almost 2 weeks after the VA data was reported stolen. The delay in notifying the Secretary resulted in delays in notifying the Congress and veterans. The public announcement by VA did not occur until May 22, 2006, which was almost 3 weeks after the burglary occurred.

The employee works for OPP&P in VA Central Office (VACO). The employee was responsible for providing data analysis and statistical expertise to support the functions of OPP&P. Among other duties, OPP&P conducts independent analyses for VA decision makers regarding existing policies and programs, including administering a national statistical center to support the continuous enhancement of benefits and services to veterans. Projects can be requested by the employee's supervisors and managers, VA officials outside OPP&P, VA contractors, and entities external to VA, or self-initiated by the employee.

An Assistant United States Attorney has declined prosecution of the employee for any criminal activity on his part relating to taking VA data to his home. The OIG, in coordination with the FBI and the Montgomery County Police Department in Maryland, are continuing to pursue the criminal investigation into the burglary. On June 28, 2006, the stolen laptop computer and external hard drive were recovered intact. Based on all the facts gathered thus far during the investigation, as well as the results of computer forensics examinations, the FBI and OIG are highly confident that the files on the external hard drive were not compromised after the burglary.

Scope and Methodology

To address the objectives of this review, we interviewed the employee; his supervisors, project managers, and co-workers; privacy, information security, and VA law enforcement officials; VA Austin Automation Center (AAC) officials; Office of General Counsel (OGC) attorneys, including the General Counsel and Deputy General Counsel; the Chief of Staff; the Deputy Secretary; and other Department officials. We reviewed the employee's position description and performance standards; the local jurisdiction's police report of the theft; e-mail, notes, memoranda, and other documentation; chronologies of events prepared by the employee, OPP&P staff, OGC staff, and others; documentation of the employee's access to VA databases; the VA Security Operations Center (SOC) incident report; and other pertinent information. We reviewed cyber security and information security policies published by VA and its organizational components, relevant online training modules, and VA contract documents and contract administration records. We also conducted a forensic analysis of the contents of the compact disks (CDs) and other media the employee had at his home on the day of the burglary, as well as a forensic search of the contents of two other computers at his home.

Results and Conclusions

Issue 1: Whether the Employee Had an Official Need to Access the Data That Was Stolen, Whether He Was Authorized to Take It Home, and Whether It Was Properly Safeguarded

Findings

The employee reported having VA databases and other files containing veterans' personal identifiers on the external hard drive that was stolen from his home, including large record extracts from the Beneficiary Identification and Records Locator Subsystem (BIRLS) and the Compensation and Pension (C&P) file. BIRLS is a computer file of information concerning veterans and benefits. Among other purposes, it is used to determine the location of a veteran's file or to record a veteran's death. Some of the BIRLS database fields include name, social security number, military service number, claim number, date of birth, date of death, and dates of military service. BIRLS is not a national security system. The C&P file consists of records of veterans and beneficiaries receiving VA benefits, and includes database fields such as name, social security number, disability diagnostic codes and ratings, and addresses.

Because the employee was responsible for planning and designing analytical projects and supporting surveys involving all aspects of VA policies and programs, he was authorized access to, and use of, these and other large VA databases. However, at the time of the burglary he had no official need or permission to take the data home. In addition, he reported that the data stored on the stolen external hard drive was neither password-protected nor encrypted. The employee explained that much of the data that he had stored on the stolen external hard drive was for a "fascination project" that he self-initiated and worked on at home during his own time. It is important to note, however, that this self-initiated project was related to VA and, if the employee was successful in accomplishing his goal, he believed it would be of benefit to VA decision makers. His supervisors or managers were not aware that he was working on the fascination project, and acknowledged that if they did, they would not have authorized him to take such large amounts of VA data home.

The Employee Had an Official Need to Use Large VA Databases

According to the employee's current position description, he is responsible for designing and programming information systems and databases "comprised of millions of records" to facilitate analyses used by senior VA officials for policy consideration. He is responsible for planning and designing analytical projects and studies to improve the management of databases and for supporting ongoing VA surveys. The employee is expected to plan and execute his assignments independently and to initiate projects and methods of analyzing large databases. The position description notes, in particular, that the incumbent supports in-house analyses on the data collected through the National Survey of Veterans (NSV). His performance standards for the 12-month period ending

September 30, 2006, included providing computer specialist expertise to support the administration of the NSV and to support a program of research to continually enhance the veteran survey program.

We confirmed that he used VA data in a multitude of analytical projects requiring access to major VA databases that contain personal information involving millions of veterans, and that access to these databases was requested and granted for official purposes. For example:

- In February 2002, the Veterans Health Administration (VHA) approved giving the employee access to an extract of its National Enrollment Data file, which includes a list of all veterans enrolled to receive VA medical care. The extract includes such identifiers as name, date of birth, address, social security number, and enrollment status and priority. Access was granted for the purpose of supporting national reporting of enrollment data.
- In August 2005, the employee obtained access to the full C&P file, which the AAC provided to OPP&P so it could review issues related to the OIG report, *Review of State Variances in Disability Compensation Payments*, issued May 19, 2005 (Report No. 05-00765-137).
- In October 2005, based on Veterans Benefits Administration (VBA) approval, the AAC gave the employee access to an extract of the BIRLS file. Mr. Dat Tran, Acting Director of the Data Management and Analysis Service in OPP&P and one of the employee's project managers, requested the access, stating that, "We are frequently required to conduct data cross matching across various VA databases and the BIRLS is a key database that we would like to have access to." Mr. Tran also specifically noted in the request for access the employee's data matching efforts to help identify veterans exposed to mustard gas.

We also confirmed that the employee used these and other databases for authorized purposes. Following are some examples:

- In October 2004, using the NSV database provided by the contractor who conducted the survey, the employee responded to a request from VHA for information on the insurance coverage of veterans who received VA inpatient, outpatient, and emergency room care, by priority status.
- In April 2005, as part of an OPP&P ongoing analysis of recipients of the Vocational Rehabilitation and Employment Program, the employee prepared frequency distributions on demographic variables, military service, and disabilities for veterans entitled and not entitled to such program services, and matched the social security numbers of veterans in both groups against the C&P file.

- In August 2005, he prepared a spreadsheet for the Congressional Budget Office showing VA disability compensation by percentage of disability, using the C&P file and the NSV database.

Some of the employee's recently requested and ongoing work that required access and use of large VA databases included:

- An employability research study using the C&P file to compare veterans who had discontinued their involvement in the vocational rehabilitation program with the veterans' degree of disability.
- A project working with the Institute for Defense Analyses (IDA), which was conducting a study of the geographical variations in compensation payments to veterans, to provide IDA an extract with scrambled social security numbers which was based on information in BIRLS. The employee was working on this project shortly before he reported his house had been burglarized.

The employee described to us the projects he had been working on at his home using most of the files he had stored on his stolen external hard drive. One project involved the 2001 NSV. The employee said that the contractor responsible for conducting the survey contacted approximately 7,000 of the 14,000 veterans whose names they sampled from VA files (veterans who were receiving VA benefits or health care) but, rather than providing OPP&P the social security numbers of only those veterans contacted, they provided all 14,000 social security numbers. The employee told us he was attempting to identify the 7,000 veterans actually contacted so he could compare their survey responses with information VA already had on file about them. He said he wanted to determine the extent to which the responses were accurate because OPP&P had received much criticism regarding the reliability of the survey.

The employee told us the survey data included the telephone numbers of all veterans contacted so he was able to begin the identification process by comparing those telephone numbers with numbers in the VA files from which the sample was taken. He said he then used a 2001 online reverse telephone directory to continue identifying other veterans. The employee explained that if he judged a name and address in the reverse telephone directory to match a name and address of one of the 14,000 veterans, he inserted the veteran's social security number into his file.

The employee told us he was personally interested in the process of identifying the approximately 7,000 veterans, referring to the effort as his "fascination project." He said he began the project in 2003, but could not recall spending time working on it during calendar year 2006. According to the employee, he worked on the project at home because it was very time-consuming and he could not devote sufficient time to it at the office. He said he was willing to invest his own time to see if he could make progress in identifying the veterans. The employee told us he never came up with a list of veterans that he considered to be adequately matched.

Ms. Susan Krumhaus, OPP&P Project Manager for the NSV, told us she worked with the employee on the survey until sometime in 2004. She said the two of them wanted to validate survey responses to determine, for example, if veterans experienced memory lapses while taking the survey and what could be done to improve that. However, she said the validation the employee was doing occurred several years ago, and she was not aware that he was working on the project in May 2006.

Mr. Michael McLendon, Deputy Assistant Secretary for Policy and the employee's second-level supervisor, told us the NSV is the largest survey of veterans conducted, and the only source for certain data to characterize the veteran population. He said he assumed the employee was attempting to match survey veterans with veterans in the C&P database or in other records to obtain additional information about them and their cohort group. He noted that VA did not have good integrated data to profile different cohorts of veterans, and that he believed any attempt to give the agency better insight into the veteran population by matching the survey data with information already in VA databases was a legitimate work effort, although he was unaware of the project.

The employee described a second project involving files he had saved on his stolen hard drive. He said he had attempted to identify veterans exposed to mustard gas and other hazardous material, most of whose names, but not social security numbers, were in a Department of Defense (DoD) data file he received from VBA. The employee told us that once a veteran was identified, he provided the veteran's social security number to C&P Service so VBA could begin outreach efforts. According to the employee, the January 2006 extract of the BIRLS file he had taken to his home provided him, for the first time, veterans' service numbers and by matching those numbers with service numbers in the mustard gas file he could then determine, from the BIRLS file, the veterans' social security numbers. Mr. Dat Tran, Acting Director, Data Management and Analysis Service, confirmed that OPP&P was asked to help identify veterans DoD included in its mustard gas file, and that he assigned the project to the employee.

Part of the issue of who knew what concerning the work of the employee was that it was not clear who actually supervised him. For example, in a recent memorandum from Mr. Tran, he makes the point that even though the employee stated that he was his supervisor, he was not. Mr. Tran said they were colleagues and that Mr. Michael Moore performs the supervisory functions of the employee. While Mr. Moore is the employee's first-line supervisor, he admitted that he had no idea what projects the employee was assigned, nor did he have any understanding of the size or contents of the databases with which the employee routinely worked. According to Mr. McLendon, Mr. Moore was given responsibility for first-line supervision of the employee as a result of the reassignment of personnel that occurred because of intense disagreement between Mr. Dennis Duffy, Acting Assistant Secretary for OPP&P, and himself.

The Employee Had No Official Need to Have the Data at Home

As discussed in Issue 5 of this report, VA regulations require that VA will safeguard an individual against the invasion of personal privacy (38 C.F.R. 1.576). However, we

could not identify any VA policy that specified how protected information not maintained on a VA automated system should be safeguarded, particularly when it is removed from the workplace.

The employee told us he had been taking data containing personal identifiers home since 2003, never asked anyone's permission to do so and, to his knowledge, no one was aware he had it at home. The employee noted, however, that he was issued a VA laptop computer in 2004 and 2005, along with remote access to VA's virtual private network (VPN) and frequently took the laptop, with personal identifiers in it, home, and that his supervisors were aware of it.

According to the employee, when he turned in his VA laptop in January 2006 he continued to take work home and began using a personal laptop and external hard drive, which he had purchased in mid-2005. He used CDs, Digital Versatile Discs (DVDs), floppy disks, and, more recently, a personal flash drive to transport VA data home, where he transferred it to his personal external hard drive. He said he did not believe the information he saved to his external hard drive was at risk because he was careful not to access the Internet with the external hard drive connected to his laptop. He also stored the external hard drive and his laptop in separate parts of his house with the hard drive hidden from view, but acknowledged he took the physical security of the VA data for granted. The employee advised us that he did not store VA data on his personal laptop, but did store unencrypted VA data without password protection on the external hard drive.

Mr. Tran told us the employee never told him he took data with personal identifiers home and he was not aware the employee had done so. On May 17, 2006, Mr. Tran wrote a short statement for VA management noting that the employee's action was self-initiated, and not at the direction of OPP&P management.

Of particular note is the fact that OPP&P managers characterize the employee as a very motivated, hard-working, and dedicated individual who worked long hours and produced meticulous work. The employee was described as a detailed and comprehensive analyst with respect to programming and analyzing data. For his most recent performance appraisal period, the employee was rated "Outstanding," the highest rating in VA's performance appraisal system. He also received a monetary award for his accomplishments in December 2005.

The Employee Likely Had Large VA Databases on His Stolen External Hard Drive

According to the employee, he may have had six files containing VA data stored on his stolen external hard drive. He said he had attempted to recall which files may have been on the external hard drive based on what he knew was on a flash drive and some CDs he had at his home, none of which were stolen, and based on what he knew he had been working on at home. The six files were:

- A BIRLS extract, with information as of January 2006, containing approximately 26 million records. According to the employee, 19.6 million of those records contained social security numbers. Additionally, the employee stated that the extract contained information such as the veteran's full name, date of birth, service number(s), and combined degree of disability. The employee stated he was certain he transferred the file from his VA desktop computer to his personal hard drive, but he could not recall if he had deleted it before the burglary.
- An extract of the August 2005 C&P file, containing social security numbers, matched with veterans' full names and dates of birth from BIRLS, and containing records of over 2.8 million living veterans.
- A file containing information obtained from veterans during the 2001 NSV. Data collected included socio-demographic and economic characteristics, military background, health status, VA benefit usage, and anticipated burial plans. According to the employee, this file contained records, all of which included telephone numbers, on over 20,000 veterans. He stated the records included responses received from the survey questions and contained over 6,200 social security numbers.
- A file extracted from both the VHA National Enrollment Data file and the C&P file. The file represented the population from which some veterans were sampled during the NSV (other veterans were selected based on random telephone dialing). According to the employee, the file contained over 5.5 million records, containing the veteran's address, date of birth, claim number, combined degree of disability, enrollment priority, social security number, and telephone number.
- A file the employee created matching veterans' names and addresses contained in the above NSV sample frame with names and addresses contained in a reverse telephone directory look-up file. The employee did not quantify the number of veteran records in this file, but noted that some records may have contained social security numbers.
- A file of over 6,700 service members and civilians who, according to DoD, had been exposed to mustard gas and other substances. According to the employee, many entries contained service numbers but few included social security numbers. He stated that information on a veteran may have included name; date of birth; exposure type, site, and date; service connected percentage; and diagnostic codes.

We determined that the above files, numbers of records, and identifying information were on the CDs, flash drive, and other media the employee had at his home at the time of the burglary, and thus could have been on his stolen hard drive. Subsequently, it was determined that as many as 2.2 million U.S. military personnel could have been in

the BIRLS data that was stolen, including 1.1 million active duty personnel, 430,000 National Guard members, and 645,000 reserve members.

The employee noted, and we confirmed, that he had a file on his flash drive containing data extracted from the VHA patient treatment file regarding a single veteran who visited VA health care facilities on 57 different dates. The file of the deceased veteran contained a partial social security number and diagnostic codes describing each visit. The employee said he did not believe this file was transferred to his hard drive because he used it only to debug a program to summarize such information and said the file was of no further use to him. Regarding another file found on one of the employee's CDs, he told us it pertained to a project he was working on using vocational rehabilitation data and said he did not believe it was on his stolen hard drive because he had no interest in working on that project at home.

Conclusion

While the employee had authorization to access and use large VA databases containing veterans' personal identifiers in the performance of his official duties, he had no need or authorization to take the data home. However, by storing the files on his personal external hard drive and leaving it unattended, the employee failed to properly safeguard the data and unnecessarily exposed it to risks greater than those existing in the workplace. While much has been made about the burglary of the employee's home and theft of the external hard drive, the loss of VA data was possible because the employee used extremely poor judgment when he decided to take personal information pertaining to millions of veterans out of the office and store it in his house without password protecting and encrypting the data. The employee is personally accountable for this serious error in judgment. The Department has already proposed administrative action.

Issue 2: Whether the Response of Managers and Senior Executives in OPP&P to the Notification of the Stolen Data Was Appropriate and Timely

Findings

Although senior managers and other staff in OPP&P were informed of the possible loss of VA data on May 3, 2006, the date of the burglary at the employee's home, the incident was not communicated up the chain-of-command until the VA Chief of Staff was notified 6 days later on May 9, 2006. This delay occurred in large part because senior executives in OPP&P failed to take appropriate and timely action to determine the extent and scope of the stolen data. Furthermore, VA Security and Law Enforcement officials focused on whether VA "equipment" had been stolen and not on the fact that the theft included VA information. Finally, OPP&P executives erroneously assumed that the SOC was sufficiently addressing the reported data loss and would make appropriate notifications.

OPP&P Officials Waited 6 Days before Notifying the Office of the Secretary and Failed to Determine the Magnitude of the Data Loss

Upon discovering the theft of his personally-owned laptop computer and external hard drive on May 3, 2006, the employee telephoned his office around 5:00 p.m. to report the burglary and data theft. During the next couple of hours, the employee talked to Mr. McLendon, Mr. Tran, and Mr. Kevin Doyle, Security and Law Enforcement Police Operations Team Leader. The employee told us that he advised each of them about the burglary and possible theft of VA data.

Shortly after 5:00 p.m., the first person the employee talked to was Mr. Doyle. Mr. Doyle's recollection of the call was that the employee only told him that he had a burglary at his home and that he had personal property missing. Mr. Doyle told us he did not remember being told anything about VA data. He added that the caller was very upset and noted that this could be "a career-ending incident," but did not get the employee's name because he was on a Metro train when he took the call. Mr. Doyle recalls telling the caller that since the incident did not occur at VA and no VA property was taken, the caller needed to coordinate through his local police department. Mr. Doyle said he did not query the individual further for details, and the call only lasted a couple of minutes. Mr. Doyle told us that because he was on annual leave the next day, he telephoned Mr. John Baffa, Deputy Assistant Secretary for Security and Law Enforcement, to ask if anyone reported a burglary or a missing computer.

The employee's recollection of this call was that he did tell Mr. Doyle that the stolen computer equipment had VA data on it. When questioned further about what he told Mr. Doyle, the employee said, "I wouldn't just report the theft of my private property to him." Also, when we interviewed Mr. Baffa, he testified that Mr. Doyle told him the next day that the employee told him that there might have been some VA material on the stolen computer equipment.

About 5:30 p.m., the employee then talked to Mr. McLendon. Mr. McLendon stated that the employee was very upset about the incident and that the local police were still at the employee's residence. According to Mr. McLendon, he did not discuss the specific type or amount of data possibly located on the stolen external hard drive with the employee because, "There was no way to have a detailed dialogue at that time about what data was missing." Mr. McLendon told the employee to take the next day off to deal with the burglary, and never personally followed up with the employee again.

Around 6:45 p.m., Mr. Tran telephoned the employee to obtain a better sense about the data theft. The employee advised Mr. Tran that he believed that the stolen external hard drive potentially had a copy of a BIRLS extract that he had downloaded from the AAC. Mr. Tran did not attempt to obtain any further information at that time, nor did he have a follow-up conversation with the employee until May 8, 2005.

On Thursday, May 4, 2006, Mr. Tran advised Mr. McLendon and the OPP&P Information Security Officer (ISO) that the employee believed that a copy of a BIRLS extract was probably on the external hard drive that was stolen. At the direction of Mr. McLendon, Mr. Tran met with the ISO, who also serves as the Privacy Officer (PO) for OPP&P, to identify what action was required. No further significant action was taken that day since the employee was at home, and no notifications were made to senior VA management officials.

Despite being notified of the loss of VA data on May 3, 2006, Mr. McLendon did not inform his direct supervisor, Mr. Duffy. Mr. Duffy advised us that he did not learn of the theft until Friday morning, May 5, 2006, around 9:45 a.m., when he spoke with the OPP&P ISO, in what Mr. Duffy described as a rather "casual hallway meeting." The ISO advised Mr. Duffy of the circumstances surrounding the burglary and theft of protected veteran data, and indicated that he was working with Mr. McLendon and Mr. Tran on the matter.

When we asked Mr. Duffy if he discussed the matter with Mr. McLendon on May 5, 2006, he said no, noting that there had been a long and very strained relationship with him. Mr. Duffy said that Mr. McLendon had a very strong belief that, as a political appointee, he reported in some fashion to the Secretary and that there was no need for a careerist to supervise him. Mr. McLendon characterized the OPP&P as one of the most dysfunctional organizations in VA, and that it was one of the most hostile work environments "he ever set foot in."

During the hallway conversation with Mr. Duffy, the OPP&P ISO also stated that he had notified the SOC as part of his ISO duties and responsibilities. Mr. Duffy recalled directing the ISO to provide him with as comprehensive a list as he could of the data sets and the specific personal identifier data elements that were believed to have been stolen and the magnitude. We determined that Mr. Duffy later briefed the VA Chief of Staff on the stolen data without following up to determine if a comprehensive list was developed or if the magnitude of the loss was determined.

When asked why no one in OPP&P attempted to quantify the loss until directed to do so on May 16, 2006, by OGC, Mr. Tran stated that they followed the prescribed procedure issued by Cyber Security or the SOC, that basically says when you have an incident you report it your ISO, and then your ISO will follow the prescribed process. Mr. Tran's assertions that he was unfamiliar with the size of the BIRLS extract are undermined by an e-mail sent to him by the employee on April 6, 2006, approximately a month before the burglary, in which the employee noted that he downloaded the April 2006 BIRLS extract and that the file contained 26,503,436 records.

Mr. Duffy asked the OPP&P ISO to advise him what the procedures and obligations were with respect to notification, since he was both the ISO and PO. Both Mr. Duffy and Mr. McLendon admitted that they had no knowledge of what the SOC would do with the information, but assumed erroneously that the SOC would make appropriate notifications. In fact, Mr. Duffy said he did not even know that there was a SOC before the burglary.

Mr. McLendon recalled thinking he fully expected the next day to see a "wave of IG people," or people calling from upstairs saying "come up here and give us a simple version of this and what you think our potential exposure may be, but nobody ever called." Instead, he noted, "We waited. The process has been notified. The process will tell us what we're supposed to do here."

Mr. Duffy and Mr. McLendon said that they relied almost exclusively on OPP&P's GS-13 ISO/PO to investigate and report his findings to the SOC, thereby absolving them of any responsibility for insuring that law enforcement had all of the information about what was actually stolen. Ironically, when questioned about his role as an ISO for the SOC, the OPP&P ISO said "I'm not an investigator. I'm a computer tech guy that has a job."

The OPP&P ISO interviewed the employee on Friday, May 5, 2006. He advised us that because the employee was so flustered and because he knew the employee was going to be interviewed by a "bunch of people," he did not want to become part of it.

The OPP&P ISO told us that within 3 or 4 minutes into the conversation the employee was going in so many different directions he could not take good notes, so he told the employee to write it down and send it to him. Based on the employee's report, which was received around 2:00 p.m., the ISO drafted a "White Paper on Lost Data" that he e-mailed to Mr. Duffy and Mr. McLendon around 3:30 p.m. Shortly after that, Mr. McLendon responded to Mr. Duffy and the ISO indicating that he would review the document over the weekend. No further action on this matter appears to have occurred during the next 2 days (weekend), including any notifications to senior VA management officials.

On Monday morning, May 8, 2006, Mr. McLendon advised Mr. Duffy that, in his view, the OPP&P ISO's white paper was inadequate and did not appropriately address the event. Mr. McLendon stated he would re-draft the ISO's white paper. In preparation for

finalizing the revised white paper, Mr. McLendon stated that Mr. Tran would query the employee about the data that was on the hard drive and disks, citing a need to “be as precise as possible and not leave huge gaps where people will jump to conclusions.” Mr. McLendon stated that the section describing what may have been lost would be updated, and that Mr. Tran “accelerated his discussions with the employee.”

Mr. McLendon’s assertion that Mr. Tran continued to query the employee about the data that was on the hard drive and disks is disputed by Mr. Tran, who advised us that his sole purpose in contacting the employee on May 8, 2006, was to determine if CDs and the flash drive were actually stolen during the burglary, not what was on them. Mr. Tran stated that prior to May 16, 2006, he never attempted to quantify the number of records in any of the databases believed to have been stolen in any of his conversations with the employee, and he was not asked to.

Later that day, Mr. McLendon forwarded the revised white paper to Mr. Duffy, Mr. Tran, and the OPP&P ISO. Mr. McLendon, who titled his memorandum “Possibly Lost Veterans Data,” noted that he had added further detail for clarity. Our review of the two papers indicated that Mr. McLendon’s changes to the white paper focused on providing more background information on the burglary and who was notified, and information concerning the fact that most of the critical data was stored in files formatted in Statistical Analysis System (SAS).

This revised white paper which was completed on May 8, 2006, and put in memorandum format, inaccurately retained the May 5, 2006, date and the OPP&P ISO’s name and title. Also, while the memorandum did provide additional clarification on some aspects, it did not address the magnitude or extent of the stolen data in terms of numbers of veterans. Even though the ISO’s May 5, 2006, white paper indicated that one of the files believed to be stolen contained “BIRLS’ First, Last, and Middle Names for each veteran in the C&P Mini-Master, using SSN as the matching criteria,” there is no testimonial or documentary evidence that Mr. McLendon either personally or via a subordinate attempted to quantify the number of records in the stolen BIRLS or C&P files until OGC requested further review on May 16, 2006.

In what we conclude was an effort to mitigate the loss of data, Mr. McLendon’s primary contribution to the editing of the OPP&P ISO’s white paper was the assertion that SAS formatting protected most of the stolen data from all but SAS programmers with access to an expensive copy of the SAS application. This is not the case because we were able to display and print a portion of the SAS formatted data without the SAS program. Finally, Mr. McLendon, who is not an expert in SAS, failed to consult with the OPP&P SAS expert before revising and forwarding the white paper to upper management; implying that the SAS formatting afforded protection for most of the stolen data.

Late in the afternoon on Tuesday, May 9, 2006, Mr. Duffy met with Mr. Thomas Bowman, VA Chief of Staff, to discuss a number of issues, including the burglary that Mr. Duffy said he characterized to Mr. Bowman as a “fairly serious breach of sensitive data.” Mr. Duffy suggested to Mr. Bowman that it was important for the VA senior

leadership to meet and assess VA's affirmative obligation to notify the beneficiary population whose data may have been compromised.

On Wednesday morning, May 10, 2006, Mr. Duffy again briefed Mr. Bowman and provided him with a copy of the May 5, 2006, memorandum. Mr. Duffy recalled that he defined terms and acronyms contained in this memorandum, such as SAS, NSV, and BIRLS, for Mr. Bowman. Mr. Duffy stated that Mr. Bowman made a number of notations on the memorandum. Although Mr. Duffy recalled explaining that the BIRLS system is used by VBA, in particular, to identify veterans and match up names, social security numbers, and claim numbers, he could not recall providing Mr. Bowman with an estimate of the number of records lost in the burglary.

Mr. Duffy stated that it was his intention to reveal the loss of data to the Deputy Secretary, but decided to inform Mr. Bowman on May 9, 2006, when the weekly Tuesday meeting convened by the Deputy Secretary was cancelled. When asked why he did not notify the Chief of Staff or the Deputy Secretary when the OPP&P ISO's original "White Paper" was completed on May 5, 2006, Mr. Duffy admitted that there was no real sense of urgency on his part. He perceived the problem to be limited to the 20,000 or so veterans in the NSV and the approximately 6,000 veterans in the mustard gas file. He acknowledged knowing there were personal identifiers in the stolen information and that VA had an obligation and a responsibility to mitigate it. However, he added that he knows how VA operates—"they do not do crisis management." Mr. Duffy said he did not perceive this as a crisis. In hindsight, he added that his greatest regret is that he "failed to recognize the magnitude of the whole thing."

Mr. Duffy advised us that he was not contacted about the incident after his May 10, 2006, meeting with Mr. Bowman until May 17, 2006, when he was invited to participate in a pre-brief for the congressional hearing and was handed a copy of a May 17, 2006, memorandum written by Mr. McLendon. This was the first time Mr. Duffy saw that more than 26 million records were involved and included social security numbers and other information. Mr. McLendon's May 17, 2006, memorandum was written in response to a request from the VA General Counsel on May 16, 2006, asking that specific information about the loss be determined and documented by OPP&P. Mr. Duffy was not aware of the request from OGC or Mr. McLendon's response after it was submitted to OGC.

The Deputy Assistant Secretary for Security and Law Enforcement Did Not Make the Appropriate Inquiries to Notify Appropriate Law Enforcement Entities of the Potential Impact on VA Programs and Operations

VA regulations require all VA employees to immediately report information about actual or possible violations of criminal laws related to VA programs, operations, facilities, contracts, or information technology systems to their supervisor, any management official, or directly to the OIG (38 C.F.R. 1.201). Information about actual or suspected violations of criminal laws related to VA programs, operations, facilities, or involving VA employees, where the violation of criminal law occurs on VA premises will be reported by VA management officials to the VA police (38 C.F.R. 1.203).

Our investigation found that the employee complied with the provisions of §§1.201 and 1.203 when he reported the theft of his personal computer and external hard drive to his supervisors and VA law enforcement. We concluded that Mr. John Baffa, Deputy Assistant Secretary for Security and Law Enforcement, failed to take appropriate action to determine if there was an actual or possible crime involving VA programs and operations. If he had made the proper inquiries, he would have known that the theft was a possible violation of criminal laws relating to VA programs that was required under §1.203 to be reported to the appropriate Federal law enforcement entity for investigation, including the VA Inspector General. An inquiry also would have determined that the theft of the data was a potential felony involving VA programs that was required to be reported to the OIG under the provisions of 38 CFR §1.205.

Mr. Baffa told us that late morning on May 4, 2006, Mr. Doyle called him and asked if he heard anything regarding a burglary or theft of a computer. Mr. Doyle advised Mr. Baffa that an employee had called him the day before and was “concerned because his house had been broken into and his personal computer stolen” and, when the employee was asked why he was calling the Office of Security and Law Enforcement, “he said that there might have been some VA material on it.”

Based on his conversation with Mr. Doyle, Mr. Baffa was aware that the stolen data may have contained VA material. While he may not have had sufficient information at the time to comprehend the significance of the incident, he did not take appropriate action to determine if there was a crime involving VA programs, operations, or employees. He did not make any inquiries to determine what “VA materials” may have been stolen; whether the “VA materials” included information protected by the Privacy Act, a VA confidentiality statute, or the Health Insurance Portability and Accountability Act (HIPAA); whether the employee had violated Federal law by inappropriately accessing the information; whether the employee had violated the Privacy Act or other statute by disclosing protected information, etc. Had he made these inquiries, he should have recognized the significance of the matter and contacted the Department of Justice (DOJ), the OIG, or other appropriate law enforcement entity to ensure that they were aware of the magnitude of the data on the stolen and the potential impact on VA.

In his interview, Mr. Baffa implied that he may have acted differently if he had been informed that the employee had told Mr. Doyle that the theft “could be a career-ending incident for him.” We do not believe this exonerates Mr. Baffa from his obligation to determine if there was a crime or possible crime that potentially involved VA because Mr. Baffa knew the most important fact— that VA material may have been stolen.

Mr. Baffa’s decision not to take any further action because the OPP&P ISO was working on the issue also does not relieve him of his duty to exercise due diligence to determine if a crime occurred involving VA programs and report to the appropriate law enforcement entity. Mr. Baffa also told us that later in the day on May 4, 2006, he

looked in the VA directory and determined that the employee worked in OPP&P. He then went there to inquire whether someone reported the theft of a computer. He said he met with the ISO, who told him that he was working on it. Mr. Baffa said that he took no further action because he felt it was the ISO's responsibility as the ISO to investigate the matter, which he understood to be a computer security issue. He added that if nothing had been physically stolen from VA and the SOC is notified, then once they do what they have to do they would then notify him that he had a problem.

There is nothing in the law or policy that provides the ISO jurisdiction to investigate potential criminal activity. As discussed in Issue 5, the relevant VA policies, VA Directive and Handbook 6210 and VA Handbook 6502.1, do not require the ISO or PO to conduct a criminal investigation and do not require any reporting to law enforcement. In addition, there is no VA policy that requires the Office of Security and Law Enforcement to wait until the ISO or PO conducts an investigation. The Office of Security and Law Enforcement has responsibility for ensuring that crimes or potential crimes involving VA property, programs, and operations are investigated.

Conclusion

While no policy was violated in the handling of the incident, staff and senior managers who were notified of the theft failed to take appropriate action to determine the magnitude of what was stored on the stolen external hard drive, or whether it was encrypted or otherwise protected. The failure to determine this resulted in not recognizing the potential significance on VA programs, operations, and veterans. Since the local police were not told for 13 days that VA data was stolen during the burglary, valuable forensic evidence was most likely lost. The delay also prevented the burglary from receiving the urgency it warranted from Federal law enforcement agencies.

Poor communication, partially resulting from a dysfunctional working relationship among senior OPP&P executives, contributed to the 6-day delay in notifying the Office of the Secretary. While there was considerable rhetoric among OPP&P management concerning the need to identify the extent and scope of the stolen data, there was virtually no follow-up to obtain results. Also, the lack of urgency in addressing this issue was impacted by the false assumption that the SOC had the responsibility to investigate the incident and make all required notifications. This led to the situation where the magnitude of the problem was still undetermined when brought to the attention of the VA Chief of Staff 6 days after the burglary. Both Mr. Duffy and Mr. McLendon bear responsibility for the impact that their strained relationship, which both acknowledged, may have had on the operations of OPP&P in handling the aftermath when it occurred.

Recommendation

Based on the circumstances presented in this section, we recommend that the Secretary take whatever administrative action he deems appropriate concerning the individuals involved.

Issue 3: Whether the Secretary's Immediate Staff Demonstrated a Lack of Urgency in Notifying the Secretary

Findings

On Tuesday, May 9, 2006, Mr. Duffy notified Mr. Bowman of the data theft. Mr. Bowman asked Mr. Duffy to provide him additional details regarding what data may have been breached, and the following morning, Wednesday, May 10, 2006, Mr. Duffy gave Mr. Bowman the "May 5th memorandum," as discussed in Issue 2. At approximately 1:30 p.m. on May 10, 2006, Mr. Bowman provided a copy of this memorandum to Mr. Jack Thompson, Deputy General Counsel, and asked him to provide an assessment of the agency's duties and responsibilities to notify individuals whose identifying information was compromised. Also on the afternoon of May 10, 2006, Mr. Bowman informed Mr. Gordon Mansfield, Deputy Secretary, of the burglary and the stolen VA data.

It was not until the morning of May 16, 2006, after the Chief of Staff was informed by the Inspector General that the stolen data most likely contained records with personal identifiers on approximately 26 million records, that Mr. Bowman notified the Secretary of the theft and magnitude of the lost data. Six days of the 7-day delay in notifying the Secretary was spent waiting for legal advice from OGC on VA's legal responsibility to notify individuals potentially impacted by the loss of the data. This 6-day delay can be attributed to a lack of urgency on the part of those requesting this opinion and those responsible for providing the response. This is not to say that everyone who was notified of the incident failed to recognize the importance of this matter, but no one clearly identified this as a high priority item and no one followed up on the status of the request until after the May 16, 2006, call from the Inspector General.

VA Chief of Staff and Deputy Secretary Waited 7 Days Before Notifying the Secretary of the Data Loss

Mr. Bowman told us that Mr. Duffy first informed him of the burglary and loss of data containing personal identifiers on Tuesday, May 9, 2006. He said they had been having some "light conversation" when Mr. Duffy said, "I may as well bring to your attention the fact of this loss of information." Mr. Bowman said he asked Mr. Duffy to provide him written details regarding what data may have been stolen from the employee's home because he wanted to provide those details to OGC and obtain advice as to what VA must do with respect to notifying veterans about the loss.

According to Mr. Duffy and Mr. Bowman, the two met again the next morning, May 10, 2006, and Mr. Duffy provided Mr. Bowman a copy of the May 5, 2006, memorandum. Mr. Bowman told us that when they discussed the memorandum, he wrote notes on his copy as Mr. Duffy talked. One notation was "20k records." Mr. Bowman told us he thought that note referred to the size of the 2001 NSV database and several witnesses confirmed that approximately 20,000 veterans were surveyed. Mr. Bowman's note, however, was placed on the memorandum next to the description of BIRLS and not

near the description of the NSV. Nevertheless, according to Mr. Bowman, Mr. Duffy said the loss “could be as little as 20-some thousand or it could be millions.”

Mr. Bowman said he questioned Mr. Duffy if he was referring to BIRLS when he said the loss could be millions, and said Mr. Duffy responded, “It could go that high if that’s in fact what was lost.” He said he recalled Mr. Duffy using the figure “up to 24 million,” to explain the magnitude of records contained in BIRLS.

Mr. Bowman informed us that on May 10, 2006, he took a copy of the May 5, 2006, memorandum to Mr. Thompson and asked for advice on what the VA’s notification requirements were as a result of the loss of sensitive data. He told us he did not recall giving Mr. Thompson a deadline to provide a response, nor did he remember whether he conveyed a sense of urgency regarding the need for a quick response.

Mr. Bowman stated he also informed Deputy Secretary Mansfield on May 10, 2006, and provided him a copy of the May 5, 2006, memorandum with his “20k records” notation. According to Mr. Bowman, he told Mr. Mansfield that the loss could be “as small as 20,000 and it could be in the millions— the BIRLS system.” Again, he told us, “I remember specifically telling the Deputy...we don’t have any feel for whether it is as little as 20,000 or in the millions.” Mr. Bowman said he told the Deputy Secretary that he requested legal advice from OGC, and that the Deputy Secretary asked to be kept informed.

Mr. Mansfield confirmed that Mr. Bowman told him about the loss of data on May 10, 2006. He said Mr. Bowman gave him a copy of the May 5, 2006, memorandum containing Mr. Bowman’s handwritten notes, including the notation “20k records.” Mr. Mansfield told us it was his understanding that the 20,000 records represented an extract of BIRLS and that OPP&P was attempting to determine which subsets of that database were involved. He said he asked Mr. Bowman to find out more information regarding how many and which files were stolen. He told us that based on the briefing he received from Mr. Bowman, he believed potentially 20,000 records were involved.

Because the Deputy Secretary’s recollection of the conversation differed from Mr. Bowman’s concerning the issue of the magnitude of the loss we had a follow-up conversation with Mr. Bowman, who stated that it is possible that he advised the Deputy Secretary that BIRLS may have been lost, assuming that the Deputy Secretary would have recognized that BIRLS contained millions of records.

Mr. Mansfield told us that he and Mr. Bowman did not discuss notifying the Secretary. He said they were trying to get more information about the loss in order to be able to give the Secretary more details and to identify what needed to be done as far as notifying what he believed at the time was approximately 20,000 veterans. He said had he known the loss affected 26 million veterans he might have notified the Secretary immediately, but thinking the loss was around 20,000 records he wanted to get more information on exactly what happened.

Mr. Mansfield told us that, although he and the Secretary converse on a daily basis, he did not notify the Secretary about the data loss immediately after he first learned of it. Mr. Mansfield said that he had commented during the meeting with Mr. Bowman on the need to find out exactly what the size of the lost data was and to check with OGC on what else they needed to do to brief the Secretary. After the meeting, the Deputy Secretary left work on a personal matter and was out of the office either on personal business or speaking engagements from the afternoon of May 11-16, 2006.

Mr. Bowman took no further action on this matter until he received a telephone call from the Inspector General (IG) at approximately 8:30 a.m. on Tuesday, May 16, 2006. During the call, Mr. Bowman was informed that OIG staff learned through an interview with the employee that personally-identifiable data, including names, dates of birth, and social security numbers for as many as 24–26 million veterans may have been taken during the burglary. Mr. Bowman acknowledged to the OIG officials that he was aware of the incident, but did not know the magnitude of the loss. Mr. Bowman acknowledged that he thought the incident involved “hundreds of thousands” of records. The IG informed Mr. Bowman that the Secretary needed to be briefed on this issue.

Shortly after the telephone call from the IG on May 16, 2006, but before he received the memorandum from OGC, Mr. Bowman met with the Secretary to inform him of the theft and loss of data. He told us he informed the Secretary that he had informed the Deputy Secretary of the incident and that the scope of the loss, according to the OIG, was 24–26 million records. According to Mr. Bowman, after he advised the Secretary of the possible loss, Mr. McClain provided him the memorandum he requested at approximately 11:00 a.m. that morning. The memorandum was dated May 16, 2006.

Mr. Bowman told us he did not notify the Secretary sooner because he was waiting for the OGC memorandum. He said he wanted “substance and at least some organizational understanding” of what he needed to report, as he did not want to alert the Secretary “to something that is dramatic unless there is a basis for it,” and if the facts showed that the matter was not urgent he did not want to “take up time with something that...can maybe be put in a memo that he can look at leisurely.” While acknowledging that he enjoyed an “open door” relationship with the Secretary, Mr. Bowman decided he wanted to first work with the Deputy Secretary and other senior leadership, using the anticipated advice from OGC, to develop a strategy for responding and a set of recommendations. However, Mr. Bowman said that, after receiving the telephone call from the Inspector General, he felt he needed to tell the Secretary without waiting any longer for the OGC memorandum. He told us, in retrospect, he realized he should have given the Secretary the same notice he gave the Deputy Secretary on May 10, 2006.

A Lack of Follow-Up and Editorial Changes Delayed OGC Legal Advice to the Chief of Staff for Several Days

At approximately 1:30 p.m. on Wednesday, May 10, 2006, Mr. Bowman met with Mr. Thompson and provided him a copy of the May 5, 2006, memorandum. According

to Mr. Thompson, Mr. Bowman asked him what VA's legal obligations were to the individuals whose identities may have been compromised as a result of the theft. While Mr. Thompson acknowledged he knew the issue was significant because it was unusual for the Chief of Staff to personally request an opinion, he told us Mr. Bowman neither told him about the magnitude of the loss nor gave him a deadline for responding. Regarding a deadline, Mr. Thompson noted that Mr. Bowman had come to his office about an hour earlier on another matter and gave him a 30-minute deadline to respond.

Mr. Thompson put a routing slip on the memorandum Mr. Bowman provided and wrote on it, "The Chief of Staff asks, 'What is VA's responsibility in terms of notifying the individuals whose identities may become known as a result of this theft?' " He addressed the routing slip to OGC Professional Staff Group 4 (PSG 4), which handles information law issues, but did not establish a deadline for the response. He said he believed it was "self evident that this was a priority matter" because the Chief of Staff had handed the memorandum to him and he had it hand-carried to the individuals responsible for addressing the issue.

According to Mr. Thompson, an administrative assistant delivered the memorandum to PSG 4, where another administrative assistant told us she recalled leaving the package on the chair of Mr. Jeff Corzatt; an attorney in PSG 4. Mr. Corzatt told us he found the folder in his chair on May 10, 2006. He said he wrote a response to the question written on the routing slip that afternoon, thought overnight about what he had written, and made some changes the next day, May 11, 2006. He said he then gave the response to his supervisor, the PSG 4 Deputy Assistant General Counsel, that afternoon. Mr. Corzatt told us he considered the response final on May 11, 2006, less than 24 hours after he was assigned to write it. He told us he was not at work on Friday, May 12, 2006.

The PSG 4 case tracking system documents that the response was approved by its management on Friday morning, May 12, 2006, and hand-carried to the General Counsel's office for review and approval. An administrative assistant in the General Counsel's office told us she received it that morning, and while proofreading it she noticed a need for minor edits. She marked them and personally hand-carried the folder on Friday afternoon to an administrative assistant in PSG 4 to have the edits made. The case tracking system indicates the edits were made on Monday, May 15, 2006, and returned that afternoon.

Mr. Thompson told us he did not discuss the Chief of Staff request with the attorney who prepared the memorandum, nor did he follow up on it. Mr. McClain said he was not aware of the request for legal advice by Mr. Bowman prior to May 16, 2006, and that Mr. Thompson had not talked to him about either the loss of data or the request. Mr. McClain said he first saw the memorandum in his in-box in the early morning of May 16, 2006, and reviewed it and signed it. Mr. McClain said that the call from the IG came shortly after that. He then went back to his office and retrieved the memorandum, made copies, and took it to the 11:00 a.m. meeting with the Chief of Staff and others.

The May 5, 2006, memorandum that Mr. Bowman gave Mr. Thompson expressly stated that the information possibly stolen contained “a copy of the BIRLS production file in SAS format which contained SSN, DOB and NAME for living and deceased veterans.” In addition, the memorandum also mentioned that a CD “contained BIRLS’ First, Last, and Middle Names for each veteran in the C&P Mini-Master.” Prior to becoming Deputy General Counsel, Mr. Thompson spent many years in OGC as the Assistant General Counsel for PSG 2, which provides legal advice and assistance to VBA. As an attorney for VBA, Mr. Thompson should have had knowledge about major VBA databases such as BIRLS and the C&P file. While he may not have been familiar with the full extent of details in these databases, he should have known that the records of millions of veterans were contained in them and, therefore, were potentially compromised.

The OGC attorneys involved in addressing Mr. Bowman’s request limited their response to the specific question he asked: “What was the duty of VA to notify the individuals whose personal data may have been lost or compromised?” Between May 10 and May 16, they took no affirmative action to assist or advise VA of any other issue related to the incident until after the IG provided information on the magnitude of the loss.

Conclusion

Although Mr. Bowman acknowledged he knew the VA data stolen on May 3, 2006, could affect the records of millions of veterans, he demonstrated no urgency in notifying the Secretary of the incident. He notified Mr. Mansfield the day after he learned of the loss, but Mr. Mansfield too decided not to raise the issue to the Secretary until they knew more information on what VA’s legal responsibilities were and more about the magnitude of the problem. Mr. Mansfield recalled instructing Mr. Bowman to focus on identifying these issues; however, Mr. Bowman does not recollect being asked to obtain any additional information other than the legal advice from OGC. Yet, during the 6 days following his request for legal advice from OGC, Mr. Bowman did not follow up to determine its status of the request, or task anyone to develop a more definitive description of how many veterans’ records may have been stored on the stolen external hard drive. While Mr. Bowman states that he was aware that it could have been millions, no effort was made to clearly identify what was in the stolen files. The OIG was able to determine the extent of the stolen data after one interview with the employee on May 15, 2006. It is unexplainable as to why the employee, who reported the stolen data, was never consulted by anyone in the management chain-of-command except the GS-13 ISO/PO for OPP&P, until May 16, 2006.

Recommendation

Based on the circumstances presented in this section, we recommend that the Secretary take whatever administrative action he deems appropriate concerning the individuals involved.

Issue 4: Whether Information Security Officials Effectively Triggered Appropriate Notifications and an Investigation of the Stolen Data

Findings

As soon as the employee returned to duty on May 5, 2006, the OPP&P ISO obtained from him information concerning the theft of the data and forwarded it to the SOC, an organizational component of the Office of Cyber and Information Security, and to the District ISO, who is responsible for coordinating ISO activities among VACO staff offices. However, the OPP&P ISO's incident report had significant errors and omissions, and information security officials did not adequately attempt to identify the magnitude of the incident or elevate it until their role was overtaken by events on May 16, 2006.

At nearly every step, VA information security officials with responsibility for receiving, assessing, investigating, or notifying higher level officials of the data loss reacted with indifference and little sense of urgency or responsibility. Although the employee met with the ISO for OPP&P on his first day back in the office following the burglary, no effort was made to determine the magnitude of the data loss at this meeting or later when the information was relayed to other responsible officials, including the District ISO and officials in the SOC. At no time prior to the IG call on May 16, 2006, did anyone attempt to re-interview the employee to gain a better understanding of the scope and severity of the potential data loss.

Efforts to investigate the incident were further impeded by errors and omissions in the ISO incident report and were delayed due to ineffective coordination between the OPP&P ISO and the SOC incident team lead. The senior management official with responsibility for the SOC reacted with indifference by not attempting to ascertain the scope of the potential breach and relying on lower-level employees to investigate and document the incident appropriately and in a timely manner without sufficient follow-up or oversight. His superior acknowledged that he was not informed by any of his staff about the incident, and also did not become aware of it until May 16, 2006.

Twelve days after receiving the original incident report, the SOC had made no meaningful progress in assessing the magnitude of the event and had attempted to pass responsibility to gather information on the incident back to the OPP&P PO. Coincidentally, this is the same individual who referred the matter to the SOC in the first place, which he did in his dual capacity as ISO for OPP&P.

The OPP&P ISO's Incident Report Contained Significant Errors and Omissions

To ensure timely and appropriate responses to information security incidents, VA policy requires VA organizations to notify their assigned ISO promptly when such incidents occur, including incidents of unauthorized disclosure or loss of VA data. The policy further assigns the ISO responsibility for reporting these incidents to the SOC. The ISO for OPP&P has served in that capacity since 2002.

On the morning of May 5, 2006, the OPP&P ISO briefly interviewed and requested a written statement from the employee concerning the theft of VA data from his home. The OPP&P ISO consulted with the GS-14 District ISO responsible for coordinating ISO activities among VACO staff offices, who in turn asked him to provide her a brief written description. Later that day, the employee provided the written statement to the OPP&P ISO as requested, noting that his personally-owned laptop computer and external hard drive were taken during the burglary and that VA data files containing personal identifiers had been stored on the missing external hard drive. Based in part on his review of VA data stored on CDs and a flash drive that had not been taken in the incident, the employee listed the files he believed were on the missing hard drive.

The OPP&P ISO quickly edited the employee's statement to serve as the basis for his information security incident report, which he sent by electronic mail to the SOC and the District ISO shortly before 4:00 p.m. on Friday, May 5, 2006. The District ISO provided a copy of the report to the SOC on this same day. When editing the employee's statement, the OPP&P ISO deleted what he felt were unnecessary details of the burglary but also mistakenly changed the report to erroneously state that the CDs and flash drive— key evidence of what VA data were likely on the missing hard drive— had themselves been taken in the incident. This error resulted in a missed opportunity in the early stages of the incident to re-create the likely contents of the employee's laptop and external drive and to recognize the magnitude of the potential loss of data.

Additionally, although the employee's report contained information on the number of records (6,744) at risk in the mustard gas file, the OPP&P ISO forwarded the information without attempting to determine or report the number of records in the other files the employee had on his hard drive. Simple follow-up questions on the nature of the contents and size of the BIRLS extract or C&P list would have shown that sensitive information on millions of veterans' records were at stake. Finally, the incident report did not contain the employee's name or other contact information to facilitate confirmation of the incident.

The OPP&P ISO told us that after he filed the incident report with the information security officials, he was waiting on the results of an investigation into the matter by the SOC and did not take any further action. When asked if he re-interviewed the employee the following day (May 8, 2006) after May 5, the OPP&P ISO responded, "No. I took his email. I did not want to talk to him again. I didn't want to – if he had changed his mind or did whatever, I didn't want to know, and I didn't want to hear it. I didn't want to be involved with a conflict, having one statement or then having another statement and then having to go back. I didn't want that... If he had requested to talk to me, then I would have if he had something to share, but I gave him the opportunity to send the email and get everything in it. He sent it, and we've had no contact since."

Because the OPP&P ISO also serves as the OPP&P PO, we asked him why he did not pursue this incident as a privacy issue. He responded that he was waiting for the SOC to investigate what files were missing and to determine if the loss was a privacy

violation. Ironically, 12 days after receiving the OPP&P ISO's incident report the SOC had referred the matter back to the ISO for action as a privacy violation.

Cyber Security Operations Officials Did Not Ensure That a Timely Investigation and Notifications Were Made Concerning the Severity of the Data Loss

A GS-13 information technology specialist in the SOC received the OPP&P ISO's e-mail regarding the incident on Friday, May 5, 2006, in the late afternoon. As the SOC incident management team lead, he was responsible for reviewing the reported event, determining whether the incident could be confirmed, prioritizing the incident as to its severity and urgency, determining the proper incident category, and initiating incident notifications.

That same afternoon, the SOC incident management team lead left the OPP&P ISO an after-hours voice mail requesting a call back. The OPP&P ISO told us he did not receive that message until late on Monday, May 8, 2006, because he had been busy that day. On May 10, 2006, the SOC team lead notified the OPP&P ISO by e-mail that the SOC had established an incident case number for the event, that he should ensure the local privacy officer was notified, and that any additional pertinent information be forwarded to the SOC. In addition to the above confirmed contacts, the SOC team lead said that he called or left voice mail messages for the OPP&P ISO on other occasions following the incident, but the ISO told us he did not recall receiving these communications. In any event, 12 days lapsed without the SOC team lead and the OPP&P ISO, who work in the same building several floors apart, from making any progress in investigating or determining the severity of the incident. The SOC team lead told us that he determined that the incident appeared to be primarily a privacy incident rather than a cyber security incident, so he expected that the OPP&P ISO, as the OPP&P PO, had primary responsibility to obtain information on the event.

Also on May 5, 2006, the District ISO advised her supervisor, Mr. Johnny Davis, Jr., of the possibility that sensitive data was stolen from a laptop of a VA employee. As the Director of the Cyber Infrastructure Protection Service, Mr. Davis has supervisory responsibility for the SOC, and also serves as the Acting Associate Deputy Assistant Secretary for Cyber Security Operations. Mr. Davis told us that this conversation occurred in passing in the hallway and that the District ISO did not have details on the nature of the missing data. Nonetheless, Mr. Davis said he directed her to ensure that the incident was reported to the SOC and the Privacy Office, and that he relied upon her as a GS-14 employee to carry out these instructions without the need for supervisory follow-up. While she did in fact submit a report to the SOC, the District ISO acknowledged that she became disengaged from the process, and Mr. Davis did not follow up further with her or the SOC team lead to determine whether any progress was being made.

Mr. Davis also told us that the SOC routinely receives reports of incidents from ISOs, which they must attempt to confirm and analyze before making further notifications. According to Mr. Davis, however, national level incidents are to be brought to his

attention immediately so he can brief his supervisors. No such notifications were made because of the failure to develop timely information on the magnitude of the data loss by each person in the notification chain: the OPP&P ISO, the District ISO, and the SOC team lead. These failures were further compounded by Mr. Davis's failure to follow up on the actions of his staff.

It was not until May 16, 2006, when Mr. Davis' supervisor, Mr. Pedro Cadenas, Acting Deputy Assistant Secretary for Cyber and Information Security, who also serves as the Acting Deputy Chief Information Officer (CIO), asked him about the incident that Mr. Davis followed up with his staff. Finally on May 17, 2006, 12 days after receiving notification in the SOC on the incident, the SOC team lead met with the OPP&P ISO in person, interviewed him, and began preparing an incident report. Mr. Davis provided a follow-up report to Mr. Cadenas, and Mr. Cadenas reported the results to his superiors. When asked why the notification was not made earlier, Mr. Cadenas told us that in accordance with their procedures, notification is only done after an incident has been validated as a cyber security incident. In this case, his staff had determined that it was a privacy matter and not a cyber security matter, and took steps that same day to ensure that the incident was entered into the privacy violation tracking system. Accordingly, the SOC had referred the incident back to the person who initially reported the incident 12 days earlier to the SOC, the OPP&P ISO, in his capacity as OPP&P PO, who had initially stated he did not want to talk to the employee again.

Conclusion

As the person responsible for making the first notification to information security officials, the OPP&P ISO failed to adequately and accurately describe the loss of data that occurred, particularly the magnitude of the number of records stolen. His failure to discharge his duties and responsibilities— whether by not re-interviewing the employee or by failing to respond to numerous contacts by the SOC— hampered other officials in understanding the true scope of the data breach and reacting accordingly. The OPP&P ISO acted as if he had no further responsibility after he notified the SOC. As the OPP&P privacy officer, the matter was eventually referred back to him for action.

The absence of sufficient detail concerning the magnitude of the loss hampered the efforts of the SOC team lead to assess the severity of the incident. However, despite whatever difficulties the SOC team lead may have had reaching the OPP&P ISO by telephone; he was not sufficiently diligent in obtaining information about the incident. Since the two worked in the same building, the SOC team lead should have sought out the ISO by going to see him in his office.

After reporting the incident to Mr. Davis on May 5, 2006, the District ISO became disengaged and took no further action to monitor the situation or keep her supervisor apprised of the status. Mr. Davis, who has supervisory responsibility for the SOC, learned of the incident on May 5, 2006, but did not follow up in a timely manner to ensure it was investigated and did not report it to his supervisor, Mr. Cadenas, so that notification could continue to the Chief Information Officer, Deputy Secretary, and

Secretary. Although the SOC team lead, Mr. Davis, and Mr. Cadenas said they thought the incident was a privacy issue, VA policy identifies the loss of sensitive computer data as a reportable information security incident. The failure to realize the magnitude of this incident, combined with a bureaucratic process that took 12 days to determine that this was a privacy issue and not an information system security issue, not only delayed notification to higher-management, it also resulted in the matter being referred back to where it originated, with the OPP&P ISO/PO.

Recommendation

Based on the circumstances presented in this section, we recommend that the Secretary take whatever administrative action he deems appropriate concerning the individuals involved.

Issue 5: Whether VA Policies Safeguard VA Information

Existing VA policies, procedures, and practices need to be consolidated and strengthened to ensure that personal or proprietary information used by VA employees and contractors are adequately safeguarded. They also need to be readily accessible by VA and contract employees to ensure compliance.

We found that VA's policies and procedures for safeguarding information and data were not consolidated or standardized to ensure all employees were following all applicable requirements in a similar fashion, and that policies and procedures were not adequate in preventing the loss of the data. We also found that VA employees and contractors were not adequately trained and reminded of the policies and procedures to follow to safeguard personal or proprietary information, sensitivity level designations were not always accurate, information and data provided to contractors need to be better safeguarded, and VA incident reporting procedures and controls need improvement.

Since the incident in which millions of VA records containing protected information were stolen, VA managers have attempted to strengthen policies, procedures, and controls to prevent similar disclosures, but additional actions are need to be taken to safeguard protected information and VA's automated systems. Personal and proprietary information is referred to throughout this section as protected information.

VA Policies, Procedures, and Practices Were Not Easy to Identify, Current, and Complete

VA needs to consolidate and standardize policies, procedures, and practices for safeguarding VA protected information and ensure that they are accessible to employees and contractors. Our review found that policies and procedures have been issued at irregular intervals over a long period, and in separate guidelines, memoranda, directives, and handbooks, and in response to various laws and other legal requirements. As such, there was no consolidated repository of instructions and requirements that employees could research and follow, nor was there an adequate method for ensuring that all policies and procedures issued by VA were current. Managers in each of the administrations within VA have issued their own local policies and procedures which has increased the potential for inconsistencies and further fragmented directions provided to employees and contractors.

The fragmentation of VA policies and procedures issued over a long period, and the issuance of numerous local policies and procedures issued independently by each administration within VA, contributed to many of the procedural and control inconsistencies that are noted throughout this report.

To evaluate whether VA had policies and procedures in place to safeguard against the disclosure of protected information if the information was lost or stolen, we asked VA to provide us with all relevant policies and procedures. We received a fragmented number of policies and procedures that have been issued to employees by VA over time. We

researched and found other policies and procedures that were not provided to us in response to our request.

To illustrate, VA provided us the following documents:

- Security Guideline for Single-User Remote Access, March 10, 2006.
- An April 20, 2006, memorandum from the Assistant Secretary for Information and Technology to remind all employees, contractors, students, and volunteers that they must complete Cyber Security Awareness training by September 30, 2006.
- A February 13, 2006, memorandum from the Assistant Secretary for Information and Technology advising VA leadership of the requirement that they must complete the Enterprise Privacy Program privacy training by September 30, 2006. The memorandum also advises of other training options including two prepared by VHA.
- VA Directive 6502, Privacy Program, June 20, 2003.
- VA Handbook 5011/5, Hours of Duty and Leave, September 22, 2005, which revised the policies and procedures for telework.

In addition to the documents provided by VA, our research identified additional VA Directives and Handbooks on the subject of IT security and privacy of information:

- VA Directive 6210, Automated Information Systems Security, January 30, 1997, and VA Handbook 6210, which establishes policies and procedures for cyber security.
- VA Handbook 6502.1, Privacy Violation Tracking System, March 25, 2004.
- VA Handbook 6502.2, Privacy Impact Assessment, October 21, 2004.
- VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, January 12, 1998.
- VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, January 12, 1998.

Our review confirmed that there was no consolidated and current set of policies and procedures that employees and contractors could access to ensure all applicable requirements are being met. We found that the VA intranet posed a considerable challenge to employees seeking to learn about VA policies on privacy and cyber security. There was no direct link on the main VA home page to VA-wide directives; therefore, employees not familiar with the Office of Information Technologies Directives

Homepage must conduct multiple time-consuming searches and sort through tens of thousands of “hits” before locating pertinent directives. Without clearer directions on how to locate these directives, VA will not achieve compliance.

We also found that managers within each region and local facility within VA developed and implemented their own policies and procedures on many of these requirements, which further subjected the criteria to multiple, differing interpretations.

VA Policies and Procedures for Safeguarding Against the Disclosure of Protected Information Were Not Adequate to Prevent the Data Loss Incident

VA did not have sufficient policies and procedures in place to prevent this recent data loss incident, or any other such incident, that would have involved the disclosure of protected information. We did not identify any VA policy that prohibited employees or contractors from removing protected information from the VA worksite, required employees or contract employees to obtain authorization before removing the information, prohibited the use of non-VA computers to process or store protected information, or that required safeguards such as password protection or encryption when protected information was stored on portable storage media or non-VA computers.

VA Directive 6502, Privacy Program, which was provided to us by VA in response to our request, states that VA will ensure that all privacy-protected data maintained by or for, VA in any medium, is kept confidential, except when disclosure is permitted by law. The Directive does not specify how the information will be protected and does not require safeguards for proprietary information.

The Privacy Service in the Office of Information and Technology is responsible for VA Directive 6502. The Director, Privacy Service, told us the administrations, particularly, VHA, have great latitude in terms of establishing local policies and, unless Privacy Service is asked to look at a policy, they “have no idea what exists out there.” The Privacy Officer for VHA told us that they do not review all of the policies issued by field facilities. This decentralized approach to policy making leads to inconsistencies in protecting information.

None of the employees we interviewed was able to identify a policy or other requirement in place prior to May 3, 2006, that established specific requirements for safeguarding protected information when removed from the worksite. One of the documents VA provided in response to our request was titled “Security Guidelines for Single User Remote Access” (Security Guideline), March 10, 2006. We determined that this document was not an approved or published VA Directive, Handbook, or policy at the time of the incident or at the time it was provided to us. Nonetheless, we reviewed the document and determined that the provisions did not provide adequate safeguards for information stored on portable media. Also, statements throughout the document indicate that the guidelines were only applicable to employees with remote access to the VA intranet.

Our research identified a reference to removing Privacy Act protected information in Section 9 of VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, issued January 12, 1998. Paragraph b (2) of Section, Systems of Records on Personal Computers, states:

“Records subject to the Privacy Act that are maintained on PCs must be protected from unauthorized disclosure in the same manner as all records subject to the Act. To ensure proper protection of records on ‘floppy disks,’ procedures will be established by management to ensure these disks are not removed or used outside Government buildings or installations without proper authorization and documentation. ‘Floppy disks’ containing personal information subject to the Act will be properly secured when not in use to prevent unauthorized use or access.”

Not only is the Handbook outdated with respect to the current technology used to store information, employees would not be familiar with the cited provision unless they were processing a request for Privacy Act records. The provision in Section 9 does not prohibit removing protected data from the worksite. While it does require that the agency implement procedures to ensure data is not removed from the worksite without proper authorization and documentation, we could not identify any such procedures. Also, the individuals we interviewed were not aware of any policies or procedures.

We also could not identify any VA policy in effect at the time of the incident that required protected information stored on portable media be password protected or encrypted, or that the media devices or hard copy of records be secured by any specific means. VA Handbook 6300.4 only requires that “floppy disks” containing personal information subject to the Privacy Act will be “properly secured when not in use to prevent unauthorized use or access.” Criteria to satisfy the “properly secured” requirement were not delineated in VA Handbook 6300.4 or any other VA policy that we were provided or that we located ourselves using the VA intranet.

In response to our request, VA provided VA Handbook 5011/5, which provides policy and procedures for telework. Although the employee was not teleworking when the incident occurred, the telework policy is significant because the program supports the concept of employees taking work from the VA worksite to their home or other remote location. The policy only prohibits taking, using, and storing “classified” information at the employee’s home or telecenter. At VA, however, most VA employees do not handle classified data. The telework policy specifically allows employees to remotely access Privacy Act materials and VA data and systems provided the employee agrees to protect the records from unauthorized disclosure or damage. The policy also requires employees to comply with all legal requirements of the Privacy Act and other statutes, policies, and procedures, to protect the VA data and systems to which the employee will have access under the telework arrangement, but lacks sufficient detail to say how this should be done.

The use of non-VA computers to work at home or other remote location was not prohibited by VA's telework policy. Also, this policy does not require the same safeguards VA requires for VA owned computers. The policy does not require that personal computers be password protected, have antivirus or intrusion software, or that confidential or other protected information be encrypted or password protected, and does not have requirements for the destruction of data, even when non-VA computer is discarded.

Employees who use VA's Virtual Private Network (VPN) to access the VA intranet remotely are required to comply with requirements for remote access. This provision has limited impact because employees are not required to have remote access to work from home or other remote site and the policy permits the use VPN on non-VA computers. Remote access through VPN only protects the firewall for VA's intranet; it does not prohibit the employee from downloading protected information and does not protect the information after it has been downloaded onto a non-VA computer. The ISOs, who have responsibility for obtaining signed Rules of Behavior for VPN users, told us that they do not have any involvement with telework arrangements unless the employee is using remote access to the VA intranet.

Our review showed that current VA policies and procedures need to be clarified to distinguish between information law and information security law requirements. Information laws and regulations identify information to be protected from disclosure, establish the conditions under which the information may be disclosed, and prescribe penalties for illegal disclosure. Information law requirements applicable to personal information in records VA maintains include the Privacy Act;¹ VA confidentiality statutes,² and Health Insurance Portability and Accountability Act (HIPAA) regulations.³ These laws also prohibit the disclosure of proprietary information maintained by VA.⁴

Conversely, information security laws focus on protecting automated systems that store the information from unauthorized access. Information security laws require VA to take action to protect the automated systems that contain protected information from unauthorized intrusions, unauthorized access, and viruses that can impact both the information system and the integrity of the information. The Federal Information Security Management Act of 2002 (FISMA)⁵ provides the framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

The circumstances surrounding the theft of the employee's personal external hard drive on which protected information was stored highlight a gap between information law and information security law requirements, and raises issues concerning the VA policies and

¹ Title 5 U.S.C. § 552a.

² Title 38 U.S.C. §§ 5701 (protects claims for benefits, including names and addresses), 5705 (protects medical quality assurance records), 7332 (protects records relating to the treatment of drug and alcohol abuse, sickle cell anemia, and HIV).

³ Title 45 CFR §§ 160 *et seq.*

⁴ Title 18 U.S.C. § 1905.

⁵ Title III of Public Law 107-347, E-Government Act of 2002.

processes designed to ensure compliance with these laws and how problems are investigated and resolved.

Our review found that the gap is in the assignment of responsibility for establishing and enforcing VA policy with respect to these two sets of laws. Privacy Officers see their role as identifying the information that should be protected and the criteria for disclosure. Information Security Officers see their role as safeguarding information by protecting the automated systems in which the information is stored. The gap is safeguarding information not stored on VA automated systems.

VA policies did not sufficiently address safeguards for protecting information from loss or theft when the information does not reside in a VA automated system. This includes hard copy records as well as records stored electronically on portable media storage devices and non-VA computers. Portable storage devices allow employees and contractors to store and transport millions of records to alternate work sites. While this could improve the efficiency of Government by allowing employees and contractors to work from remote and non-traditional locations, there are inherent risks associated with the removal of the data from a protected environment that can result in potential disclosure of protected information through loss or theft that need to be addressed in VA policies and procedures.

Clarifications to VA policies are also needed in describing the terminology used when discussing issues of information law versus information security law. For example, the word “system” as used by ISOs refers to the automated systems, hardware, and program applications that store the information; whereas to a PO the word “system” refers to a “system of records” as defined in the Privacy Act. The Privacy Act and other confidentiality statutes use terms such as “privileged” or “protected” information, whereas FISMA uses the term “confidential” and VA policies use the term “personal” or “sensitive” to describe certain information. Personal information pertains to personal identifiers related to individuals such as social security numbers, dates of birth, claims numbers, and health information. Proprietary information relates to information provided by vendors during the acquisition process and internal configuration and design information concerning VA automated systems. We concluded that VA needs to apply consistent and comprehensive terminology throughout its policies and procedures to better standardize its criteria for safeguarding protected information.

VA Training Tools Are Not Adequate to Ensure that VA and Contractor Employees Are Sufficiently Trained

Our review of employees’ and contractors’ training on policies and procedures found that cyber security and privacy awareness trainings were inadequate. VA requires all VA employees and contractors who have access to VA’s automated systems to complete training annually on cyber security awareness and privacy. We reviewed all of the training modules to determine whether they effectively informed employees and contractors about their duties, responsibilities, and accountability for protecting VA’s automated systems and protected information.

We found that these modules are difficult to locate, do not adequately address safeguarding protected information when it is removed from VA premises, are not constructed to ensure that employees are tested on comprehension of course content, and that most modules are general in nature and do not contain citations or links to applicable directives.

In our search of the VA intranet, we experienced difficulty locating the required training, netting over 100,000 possible matches when using the phrase “Cyber Security Training.” Our search also revealed that a link on the VA intranet provides the questions and answers to questions asked during the training and allows employees to print a “Certificate of Training” without accessing the training module.

Cyber Security Awareness training is basic in nature and does not cite any VA directive, handbook, or other policy relating to cyber security. For example, the training does not cite VA Directive 6210, which prohibits using e-mail to transmit protected information unless the information is encrypted. It also does not cite VA Handbook 6300.4, which at the time of the data loss, was the sole VA directive that addressed protection of information when removed from VA premises on floppy disks.

We reviewed the three online training modules on privacy available to employees: “Privacy, Department of Veterans Affairs, and You,” “Privacy Awareness for Senior Executives,” and “VHA Privacy Policy Web Training,” and found varying levels of specificity and effectiveness.

- “Privacy, Department of Veterans Affairs, and You,” which is geared to employees needing a general knowledge on privacy requirements, provides an adequate overview of privacy issues but does not reference specific laws or VA policies except the provision in VA Directive 6300 that addresses the destruction of records.
- The “Privacy Awareness for Senior Executives Training” provides links to directives, manuals, and policies, and more detailed information on privacy protection, but lacks helpful ideas on how senior managers can implement policies to safeguard data adequately. A June 7, 2006, memorandum from the Under Secretary for Benefits to VBA employees states that the “Privacy Awareness for Senior Executives” training module does not satisfy the Secretary’s training requirement.
- The “VHA Privacy Policy Web Training” is the most detailed and comprehensive with respect to the applicable information laws and HIPAA requirements. It addresses the need to safeguard confidential information, but does not provide any specific requirements for how to protect the information.

None of the courses adequately tests employees' comprehension of course content. Employees can quickly click the screens to answer questions on cyber security without reading all information, and the VHA course can be completed without answering the test questions. All training modules require updating to reflect policies issued in the wake of the data loss.

In response to the data loss, the Secretary directed that all VA employees and contractors to complete training on cyber security and privacy awareness by June 30, 2006. While this is a good first step in increasing employee and contractor awareness, actions should be taken to reassess the sufficiency of these training materials, making them easier to locate and access, and strengthening the comprehensiveness of these courses.

VA Employees and Contractors Do Not Have Appropriate Sensitivity Level Designations

Our review of VA policy and selected employees' and contractors' sensitivity level designations found that VA employees either do not have appropriate sensitivity level designations or designations were inaccurate.

VA Directive 0710 establishes policy for the management of the personnel suitability and security program. The Directive pertains to VA applicants, appointees, and contract personnel for identification of a position's risk level as it relates to the efficiency and integrity of the Federal service and for determining the scope of a background investigation as it relates to risk level. The Directive states that high and moderate risk level positions are normally designated as Public Trust, which may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, etc.

VA Directive 0710 requires background screenings commensurate with the risk involved for any positions that require access to VA information systems. The Directive requires assessments for all positions by the appropriate ISO for the possible risk or harm that could result from an incumbent's loss, misuse, or unauthorized access to, or modification of, VA information, including the potential for harm or embarrassment to an individual who is the subject of the records. Although the ISO does the assessment, the final determination rests with the program office with delegated authority to make final suitability determinations.

In the present case, VA officials recognized this problem once they realized that the employee, who had legitimate access to a large volume of protected information, had never been vetted through the background investigation process for suitability. The employee's risk level, as indicated on his VA Form 2280, Position Sensitivity Level Designation, dated April 5, 2001, indicates that the position has a limited impact on the efficiency of the service with multi-agency scope of operations.

Our review revealed that a number of other employees assigned to OPP&P, some of whom have similar data access privileges, also had no suitability determinations. In fact, one of the systems of records that these employees have access to is BIRLS, one of the system extracts reported stolen on May 3, 2006. A recent assessment conducted at the request of VBA determined that the information sensitivity for BIRLS/VADS (Veterans Assistance Discharge System) was moderate for confidentiality, integrity, and availability. The evaluation also concluded that BIRLS/VADS should be classified as a mission critical system.

Position sensitivity determinations also apply to contract personnel. Information Letter (IL) 90-0106 issued by VA Office of Acquisition and Materiel Management on July 16, 2001, provided procedures to facilitate the security programs for VA automated information systems and guidance on the acquisition process relating to the established background requirements for contractor personnel. The IL states that VA policy requires that contracts contain an investigative requirement for the contractor position based on the pre-determined position sensitivity level designation. The IL further states that automated systems that contain information that is subject to the Privacy Act, or the modification of which could adversely affect the performance of Federal programs, are designated as sensitive. The sensitivity designation in VHA is determined by each VISN office, which has resulted in inconsistent and inaccurate designations.

A review of 20 selected proposals for contracts for physician services at VA medical centers showed that the positions in 16 proposals were designated as low-risk and a no-risk determination was made in the remaining 4 proposals. However, all of the physicians providing services under the contracts will have access to VA automated systems, including patient care records. The designation of low-risk is inconsistent with the level of responsibility and impact that these health care providers have on VA programs and operations.

Staff at one of the three medical centers we visited told us that the level of risk was minimal because the physicians did not have access to sensitive information, even though they had access to Veterans Health Information System Technology Architecture (VistA). Another medical center indicated the level of risk determination was impacted by the cost of a background investigation, not the actual risk involved. We have previously recommended in our FISMA reports that risk assessments be part of every position description and contract.

VA needs to insure that all positions have appropriate sensitivity designations and have nationwide designations for positions that have like or similar duties and access to VA's automated systems. Without these safeguards, VA systems and protected information at risk.

Protected Information Provided to Contractors Is Not Adequately Safeguarded

Our review of applicable VA policies, interviews of VA management, reviews of contract documents relating to solicitations and contracts from prior and ongoing OIG

investigations, audits, and reviews, and reviews of contract administration records at three VHA facilities determined that protected information provided to contractors was not adequately safeguarded.

We found that VA policy requires inclusion of two specific clauses in contracts that include access to Privacy Act protected information, as required in the Federal Acquisition Regulation (FAR). VA Handbook 6210, “Computer Security Training Protocols,” requires training for all VA elements and non-VA organizations that use VA automated systems, including contractors, which meets the requirements of FISMA.

In our interviews with CIOs, POs, and ISOs, we were assured that contractors who were provided privacy information and/or access to VA’s automated systems, including systems of records with patient related information, were notified of the provisions of the Privacy Act, other VA confidentiality statutes, VA Directive 6502, the associated handbooks, VA’s cyber security policies, etc. We also were told that contractors were required to sign Rules of Behavior to have access to VA systems and that they were required to report privacy violations as required by VA Directive 6502.1.

In our review of contract documents, we found that many contracts did not consistently include clauses to protect the information or the systems, contractors were not required to take and/or did not take Cyber Security and/or Privacy Awareness training, background investigations were not required or not done, and contractors were not always required to sign Rules of Behavior to access VA’s automated systems. Also, contract documents seldom referenced or included VA policies relating to safeguarding protected information or the security of automated information systems.

We selected 20 proposals submitted in response to solicitations for contracts for physician services that were to be awarded to VA affiliates under the provisions of 38 U.S.C. § 8153. All 20 were subject to legal/technical review prior to being sent to the OIG Office of Contract Review for a preaward review. The results show that the majority of the proposals reviewed did not require contractor personnel to comply with VA’s training requirements, to undergo background checks, or to report privacy violations as required by VA Handbook 6502.1. The results of our review are as follows:

Required Training			Required Compliance			Key Personnel Identified	Reporting of Privacy Violations
Privacy	Cyber Security	HIPAA	Background Checks	5 U.S.C 552a (Privacy Act)	38 U.S.C. 5701, 5705, 7332		
No - 19	No - 15	No - 18	No - 3	No - 0	No - 7	No - 9	No - 18
Yes - 1	Yes - 5	Yes - 2	Yes - 17	Yes - 20	Yes - 13	Yes - 11	Yes - 2

In addition to reviewing the 20 proposals, we visited three VA medical centers and reviewed documentation relating to the administration of contracts with affiliates for physician services. The following examples illustrate the vulnerabilities that exist with VA contracts in protecting VA systems and data:

- A contract for anesthesia services in effect since July 2005 had 29 physicians as potential providers. All 29 had been provided access to the surgical primary and secondary menus in VistA, which allows the user to view, enter, and edit patient information. None of the 29 physicians had any background checks. The Supervisory Human Resource (HR) Specialist told us that they generally do not conduct background checks for anesthesiologists because their jobs are not classified as sensitive positions. The Medical Center Director told us that all physicians have lower-level background checks because they do not deal with sensitive information. We were told that for low-level rated positions, HR only needs to check references and obtain fingerprints. Only one of the 29 anesthesiologists had fingerprints on file and no other checks were done on any of the providers. Only five had Privacy Awareness training and seven had Cyber Security Awareness training, and three did not sign Rules of Behavior.
- A contract for radiology services awarded on October 1, 2005, identified 19 physicians who could provide services under the contract. Eighteen physicians had been authorized access to VistA and 13 had VPN accounts for remote access. We found signed Rules of Behavior for all 18 physicians having VistA access. Background investigations had been completed on 12 physicians. No requests for background investigations had been made for five of the physicians and background investigations were requested and pending for two physicians. The positions were all designated as non-sensitive, low-risk. Although Cyber Security Awareness and Privacy Awareness training had been completed by all 19 physicians, 8 of the physicians took the training after we announced our visit. An employee in the Chief of Staff's office acknowledged that the training was completed based on our planned visit.

We reviewed contracts related to other OIG audits and reviews and found:

- The Statement of Work (SOW) for a contract awarded in 2005 by VHA to a consultant for the evaluation of VHA's purchase of health care from the private sector stated the contractor would have access to both printed and electronic documents that may be protected by the Privacy Act and Title 38 and that unauthorized disclosure is a criminal offense. FAR clauses 52.224-1 (Privacy Act Notification) and 52.224-2 (Privacy Act) were included in the SOW. The specific Title 38 provisions were not identified and Privacy Awareness training was not required. The SOW stated that the contractor may have access to proprietary information and agreed by the terms of the contract to protect the information and to follow all Government rules and regulations regarding information security. The specific rules and regulations were not identified, and VA's Cyber Security and Privacy Awareness training were not required. Although the contractor was advised that background

checks may be required, the task was not assigned a sensitivity level and specific background checks were not required.

- On May 13, 2005, VA issued a task order against an interagency agreement with DoD to have a Federally funded research group, IDA, perform a nationwide analysis relating to the variation in disability compensation claims, rating, and monetary benefits. Performance required access to protected information. Neither the interagency agreement nor the task order stated that the information provided the contractor will be protected under the Privacy Act or any other confidentiality statute. There was no requirement for Cyber Security or Privacy Awareness training, no sensitivity level determination, and no requirement for background investigations.

Policies and Procedures for Reporting and Investigating Lost or Stolen Protected Information Are Not Well Defined in VA Policies

Our review of relevant laws and VA policies and interviews of VA personnel determined that VA policies did not include adequate procedures reporting and investigation incidents involving lost or stolen protected information. In addition to not implementing procedures required by FISMA, VA did not implement the National Institute of Standards and Technology (NIST) recommendations for security incident responses. We also found three VA policies that address reporting privacy violations and information security incidents to be inconsistent with respect to the information that should be reported, the time frames required for reporting, and to whom the incident should be reported, including reporting to law enforcement.

Section 3544 b (7) of FISMA requires VA to implement an agency-wide information security program that includes procedures for detecting, reporting and responding to security incidents. These procedures must include notifying and consulting with the Federal information security center as well as appropriate law enforcement agencies and relevant Offices of Inspector General. We did not identify a VA policy that implements this requirement.

NIST Special Publication, “Computer Security Incident Handling Guide” (Guide), does not have specific requirements for reporting to law enforcement but does suggest that the response team become acquainted with various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how the evidence should be collected. We did not identify any VA policies implementing the NIST recommendations.

VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records, Section 6, Description of Privacy Act Reviews, paragraph g, states that VA employees are required to report any suspected criminal violations of the Privacy Act. It does not provide any specific time frame or instructions for reporting. This provision is not visible to the average employee because it is contained in a policy applicable to

employees involved in establishing and maintaining Privacy Act systems of records and in a paragraph that impacts employees conducting Privacy Act reviews.

VA Directive 6210, Automated Information Systems Security, has not been updated since it was issued in January 1997. The Directive requires VA to establish, maintain, and enforce AIS security incident reporting and response capability to ensure that computer security incidents are detected, reported, and corrected at the earliest possible time. The Handbook requires that security incidents be reported to the ISO within 48 hours of the occurrence to the VA Information Resources Security Officer. The policy identifies specific information that must be reported, including whether the Inspector General or appropriate law enforcement organization was notified. It does not specifically mandate reporting the incident to the VA OIG or to another VA law enforcement entity, and it does not seem to pertain to the May 3, 2006, incident because the incident did not involve an unauthorized intrusion into VA's automated system.

The Privacy Act and other information laws do not require reporting incidents. To comply with the provisions of HIPAA, VA issued VA Directive 6502 and VA Handbook 6502.1. VA Handbook 6502.1 establishes VA-wide procedures for recording privacy-related complaints and violations in the VA Privacy Violation Tracking System (PVTS). The PVTS supports HIPAA's "documentation of complaints" requirement. The Handbook assigns POs the responsibility for recording all privacy-related complaints and violations, their updates, and resolutions to the PVTS as soon as possible. The PO also is tasked with resolving complaints and violations as soon as possible through corrective actions which include education, reprimand, sanction, or a determination that there was no breach.

The process outlined in the Handbook is the same regardless of the magnitude of the violation. The only provision for referring a complaint or violation through the privacy hierarchy is if the PO cannot resolve the complaint or violation. In contrast to VA Handbook 6210, VA Handbook 6502.1 does not provide specific time frames for reporting, investigating, or resolving complaints or violations and does not specify what information must be ascertained during an investigation.

VA Directive 6502, paragraph g (13), requires that VA officials "ensure that all alleged breaches of applicable Federal privacy law, that on their face, constitute a criminal violation of law, are referred for investigation to the Office of Inspector General." Whether this Directive applied to the May 3, 2006, incident is difficult to determine, because it would all depend on the facts presented at the time of the incident and the how the person receiving this information interpreted it. The application of this matter is discussed in more detail in Issue 4.

Policy Changes Implemented by VA Since the Incident Are a Positive Step, but More Needs to Be Done to Prevent Similar Incidents

Our review of policy changes and communications issued by VA since the date of the information security incident determined that actions taken since May 3, 2006, are insufficient to prevent similar incidents in the future. We found that VA has taken positive steps in addressing the policy inadequacies, but additional actions are needed.

VA has issued a number of statements and directives affecting the use of information by VA employees. VA has taken the following actions since May 3, 2006.

- May 22, 2006 – Memorandum to all VA employees required all employees to complete Cyber Security and Privacy Awareness training by June 30, 2006.
- May 26, 2006 – Directive required all employees to complete Cyber Security and Privacy Awareness training by June 30, 2006.
- June 5, 2006 – Memorandum required all organizations to identify teleworkers by June 6, 2006.
- June 6, 2006 – Memorandum suspended the practice permitting VBA employees to remove claims files from the regular workstations in order to adjudicate claims from an alternative worksite.
- June 6, 2006 – Memorandum issued VA IT Directive 06-2, which requires supervisory approval before removing confidential and Privacy Act protected information from the worksite in any data format.
- June 7, 2006 – All organizations were directed to complete a data access inventory for each employee by June 21, 2006.
- June 7, 2006 – VA Directive 6504, Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities.

VA IT Directive 06-2 addresses some of the gaps in policy, including requirements for data encryption and password protection in accordance with VA policy when employees are authorized to remove electronic data. Directive 06-2 also requires employees who lose confidential or Privacy Act protected data to report the loss immediately to the facility or staff office ISO, the PO, and the employee's immediate supervisor. However, Directive 06-2 does not cover issues relating to loading, processing, and storing protected information on a non-VA computer or the destruction of the data/computer. In addition, it is not clear whether use of the term "confidential" refers to personal and proprietary information, as the term is used in FISMA, or if this means "confidential" as used by the DoD. If the later, the Directive does not protect proprietary information.

Directive 6504 contains policy for 23 different items. With respect to the circumstances relating to the recent incident involving loss of data, the Directive permits VA employees to transport, transmit, access, and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor. The Directive

prohibits the use of non-VA owned equipment to access the VA Intranet remotely or to process VA protected information except as provided in the Directive.

However, we found that the Directive was difficult to understand; too technical for the average employee to understand; used terms, such as “appropriate,” that were too vague to ensure compliance; and made references to other applicable policies, guidelines, and laws without identifying them.

The following actions by VA will further ensure protected information is safeguarded:

- Issue one clear, concise policy on safeguarding protected information when stored and not stored on VA’s automated systems. The policy should clearly define what information is protected from disclosure.
- Address policies and procedures individually for accessing, using, transporting, and transmitting protected information.
- Require that all VA employees and contract employees acknowledge that they received, reviewed, and understand the policy.
- Modify Cyber Security and Privacy Awareness training to include references to all relevant VA policies and that users complete the training in their entirety to obtain certification.
- Have one Privacy Awareness training program for all employees.
- Consider prohibiting the use of non-VA computers to store and process VA protected information unless VA can be assured that the computers have the same level of safeguards to protect information as required for VA computers.
- Ensure that all VA contracts contain terms and conditions to safeguard VA protected information.
- Hold individuals accountable for non-compliance as well as responsible managers, supervisors, contracting officers, and contracting officer’s technical representatives.

Under the Privacy Act and other information laws, the Secretary is ultimately responsible for ensuring that protected information is safeguarded from inappropriate disclosure. To this end, the Secretary has the authority to issue and enforce national policy affecting VA employees and contractors who have access to protected information. Centralized policies for handling protected information will help ensure consistency in safeguarding the information and preventing the fragmentation, overlap, and the confusion that occurs when entities in VA issue their own policies. VA policies should also establish clear processes and procedures with well defined responsibilities for the reporting and investigation of protected information.

Conclusion

Our review found that VA did not have policies and procedures in place that would have prevented the potential disclosure of protected information. The patchwork of existing VA policies was difficult to locate, fragmented, overlapping and confusing. VA's Cyber Security and Privacy Awareness training do not ensure that employees and contractors are adequately familiar with the applicable laws and VA policies. The fact that VA does not adequately assess sensitivity levels to positions increases the risk of future disclosure problems. In addition, VA contracts that involve access to protected information and access to VA's automated systems do not adequately protect the information or the automated systems. We also found that VA did not have clear, consistent policies and procedures in place to ensure employees take timely and appropriate action when information is lost or stolen and that VA needs to take further action to ensure similar disclosures of protected information are prevented in the future.

Recommendations

To address the issues raised in this section, we recommend that the Secretary:

- a. Establish one clear, concise VA policy on safeguarding protected information when stored or not stored on a VA automated system, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.
- b. Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.
- c. Ensure that all position descriptions are evaluated and have proper sensitivity level designations, that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and automated systems, and that all required background checks are completed in a timely manner.
- d. Establish VA-wide policy for contracts that require access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored, or processed on non-VA automated systems is safeguarded.
- e. Establish a VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

Issue 6: Whether Audits and Reviews of VA's Information Management Security Program Controls Continue to Identify Vulnerabilities

During the past several years we have conducted a number of audits and evaluations on information management security and IT systems that have shown the need for continued improvements in addressing security weaknesses. We have reported VA information security controls as a material weakness in the annual Consolidated Financial Statements (CFS) audits since the FY 1997 audit. Our FISMA audits have identified significant information security vulnerabilities since FY 2001. We continue to report security weaknesses and vulnerabilities at VHA health care facilities and VBA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews. We have also identified IT security as a Major Management Challenge for the Department each year for the past 6 years.

Consolidated Financial Statement Audits Continue to Report Information Security as a Material Weakness

As part of the CFS audit, IT security controls have been reported as a material weakness for many years. A material weakness is defined as a weakness in internal control that could have a material effect on the financial statements and not be detected by employees in the normal course of their business. We have reported that VA's program and financial data are at risk due to serious weaknesses related to: inadequate implementation and enforcement of access controls over access to financial management systems and data; improper segregation of key duties and responsibilities of employees in operating and maintaining key systems; underdeveloped IT service continuity planning; and inconsistent development and implementation of system change controls.

Testing disclosed strong access authentication mechanisms and administration of user access have not been consistently implemented and enforced. There were ineffective monitoring and review of user access profiles. Intrusion detection mechanisms, and coordination and communication between Central Incident Response group and local security functions were not operating promptly and effectively to detect and resolve potential security violations from internal sources. Some systems have not been configured to support proper implementation of system segregation of duties. A business continuity plan at the departmental level has not been fully developed to provide overall guidance, direction, and coordination for IT service continuity and testing at certain medical facilities and data centers has not been consistently scheduled and adequately performed. Testing also disclosed that VA policy does not provide uniformed guidance for a wide-range of new and legacy applications to facilitate consistent implementation and effective monitoring of changes. As a result of these vulnerabilities, we recommended that VA pursue a more centralized approach, apply appropriate resources, and establish a clear chain-of-command and accountability structure to implement and enforce IT internal controls.

CFS audits have also found that VA managers needed to:

- Improve access control policies and procedures for configuring security settings on operating systems, improve administration of user access, and detect and resolve potential access violations.
- Evaluate user functional access needs and system access privileges to support proper segregation of duties within financial applications. Assign, communicate, and coordinate responsibility for enforcing and monitoring such controls consistently throughout VA.
- Develop a service continuity plan at the departmental level that will facilitate effective communication and implementation of overall guidance and standards, and provide coordination of VA's service continuity effort. Schedule and adequately test IT disaster recovery plans to ensure continuity of operations in the event of a disruption of service.
- Develop a change control framework and, within that framework, implement application specific change control procedures for mission critical systems.

VA has implemented some recommendations for specific locations identified but has not made corrections VA-wide. For example, we found violations of password policies which management immediately corrected, but in following years, we found similar violations at other facilities. We also found instances of terminated or separated employees with access to critical systems identified at various locations which management corrected, only to discover similar instances elsewhere. Consequently, we continue to report information security as a material weakness, which was highlighted in the VA FY 2005 Annual Performance and Accountability Report, dated November 15, 2005.

Annual Evaluations of VA's Information Security Program Have Identified Vulnerabilities That Remain Uncorrected

In all four FISMA audits of the VA Security Program issued since 2001, we reported vulnerabilities that continue to need management attention. These reports highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for centralization, remediation, and accountability in VA information security. Since the FY 2001 report, we reported weaknesses in physical security, electronic security, and internal reporting, and since 2002, we also reported weaknesses in wireless security and personnel security. Additionally, we have reported significant issues with implementation of security initiatives VA-wide.

The FY 2004 audit also emphasized the need to centralize the IT security program, implement security initiatives, and close security vulnerabilities. We previously recognized that the Office of the Assistant Secretary for Information and Technology/CIO office needed to be fully staffed, and that funding delays and

resistance by offices to relinquish their own security functions and activities delayed implementation of the fully centralized CIO contemplated by our prior recommendations. The CIO's comments to the report referenced an April 2004 VA General Counsel opinion that the CIO interpreted as restricting his office from gaining the authority to enforce compliance with the VA information security program, and hindering his ability to address the identified vulnerabilities. We again recommended that VA fully implement and fund a centralized VA-wide IT security program.

The following 17 issues continue to warrant management attention.

1. Implementation of a Centralized Agency-Wide IT Security Program

The CIO is VA's focal point for IT matters. The Secretary has designated the Assistant Secretary for Information and Technology as the VA CIO. Although the CIO is responsible for VA's information systems, operational controls were decentralized among each administration within VA. The operational control was, until recently, vested with VHA, VBA, National Cemetery Administration (NCA), and other program offices in VA. The CIO provided guidance and the tools to support the activities with operational control to secure VA systems, but the CIO did not have the ability to enforce or hold officials accountable for non-compliance. The CIO was responsible for the general management of all VA IT resources, including policy guidance, budgetary review, and general oversight. However, the implementation of the information security program was accomplished by VA personnel who were not under the direct supervision or control of the CIO.

VA informed Congress that it plans to move towards a "federated IT system" to realign department-wide IT operations and maintenance responsibilities under the direct authority of the CIO. The main feature of the realignment will place VA's IT budget, along with IT professionals involved in operation and maintenance work, directly under the authority of the CIO. However, IT employees involved in system development will remain under their respective administrations and staff offices (e.g., VHA, VBA, NCA, and some program offices). Given that the planned realignment has just begun, VA's federated IT system implementation plans will need further study. For example, we will need to review whether existing IT systems and operations under the purview of the CIO will efficiently and effectively communicate with newly designed applications implemented by these system development offices.

2. Implementation of a Patch Management Program

VA continues to review and address patch management issues to find long-term solutions. We previously identified a number of critical patches that were either not installed or not appropriately implemented at the VA facilities reviewed. VA did not have an enterprise-wide solution that could directly connect to over 250,000 points within VA. During our FY 2005 audit, VA continued to evaluate solutions to remediate this condition. VA was still in the process of developing and fully deploying a patch management program. VA's CIO identified roles and responsibilities to address VA

Enterprise Patch Management processes and standard operating procedures. A January 7, 2005, memorandum, Enterprise Patch Management, signed by the CIO, details patch management roles, responsibilities, and special considerations.

3. Electronic Security

Our reviews conducted at new sites visited during FY 2005 found potential vulnerabilities that we previously identified relating to password controls, remote access, and securing critical files. Additionally, we continued to find security vulnerabilities related to the lack of segregation of duties; unsecured critical files, which could allow attackers access to password files; and inappropriate access through remote access software. Our field work at facilities not previously visited in prior years found potential vulnerabilities warranting management attention. The reviews indicate that while managers at sites visited are addressing vulnerabilities identified during these reviews, sites not visited in prior years have not been advised that the vulnerabilities identified may be systemic in nature. VA needs a consistent approach at all of its facilities to effectively monitor networks and to use tools, such as electronic scanning, to proactively identify and correct security vulnerabilities.

4. Personnel Security

In FY 2005, we continued to find previously identified weaknesses related to position descriptions and training of VA employees and contractors. Sensitive position descriptions needed better documentation. We found the sensitivity rating was inaccurate for some employee positions at facilities reviewed and that position descriptions needed to more specifically address the levels of access relative to the positions' duties and responsibilities.

5. Background Investigations

VA needs to ensure that employee and contractor background investigation requirements are adequately identified and addressed. In FY 2005, we identified instances where background investigations and reinvestigations were not initiated in a timely manner on employees and contractors, or were not initiated at all.

6. Deployment and Installation of Intrusion Detection Systems

Although much has been done, the VA's Office of Cyber and Information Security (OCIS) still needs to validate whether VA completed installation of Intrusion Detection Systems (IDS) at all sites. Deploying and installing IDS is a key step in the process of securing VA data systems on a national basis. Implementation of IDS increases VA's ability to detect intrusions. OCIS advised us that an enterprise-wide IDS has been fully implemented. In addition, OCIS is researching the benefits of moving to Intrusion Prevention Systems in an effort to provide VA the capability to detect and prevent "attacks."

7. Infrastructure Protection Actions

VA needs to complete infrastructure planning efforts. During our FY 2004 audit, we found examples where the physical infrastructure had significant vulnerabilities and did not adequately protect data from potential destruction, manipulation, and inappropriate disclosure. During our FY 2005 field work, we found that VA was developing a Critical Infrastructure Protection Plan, and completed an identification and prioritization of critical information resources.

8. Information Technology Centers' Continuity of Operations Plans

VA is making progress and had completed Continuity of Operations (COOP) plans but full testing needs to be done. VA has issued an Emergency Preparedness Directive/Handbook 0320 for the VACO COOP. VA was developing a Master COOP for the entire VA, which will include all elements in the Central Office COOP. NIST 800-34, "Contingency Planning Guide for Information Technology Systems," dated June 2002 recommends COOP testing should be accomplished at least annually. COOPs covering Information technology Centers (ITCs) need to ensure capabilities exist to provide necessary operational support in the event of disasters. Our field tests conducted in FY 2005 showed that the ITCs have completed these contingency plans, but that testing these plans needed to be jointly done among all program offices residing in the ITCs. After FY 2005 field work was completed, we learned that VBA-related hardware had been procured at one ITC to back up data, and some independent testing has been performed. VBA informed us that they recently conducted tests at their ITCs and performed disaster recovery exercises. While this is a step forward, joint testing by all covered ITC offices is needed.

9. Certification and Accreditation Process

During FY 2005 field work, we found that VA had placed a priority on the uncompleted Certification and Accreditation (C&A) process. The number of VA systems and major applications decreased from 678 in FY 2004 to 585 in FY 2005, as a result of VA combining applications or by removing previously reported systems that did not meet the NIST criteria. At the end of our field work in the summer of 2005, VA had not completed a C&A for all systems and major applications. The Secretary had made it a priority to complete all C&A work by the end of August 2005, and in November 2005, VA reported to the Office of Management and Budget that it had completed a C&A for all VA systems and major applications.

10. Terminate/Upgrade External Connections

In prior audits, we reported security risks associated with the operation of uncertified Internet gateways. As of FY 2005, VA took actions to mitigate these risks by limiting the number of Internet gateways in order to improve control over access to VA systems. Field work conducted in FY 2005 found that VA is still unable to determine if all extraneous external connections have been terminated. We are currently unsure of the

extent VA and its affiliated and non-affiliated partners may be operating their own gateways. We also found that the standard contract VA used to procure computers included modem devices as a standard feature, which if retained in default settings could serve as access points for hackers attempting to gain entry into VA systems. A January 11, 2005, OIG report on procurement of desktop modems prompted VA to amend its contract and to address the modem security vulnerabilities with all facilities.

11. Configuration Management

Prior year audits have found instances where VA networks relied on old operating systems such as Windows 95 and Windows 98, which placed the VA networks at risk due to the lack of vendor support to upgrade security and other features. An unsupported operating system, whether desktop or production mainframe, exposes VA to potential security and operational risks, including operating system failure. During FY 2005 field work, we found VA had reduced the number of personal computers running Windows 95, but other aged computers must continue to operate due to special document scanners associated with The Imaging Management System. We were told that these scanners and personal computers are expected to be replaced or retired during FY 2006, if funds are available. Additionally, OCIS confirmed VHA has not completed the conversion of 162 older operating systems. In order to mitigate the risks associated with the older operating systems, VHA moved the devices to a virtual local area network configuration with restricted access.

12. Movement and Consolidation of VACO's Data Center

We previously reported that the VACO data center was located below ground level and experienced water damage twice in the last 10 years. VA reported the relocation of the VACO data center is in progress. In the interim, VA placed equipment in multiple locations throughout the Washington, D.C., metropolitan area until procurement and construction is completed at a new location. Even though progress has been made, we identified routers and switches that support VACO network operations that remain below ground level.

13. Application Program/Operating System Change Controls

VA change control policy does not provide uniform application development and change guidance for a wide range of new and legacy applications. Nationwide policy is necessary to facilitate consistent implementation and effective monitoring of system change controls for mission critical systems. For example, we found changes to a mainframe operating system and supporting hardware were not supported by local management authorization. Additionally, we found instances where changes to the production environment were not adequately documented or approved for major applications and critical systems. Consequently, unauthorized changes could have adversely affected the production environment or lead to misuse without warning.

14. Physical Access Controls

At previous sites visited, VA was attempting to make improvements to ensure adequate measures were implemented to secure veterans' information and provide a safe environment for employees and visitors. However, our facility reviews at new locations showed physical access controls still need improvement. For example, a number of facilities granted access to computer rooms to employees who did not have a need to be in the computer room to perform their job function, and some contractors did not have an escort while in the computer room.

15. Wireless Security

VA is making progress in reducing wireless security vulnerabilities by securing its network from outside intrusion. Actions were taken to install an encryption wireless product that is designed to prohibit unauthorized users from accessing the network. However, our penetration test showed some vulnerability in the wireless network could be used to view transmissions, including those containing patient data, and to gain access to systems residing on VA's internal networks. Despite improvements, VA's information systems remained at risk for unauthorized access or misuse of sensitive information.

16. Encrypting Sensitive Information on VA Networks

VA has stated that it was taking interim steps to improve transmission of protected and sensitive information over its networks as sensitive data continues to be transmitted in clear text on VA networks. VA informed us that installation of encryption capabilities on some of its older platforms would render the systems inefficient. VA was looking for solutions to establish controls to secure electronic protected health information. Field tests conducted in FY 2005 continued to demonstrate the need to improve controls as our contractor's penetration test showed an intruder could successfully view protected health information in unencrypted clear text from outside a VA network. Site work also showed examples where unencrypted protected health information was vulnerable at other VHA facilities. The CIO informed us that a Transmission of Privacy Information in Clear Text work group was established to determine: (1) classes of data within the VA, (2) sensitivity ratings for these data classes, (3) strategies for implementing controls for the protection of these data classes, and (4) the most efficient and effective way to protect the privacy of veteran information electronically transmitted across the network.

17. FISMA Reporting Database

FISMA establishes security requirements and requires VA to annually report vulnerabilities for systems and major applications. While VA is taking actions to address security vulnerabilities, we continue to identify weaknesses that require a centralized and coordinated effort to ensure corrective actions are taken to control access, to secure computer rooms, and to ensure facilities accurately report their security deficiencies that place VA information and data at risk. The FISMA database

contains the self-assessment surveys of VA's major applications and systems. System and application deficiencies, as well as funded and unfunded remediation plans, are reported and stored in this database. Consequently, this database needs to accurately demonstrate the security posture of VA's systems and major applications. Also, it should accurately depict the risk of loss of the critical and sensitive information contained within these systems and major applications.

Comparisons of the sites visited to the entries in the FISMA database found that not all information was accurate or complete. Most inaccuracies involved reporting of the five levels of IT security program effectiveness outlined in the Federal Information Technology Security Assessment Framework. Additionally, we found no evidence that facilities were held accountable for information inaccuracies or incomplete data in the database. For example, fields requiring information pertaining to the amount of funding needed to correct deficiencies were incomplete. Areas needing clarification included physical security controls, risk assessments performed and documented as required, password controls, personnel sensitivity designations, and personnel background investigations. VA senior leadership needs this information to determine the costs to correct the conditions identified. With inaccurate or incomplete information in the FISMA database, VA senior leadership will not have a complete picture of VA's information security posture and the level of resources and funding needed to remediate security deficiencies.

VA is currently developing policies and procedures for implementing a federated approach to managing IT security and resources, and is still in the process of addressing recommendations made during prior FISMA audits. VA has made progress during FY 2005 to improve IT controls and to implement some recommendations. For example, after the FY 2005 testing was completed, VA informed us that certification and accreditation reviews have been completed and the deployment of IDS has been accomplished. We will validate implementation in future annual FISMA audits. We have not made recommendations in reference to these issues because VA will comment on them in the most recent FISMA report.

Combined Assessment Program (CAP) Reviews Show Information System Security Vulnerabilities Continue to Exist

We continue to identify instances where out-based employees send veterans' medical information to the VA regional office via unencrypted e-mail; system access for separated employees is not terminated; monitoring remote network access and usage does not routinely occur; and off duty users' access to VA computer systems and sensitive information is not restricted. We continue to make recommendations to improve security and contingency plans, control access to information systems, complete background investigations and annual security awareness training, and improve physical security controls.

While individual and regional managers have concurred with these CAP recommendations, and our follow-up process confirms actions to resolve the specific

conditions identified at these sites, we continue to find that corrective actions are not applied to all facilities to correct conditions nationwide. As a result, we continue to find these systemic conditions at other sites we visit. For example,

- At a VA Healthcare System, we found that computer access privileges were not promptly terminated or modified when users separated from the facility. IT contingency plans did not include all critical elements to ensure continuity of operations during a disaster or emergency, and annual IT security awareness training was not completed by all active users.
- At a VARO, we identified the need for managers to ensure that Benefits Delivery Network commands requested were necessary and that employees' claims folders were electronically locked. As employees' duties change, the allowed commands and the need for new BDN access commands needs to be evaluated. Testing found that 7 of the 20 access commands authorized permitted employees the rights to use more data files than was needed to perform their current assignments.

Between FYs 2000 and 2005, the CAP program identified IT and security deficiencies in 141 (78 percent) of 181 VHA facilities reviewed. We identified IT and security deficiencies at 37 (67 percent) of 55 VBA facilities reviewed. These reviews add further support to our conclusion that VA needs a centralized approach to standardize operations and address systemic issues nationwide.

Conclusion

Our CFS audits, FISMA audits, and individual CAP reports of VA medical facilities and regional offices all highlight specific vulnerabilities that can be exploited, but the recurring themes in these reports are the need for a centralized approach to achieve standardization in VA, remediation of identified weaknesses, and accountability in VA information security. Specific recommendations were not made in this section because, while the 17 recommendations remain unimplemented, they are listed in previously issued OIG reports. We will continue to follow up on these recommendations until fully implemented.

Secretary's Comments



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

July 6, 2006

The Honorable George J. Opfer
Inspector General
Department of Veterans Affairs
Washington, DC 20420

Dear Mr. Opfer:

Thank you for the opportunity to review and respond to the report on events related to the Department of Veterans Affairs' (VA) data loss. I fully concur with the recommendations contained in the report.

The tragic event that was the impetus for the report exposed deficiencies in information security involving leadership, policies and procedures. That will change during my tenure as Secretary of Veterans Affairs. On June 28, 2006, I signed a memorandum delegating to the VA Chief Information Officer (CIO) all authority and responsibilities given to me by the Federal Information Security Management Act (FISMA). This delegation restructures responsibilities and authorities for information security here at the VA and initiates the needed cultural changes that must occur. I have made it clear to all senior managers in the Department that information security, cyber security and the reorganization of the Office of Information Technology (OIT) are my top priorities going forward.

I have promised our veterans and employees that VA will become a Gold Standard and recognized leader in security of personal information. I will settle for nothing less. To accomplish this ambitious goal we must work diligently to establish a culture that embraces these standards. We will not stop until we have accomplished our objective of leading the federal government in information and cyber security policies and procedures, just as we accomplished the monumental change in our health care system over the past decade. VA is the leader in patient safety and quality of care, and we can become the leader in information security.

The Honorable George J. Opfer
Inspector General
Page 2

Your report has provided us with a template for the changes and initiatives needed to make our transformation. Some of these changes are currently underway in the Department and some will begin soon. I realize, however, that the recommendations contained in this report are just a start. Achieving our goal of leadership in the federal government in protecting personal information will require much more. I intend to enlist the assistance of leading experts in the field of data security to assist us in identifying our path to reach the "Gold Standard." By "Gold Standard" I mean that VA must be the best in the federal government in protecting personal and health information, training and educating our employees in best practices, and establishing a culture that always puts the custody of veterans' personal information first, over and above employee convenience or expediency. It is raising our scores in the annual FISMA audit to an "A" and becoming the system to emulate for all other agencies. Our Nation's heroes deserve only the best we can provide in data protection.

Training in information and cyber security will be a vital component of our transformation. To ensure quality and consistency in training, I have directed establishment of a new Office of Cyber & Information Security Training (OCIST) in the Office of Information Technology. That office will be responsible for a training program that begins with new employee orientation and continues through senior leadership, including such programs as Leadership VA, the SES Candidate Development Program and the Senior Leadership Academy. I envision a continual emphasis on information security throughout an employee's career.

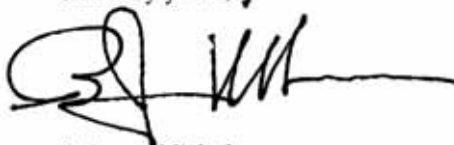
Excellence in information security will take the full commitment of VA's senior leadership, both political appointees and career senior executives. It will also take money, and we will seek the budgetary resources that we need for success from the Administration and the Congress. It will also take time, but my sense of urgency is clear. My focus is the Gold Standard for information security and I will require steady progress toward that goal. Industry experts will help us develop the program changes and validate our timelines. All employees will be held accountable for safeguarding the private information entrusted to us by veterans and beneficiaries. I will not be satisfied until VA is recognized as the leader in the federal government in information security.

The Honorable George J. Opfer
Inspector General
Page 3

Enclosed you will find a detailed response to each of the recommendations contained in the report. To address each recommendation, I have included actions taken to date and numerous other planned actions. VA will continue to work with you as we implement these changes.

If you have questions related to our responses, please feel free to contact me directly.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'R. James Nicholson', with a long horizontal flourish extending to the right.

R. James Nicholson

Enclosures

ISSUES 1 – 4: Issues Related to the Departmental Response to the Data Breach.

Recommendation 1: Take whatever administrative actions deemed appropriate concerning the individuals involved in the inappropriate and untimely handling of the notification of stolen VA data involving the personal identifiers of millions of veterans.

Concur

Target Completion: August 4, 2006

I have directed four separate Administrative Investigations (AI). The AIs are detailed below.

I have directed an Administrative Investigation to review the actions of the employees in the Office of Policy and Planning following the data breach. I anticipate the results of the Investigation by August 4, 2006. I note that Mr. McLendon resigned on June 2, 2006 and that Mr. Duffy retired on June 30, 2006. Charge letter is attached. (TAB 1)

I have directed an Administrative Investigation to review the actions of the employees in the Office of General Counsel following the data breach. I anticipate the results of the Investigation by August 4, 2006. Charge letter is attached. (TAB 1)

I have directed an Administrative Investigation to review actions of the employees in the Office of Security and Law Enforcement following the data breach. I anticipate the results of the Investigation by August 4, 2006. Charge letter is attached. (TAB 1)

I have directed an Administrative Investigation to review the actions of the employees in the Office of Cyber and Information Security and Security Operations Center as they relate to this incident. I anticipate the results of the Investigation by August 4, 2006. We note that Mr. Johnny Davis, Jr., Acting Assistant Deputy Assistant Secretary for Cyber Security Operations, transferred to another Federal Agency effective July 9, 2006, and Mr. Pedro Cadenas, Director of the Office of Cyber and Information Security, has resigned with an effective date of July 13, 2006. Charge letter is attached. (TAB 1)

With respect to the political appointees who serve on my immediate staff, I will carefully review the materials concerning their actions and make decisions accordingly. Central to all of the decisions that I will make regarding personnel cited in your report will be what is best for VA and the veterans we serve.

1. Implementation of a Centralized Agency-wide IT Security Program

As part of the actions taken to centralize the operations and maintenance function within the Office of the CIO, the responsibility for IT security has, in fact, been centralized. This will greatly enhance VA's ability to provide clear direction and enforce compliance in a wide variety of security and privacy-related areas. Additionally, the June 28, 2006, Delegation of Authority memorandum (TAB 6) will greatly enhance the ability of the CIO to enforce compliance. An organizational chart is attached. (TAB 7).

In October 2005, I signed a memorandum directing the reorganization of IT within VA. Pursuant to that reorganization, more than 4,610 IT professionals engaged in operations and maintenance of the Department's IT infrastructure, plus 560 unencumbered positions, have been detailed to the Office of Information and Technology, under the direction of the Chief Information Officer. As of the beginning of the new Fiscal Year on October 1, 2006, those IT professionals will become permanently assigned to OIT, and concurrently a new career field within OIT will be established.

In this IT reorganization, all IT professionals, except for certain software developers, are being consolidated into the Office of Information and Technology. The CIO will be responsible for enterprise architecture, project planning approval through the OMB 300 process, funding and cyber and information security for all IT professionals including software developers.

Other functions are being centralized within VA IT as well. I established the new position of Chief Financial Officer (CFO) for OIT with budget authority over all funds in the Office of Information and Technology, including the new IT Fund established by Congress. Recruiting for this position is well underway.

In the past, there have been questions regarding the authority to the CIO under the Federal Information Security Management Act (FISMA). On June 28, 2006, I signed a Memorandum explicitly delegating all information security authority and responsibilities granted to me under FISMA, including enforcement, to the CIO.

I announced at a Congressional oversight hearing of the House Committee on Veterans' Affairs on June 29, 2006, that I plan to further centralize all IT development in the future.

2. Implementation of a Patch Management Program

As stated in the VA response in the last FISMA report, OIT established a patch management program that will be further enhanced as a result of the reorganization mentioned above. This will include the implementation of an Enterprise Security Framework, which is being piloted at several sites in FY 06 in anticipation of deployment beginning in FY 07.

3. Electronic Security

As a result of our IT Reorganization, improvements have already begun to remedy these issues. The Assistant Secretary for Information & Technology has been delegated full authority and responsibility for policy, training, inspection, enforcement and incident response.

The CIO has established a "Transmission of Privacy Information in Clear Text (TOPIC)" work group to determine classes of data within the VA environment. This effort will be intensified and will focus on developing strategies for implementing controls to protect classes of sensitive information. In the interim, OCIS is working with the Administrations to increase the application of "Public Key Infrastructure (PKI)" certificates to protect sensitive email transmissions. These will include correcting deficiencies regarding password controls, remote access, and security of critical files. These efforts are expected to complete by February 2007.

4. Personnel Security

As stated in the response to Issue 5, I fully concur with this recommendation. An extensive effort is under way to improve the Department's performance in the areas of sensitivity risk identification and the corresponding background investigations.

To summarize our efforts:

VA Administrations and Staff Offices, in consultation with the CIO and HR, are undertaking a complete review of position sensitivity/risk level designations and existing background investigation levels for all employees, volunteers, interns, students, residents, contractors and sub-contractors. By October 31, 2006, all Administrations and Staff Offices will complete the review of position sensitivity/risk level designations and establish commensurate background investigation requirements. Senior executives will ensure the update of official

personnel folders and the amendment and revision of contracts, as necessary, to document the revised sensitivity level designations and commensurate background investigation requirements.

New background investigations, where needed, will be initiated as soon as possible.

VA Directive/Handbook 0710, Personnel Suitability and Security Program, will be revised by December 31, 2006 to reflect the expanded requirements.

Additionally, the performance plans for all supervisors, managers and senior executives will include a specific requirement for the protection of sensitive information and responsibilities.

Training courses in Suitability Adjudication and Position Sensitivity/Risk Designation have been conducted for human resources personnel. VA will seek a digital position management system that will automate classification and position sensitivity/risk designation.

5. Background Investigations

As stated in our response to Issue 5, an extensive effort is under way to improve the VA's performance regarding background investigations - with special emphasis on those positions requiring extensive access to sensitive information and computer systems/networks. VA is working aggressively to resolve problems that have existed for some time with background investigations. As a result, a number of activities have occurred or have been planned. Specifics are provided in item 4 above.

One of the improvements is the use of the Electronics Questionnaires for Investigations Processing (e-QIP), an OPM sponsored system designed to allow electronic completion and submission of all personnel investigation forms to OPM for completion of the investigations. VA is actively involved in the implementation of e-QIP. The current schedule will result in over 70% of VA facilities utilizing e-QIP by December 31, 2006, and 100% usage by March 2007.

6. Deployment and Installation of Intrusion Detection Systems

Although action is already underway to remedy this condition and improvements have taken place, additional review is needed. As part of the reorganization of

the Office of Information and Technology, including the Office of Cyber and Information Security, the CIO will establish a robust audit and inspection capability. This, along with the Delegation of Authority Memorandum mentioned earlier, will further enhance the ability of the CIO to ensure intrusion detection devices, to warn of unauthorized entry, are in place, and that they remain in place and in use.

7. Infrastructure Protection Actions

Work continues on the VA's critical infrastructure protection plan, but what is needed is more rigorous audit and inspection of existing conditions regarding the inappropriate destruction, manipulation or disclosure of sensitive information. A VA "Critical Infrastructure Protection Plan" is in development. Progress has been made at the Department level on completion of a Continuity of Operations Plan (COOP) and completion of an Emergency Preparedness Directive/Handbook 0320. VA is currently developing a Master COOP plan which will include the VA Central Office (VACO) and individual COOPs.

8. Information Technology Centers' Continuity of Operations Plans

VA continues to make progress in this area. The Austin Automation Center continues to conduct COOP tests annually and has worked to integrate its COOP with the resident organizations at its facility and the Hines and Philadelphia IT Centers. More extensive testing needs to be accomplished and as part of the action plan noted earlier; such testing will take place during FY 07 and be complete by August 2007.

9. Certification and Accreditation Process

Although the IG found that extensive C&A's were accomplished by the end of 2005, VA has recently discovered, as a result of a comprehensive data call, that additional systems exist which may require certification and accreditation. This additional C&A work will be accomplished by the end of FY 06.

10. Terminate/Upgrade External Connections

VA has done detailed work in this area and has reduced the known gateways to the Internet from over 200 to four. As we move to centralize the operations and maintenance domain, we will be better able to identify unauthorized connections and eliminate them and take vigorous corrective measures when violations of VA's policies are discovered.

11. Configuration Management

VA continues to operate a small number of Windows 95/98 systems for applications that are not compatible with Windows 2000 at the Veterans Benefits Administration (for The Imaging Management System – TIMS). These are expected to be retired or replaced by the end of FY 06. However, more intensive efforts need to take place to upgrade all VA computers to the XP Operating System and to upgrade peripheral devices as necessary. This effort is included in VA's FY 07 budget and completion is targeted for the end of FY 07.

With the Delegation of Authority Memorandum of June 28, 2006, the CIO has the authority to establish and implement policies and procedures to ensure compliance with National Institute of Standards and Technology (NIST) Special Publications 800-53, *Recommended Security Controls for Federal Information Systems* and 800-64, *Security Considerations in the Information System Development Life Cycle* which relate to configuration management and change control. This Delegation of Authority, together with full implementation of the IT organization realignment, will allow the CIO to direct remediation of these deficiencies. The VHA Office of Information has developed a detailed Configuration Management Plan, Change Control Process, and Maintenance Procedures to support the system development life cycle for VistA and local area networks. The CIO is tracking deficiencies for those systems not in compliance with these requirements.

12. Movement and Consolidation of VACO's Data Center

While the majority of VA's servers and other hardware have been moved to various locations in Washington, DC and Maryland, there is still network hardware located in the basement of VACO that supports VACO telecommunications. Steps have been taken to place the VACO data center in a more protected area and further action is underway to move this critical infrastructure. A site in West Virginia is under construction that will house the Metropolitan Area Network for VACO. Completion of this project is expected by December 31, 2006.

Consolidation of other data centers continues. An example of this consolidation is the migration of the White River Junction VA Medical and Regional Office Center VistA to the Regional Data Processing Center (RDPC) in Brooklyn, New York. This type of consolidation to RDPCs will significantly enhance the IT centralization efforts.

13. Application Program/Operating System Change Controls

As a result of the IT Reorganization currently under way, the CIO will mandate procedures regarding applications installed on VA computers and for any device connected to the VA Internet. The IT Tracker System will be used to ensure that equipment to be procured will be properly configured to remedy this condition. The reorganization will allow tighter controls over what gets connected to the VA backbone. In addition, an Enterprise Change Control Board will be established by the end of this calendar year to assist with enforcing standards.

14. Physical Access Controls

Better control over physical access through intrusion detection systems has already been achieved in most locations throughout VA. However, an additional assessment is needed to be sure all sites are in compliance – to include other aspects of physical security such as the conditions regarding proper escorting into secure areas. Information Security Officers who are now under the control of the CIO will have an improved capability to correct these deficiencies. The June 28, 2006, Delegation of Authority memorandum will also significantly enhance the ability of the CIO to ensure that corrective action is taken where proper access controls are not in place.

15. Wireless Security

VA had procured a product to mitigate wireless security weaknesses, but it was not kept current VA-wide. The Office of Cyber and Information Security's Security Operations Center (SOC) is establishing a wireless penetration and assessment program that will identify and assist the field with remediation of wireless security vulnerabilities. With the new IT realignment, the CIO will direct remediation of identified deficiencies in the wireless area, as appropriate.

I agree that a more extensive review of the wireless security environment needs to occur and will be one of the high priority actions for the remainder of FY 06 and expect corrective action in this regard is anticipated to be achieved by the end of FY 07.

16. Encrypting Sensitive Information on VA Networks

Encryption standards have been developed for VA-controlled laptops as directed by OMB. I directed that all VA-controlled laptops be inspected and encrypted during

VA's Security Awareness Week (June 26-30, 2006). However based upon the advice of the Department of Justice attorneys representing VA in the three class action lawsuits filed regarding the data loss, I have delayed the review of the laptops. I have been advised that plaintiffs' counsel has objected to any alteration of existing data on VA-controlled laptops. They allege that any deletion or alteration of the existing data might cause destruction of potential evidence in the lawsuits. We intend to seek review of this issue by the Courts at the earliest opportunity. Other encryption guidance will be established and disseminated by the end of August 2006.

17. FISMA Reporting Database

As indicated in the IG findings, corrective action is already under way in this area and is being further elaborated in response to the most recent FISMA Report.

This database will be updated and made more accurate. This action will be completed by the end of fiscal year 2006.

Combined Assessment Program (CAP) Reviews Show Information System Security Vulnerabilities Continue to Exist

I agree. It is absolutely critical that these security vulnerabilities be addressed. The recently published Directive 6504 described the procedures that must be followed for remote network access and the protection of information while at rest and in transit. The actions required to improve conditions relative to background checks were described in the response to Issue 5. The recently approved Delegation of Authority Memorandum together with the on-going IT realignment will provide a significant improvement for the overall environment within VA regarding information security. We will realize dramatic improvements in all of the areas cited above through the support of an enhanced VA Audit and Inspection capability.

Finding: Policy Changes Implemented by VA Since the Incident Are a Positive Step, but More Needs to be Done to Prevent Similar Incidents

Additional action is required and currently underway. As noted by the Inspector General, a number of actions have already been accomplished such as:

- May 22, 2006 – Secretary's Memorandum to VA employees required all employees to complete Cyber Security and Privacy Awareness training by June 30, 2006 (TAB 8).

- May 24, 2006 – Deputy Secretary Memorandum issuing VA IT Directive 06-1, establishing the Data Security – Assessment and Strengthening of Controls Program (TAB 2).
- May 26, 2006 – Secretary’s Directive Memorandum to all VA managers, supervisors and team leaders to reiterate their responsibility in ensuring information security in their organizations (TAB 9).
- June 7, 2006 Deputy Under Secretary for Health for Operations and Management and Deputy Assistant Secretary for Security and Law Enforcement Memorandum outlining security practices required for electronic fingerprint systems (TAB 10).
- June 5, 2006 – Human Resources and Administration Memorandum required all organizations to identify teleworkers by June 6, 2006 (TAB 11).
- June 6, 2006 – Secretary Memorandum suspended the practice permitting VBA employees to remove claims files from the regular workstations in order to adjudicate claims from an alternative worksite (TAB 12).
- June 6, 2006 – Secretary Memorandum issued VA IT Directive 06-2, which requires supervisory approval before removing confidential and Privacy Act protected information from the worksite in any data format (TAB 13).
- June 7, 2006 – OIT Memorandum directing VA to complete a data access inventory for each employee by June 21, 2006. This inventory has been completed. A special Web page on VA’s Intranet was used to guide the collect this information at: <http://vaww.survey.va.gov/surveys/AB9SEA> (TAB 14)
- June 7, 2006 – Deputy Secretary issued VA Directive 6504, Restrictions on Transmission, Transportation of Use of, and Access to, VA Data Outside VA Facilities (TAB 4).
- June 13, 2006 – VHA Deputy Under Secretary for Health for Operations and Management disseminated checklist requiring VHA senior leadership certification of privacy and security measures (TAB 15).

- June 19, 2006 – Memorandum from Under Secretary for Health to Assistant Secretary for Information and Technology regarding OIG FY 2005 Audit of Information Security Program (*TAB 16*).
- June 20, 2006 – Memorandum from Deputy Under Secretary for Health for Operations and Management guidance related to medical transcription (*TAB 17*).
- June 28, 2006 – Secretary Memorandum – Delegation of Authority for Responsibility for Departmental Information Security. This document delegates to the Assistant Secretary for Information Technology complete responsibility and authority for enforcement of information policies, procedures and practices. The Assistant Secretary for Information Technology is also responsible for all facets of the VA's information security, including budgeting, training, certification and accreditation, incident response and security systems engineering (*TAB 7*).

GLOSSARY OF TERMS

C&A's	Certification and Accreditation
CAP	Combined Assessment Program
CIO	Chief Information Officer
CFS	Consolidated Financial Statements
COOP	Continuity of Operations Plan
e-QIP	Electronics Questionnaires for Investigations Processing
FISMA	Federal Information Security Management Act
HIDS	Host Intrusion Detection System
IT	Information Technology
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
OCIS	Office of Cyber and Information Security
OCIST	Office of Cyber and Information Security Training
OIG	Office of Inspector General
OPF	Official Personnel Folder
OPM	Office of Personnel and Management
PAID	Personnel and Accounting Integrated Data
PC	Personal Computer
PKI	Public Key Infrastructure
SIC	Security Investigations Center
SOC	Security Operations Center
TIMS	The Imaging Management System
TOPIC	Transmission of Privacy Information in Clear Text
VA	Department of Veterans Affairs
VA-CIRC	VA Central Incident Response Capability
VACO	Veterans Affairs Central Office
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VPN	Virtual Private Network

ATTACHMENT INDEX

TAB 1	Administrative Investigation Charge Memoranda
TAB 2	May 24, 2006 – Memorandum issued VA IT Directive 06-1, establishing the Data Security – Assessment and Strengthening of Controls Program.
TAB 3	Timeline
TAB 4	June 7, 2006 – VA Directive 6504, Restrictions on Transmission, Transportation of Use of, and Access to, VA Data Outside VA Facilities
TAB 5	Statement of Commitment to be signed by VA employees by July 21, 2006
TAB 6	June 28, 2006 – Delegation of Authority for Responsibility for Departmental Information Security which provides the CIO the enforcement authority previously cited as lacking by the IG.
TAB 7	Organizational Chart
TAB 8	May 22, 2006 – Memorandum to all VA employees required all employees To complete Cyber Security and Privacy Awareness training by June 30, 2006.
TAB 9	May 26, 2006 – Directive Memorandum to all VA managers, supervisors and team leaders to reiterate their responsibility in ensuring information security in their organizations.
TAB 10	June 7, 2006 – Deputy Under Secretary for Health for Operations and Management and Deputy Assistant Secretary for Security and Law Enforcement Memorandum outlining security practices required for electronic fingerprint systems
TAB 11	June 5, 2006 – Memorandum required all organizations to identify teleworkers by June 6, 2006.

- TAB 12 June 6, 2006 – Memorandum suspended the practice permitting VBA employees to remove claims files from the regular workstations in order to adjudicate claims from an alternative worksite.
- TAB 13 June 6, 2006 – Memorandum issued VA IT Directive 06-2, which requires supervisory approval before removing confidential and Privacy Act protected information from the worksite in any data format.
- TAB 14 June 7, 2006 – OIT Memorandum directing to complete a data access inventory for each employee by June 21, 2006. This inventory has been completed. A special web page on VA’s Intranet was used to guide the collect this information at: <http://vaww.survey.va.gov/surveys/AB9SEA> (TAB 16)
- TAB 15 June 13, 2006 – VHA Deputy Under Secretary for Health for Operations and Management disseminated checklist requiring VHA senior leadership certification of privacy and security measures.
- TAB 16 June 19, 2006 – Memorandum from Under Secretary for Health to Assistant Secretary for Information and Technology regarding OIG FY 2005 Audit of Information Security Program
- TAB 17 June 20, 2006 – Memorandum from Deputy Under Secretary for Health for Operations and Management guidance related to medical transcription.

Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Quality of Life and Veterans Affairs,
and Related Agencies
House Committee on Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction and Veterans' Affairs,
and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG's Web site at <http://www.va.gov/oig/52/reports/mainlist.htm>. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.

Additional supporting material provided by the Department of Veterans Affairs may be requested by writing to:

Department of Veterans Affairs
Office of Inspector General
FOIA/Privacy Act Section (53B)
810 Vermont Avenue, NW
Washington, DC 20420