STATEMENT OF
GEORGE J. OPFER
INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE
THE COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES SENATE

July 20, 2006

INTRODUCTION

Mr. Chairman and members of the Committee, thank you for the opportunity to testify today on the results of the Office of Inspector General (OIG), Department of Veterans Affairs (VA), review of issues related to the loss of VA information involving the identity of millions of veterans. I am accompanied by Jon Wooditch, Deputy Inspector General, and Maureen Regan, Counselor to Inspector General.

As you know, 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 U.S. 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 notified on May 22, 2006. Since then, the Senate Veterans' Affairs Committee, as well as other congressional committees and members of Congress, have expressed considerable interest in how this incident occurred and in how VA management responded after being notified of the loss of data.

When I testified before this committee on May 25, 2006, I described the OIG's involvement as a three-pronged approach including: (1) a criminal investigation, (2) an administrative investigation of the handling of the incident once reported to VA, and (3) a review of VA policies and procedures for using and safeguarding personal and proprietary data. I am pleased to announce that we completed the administrative investigation and the review of policies and procedures, and issued our final report on July 11, 2006.

More importantly, I am also pleased to acknowledge that through the diligent and coordinated efforts of the VA OIG, the Federal Bureau of Investigation, and the Montgomery County Police Department in Maryland, the stolen data was successfully recovered on June 28, 2006. Based on all the facts gathered thus far during the criminal investigation, as well as the results of computer forensics examinations, we are highly confident that the data was not compromised after the burglary. I would also like to point out that we are continuing to pursue the criminal investigation into the burglary.

The July 11, 2006, report essentially addresses whether the employee had authorization to access and take the data home, whether management responded appropriately to the incident, and whether VA policies and procedures were adequate to protect information. The report also discusses long-standing information security weaknesses in VA, even though OIG reports have repeatedly made recommendations for corrective action.

EMPLOYEE NOT AUTHORIZED TO TAKE 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 that contained records on approximately 26 million living veterans. The extract contained veterans' social security numbers, names, birth dates, service numbers, and combined degree of disability. He also reported that the stolen hard drive likely contained an extract of the Compensation and Pension 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. By storing the files on his personal external hard drive and leaving it unattended, the employee failed to properly safeguard the data. 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 proposed administrative action prior to issuance of our report.

MANAGEMENT RESPONSE TO THE INCIDENT WAS NOT APPROPRIATE OR TIMELY

The burglary was reported to the local police on May 3, 2006. 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 (OPP&P), including Security and Law Enforcement personnel, that the stolen computer equipment contained VA data.

Mr. Michael McLendon, Deputy Assistant Secretary for Policy, was one of the managers notified on May 3, 2006. However, 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 that the ISO decided not to discuss the matter; rather he asked the employee to write down what data was lost. The employee's written account of the lost data was an identification of database extracts with little quantified information concerning the significance or magnitude of the incident. This is important because this report 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 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 with the programming expert on his staff or with the employee who reported the stolen data. Mr. Duffy provided the revised 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 also 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 this 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 data.

Shortly after Mr. Bowman received the report from Mr. Duffy on May 10, 2006, he provided it to Mr. Jack Thompson, Deputy General Counsel, and asked him to provide legal advice on the agency's duties and responsibilities to notify individuals whose identifying information was compromised. On May 10, 2006, Mr. Bowman also informed Mr. Gordon Mansfield, Deputy Secretary. 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 attempt was made to contact the employee who reported the theft to determine the magnitude of the stolen data.

The OIG was able to determine the extent of the stolen data after one interview with the employee on May 15, 2006. As soon as I learned of the magnitude of the incident on the morning of May 16, 2006, I immediately notified the Chief of Staff that the stolen data most likely contained personal identifiers on approximately 26 million records. The Chief of Staff then notified the Secretary.

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 its importance, but no one clearly identified it as a high priority item and no one followed up on the status of the request until after I notified the Chief of Staff on May 16, 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 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), 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 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 (PO).

POLICIES AND PROCEDURES DID NOT ADEQUATELY SAFEGUARD PROTECTED INFORMATION

The potential disclosure of Privacy Act protected information resulting from the theft 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, POs, 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 mandatory 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 HAVE PERSISTED FOR YEARS

For the past several years, we have reported vulnerabilities with information technology security controls in our Consolidated Financial Statements (CFS) audit reports, Federal Information Security Management Act (FISMA) audit reports, and Combined Assessment Program (CAP) 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 the effectiveness of 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.

CONCLUSION

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 his supervisors were not aware of the employee's self-initiated project and, as such, had no official need or permission to take the data home. In addition, the employee reported that the data stored on the stolen external hard drive was neither password-protected nor encrypted.

Although senior managers and other OPP&P staff were informed of the possible loss of data on May 3, 2006, the incident was not communicated up the chain-of-command until the VA Chief of Staff was notified 6 days later. Poor communication, partially resulting from a dysfunctional working relationship among senior OPP&P executives, contributed to the delay. While there was considerable rhetoric among management concerning the need to identify the extent and scope of the stolen data, there was virtually no follow-up with the employee 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.

On May 10, 2006, Mr. Bowman requested legal advice from OGC. Yet, during the 6 days following this request, Mr. Bowman did not follow up to determine the status of the request, or task anyone to develop a more definitive description of how many veterans' records may have been stolen. Although Mr. Bowman acknowledged he knew the data stolen could potentially affect millions of veterans, he demonstrated no urgency in notifying the Secretary of the incident and decided to wait for OGC's response before doing so.

Mr. Bowman also notified Mr. Mansfield on May 10, 2006, 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.

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. Efforts to investigate the incident were further impeded by errors and omissions in the ISO's incident report and were delayed due to ineffective coordination between the OPP&P ISO and the SOC. 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 OIG was able to determine the magnitude and extent of the stolen data after one interview with the employee on May 15, 2006, and I notified the Chief of Staff on the morning of May 16, 2006. The Chief of Staff notified the Secretary shortly after my call. It is unexplainable why no one in the management chain-of-command ever attempted to re-interview the employee to gain a better understanding of the scope and severity of the potential data loss, prior to my call.

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 properly safeguarded. 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.

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 VA managers have attempted to strengthen policies, procedures, and controls to prevent similar disclosures, but additional actions need to be taken to safeguard protected information and VA's automated systems.

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 our July 11, 2006, report because 17 recommendations are listed in previously issued OIG reports and are being followed up on separately.

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.

The Secretary agreed with the findings and recommendations in our report and provided acceptable improvement plans.

CLOSING

In closing, I would like to assure the Committee that we will follow up on the implementation of these recommendations until they are completed. Mr. Chairman and other distinguished members of the Committee, thank you again for this opportunity and I would be pleased to answer any questions.