STATEMENT OF GEORGE J. OPFER, INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS: accompanied by Jon A. Wooditch, Deputy Inspector General, Department of Veterans Affairs

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

MAY 25, 2006

INTRODUCTION

Mr. Chairman, Madam Chairman, and Members of the Committees, thank you for the opportunity to testify today on the loss of Department of Veterans Affairs (VA) sensitive data. I am accompanied by Jon Wooditch, Deputy Inspector General, and Mike Staley, Assistant Inspector General for Auditing. My statement will focus on the incident involving a VA employee who took home sensitive and confidential information, which was stolen when the employee's home was burglarized. The Office of Inspector General's (OIG) involvement in this matter involves a three-pronged approach including (1) a criminal investigation, (2) an administrative investigation of the handling of this matter once reported to the Department, and (3) a review of VA policies and procedures for using and protecting privacy data. In addition to discussing each of these reviews, I will also provide an overview of the OIG reports that have shown the need for continued improvements in addressing information security weaknesses in VA, and the status of OIG recommendations for corrective action.

On May 3, 2006, the home of a VA employee was burglarized. According to the employee, the information stolen included the names, birthdates, and social security numbers of approximately 26.5 million veterans that was stored on personally-owned computer hardware. The employee, a data analyst, was authorized access to sensitive VA information in the performance of his duties and responsibilities. He said that he routinely took such data home to work on it, and had been doing so since 2003.

CRIMINAL INVESTIGATION

On Wednesday, May 10, 2006, our Information Security Officer (ISO), while attending a routine meeting at VA Central Office, heard another ISO mention that a VA employee's home had been burglarized and that VA electronic records may have been stolen. Following the meeting, our ISO gathered additional facts about this incident. On the following day, he submitted a written report to his supervisor for the purpose of alerting our Office of Investigations. On May 12,

2006, a criminal investigation was initiated and efforts commenced to identify and interview the employee.

On Monday, May 15, 2006, we interviewed the employee. The employee advised us that he believed that several electronic files containing veteran information stored on personally-owned computer hardware had been stolen during the burglary at his home on May 3, 2006. He thought the stolen information included the names, birthdates, and social security numbers of approximately 26.5 million veterans.

On May 16, 2006, we met with the Montgomery County Police Department who had initiated an investigation of the burglary when notified on May 3, 2006. We informed them of the suspected loss of millions of veterans' personal identifiers. We learned that detectives were actively pursuing leads developed in a number of recent residential burglaries in the employee's neighborhood.

On May 17, 2006, we apprised the Federal Bureau of Investigation (FBI) and an Assistant United States Attorney of the details of this burglary and possible loss of data. The next day, we also faxed a letter listing these details to the FBI. Since then, we have been conducting a joint investigation with the FBI and the Montgomery County Police Department focused on the recovery of the stolen data. To date, there has been no indication that this data has been further compromised.

ADMINISTRATIVE INVESTIGATION

We have also initiated an administrative investigation to determine if notifications of the incident were made, and if those notifications were pursued in an appropriate and timely manner. We are developing a chronology of when key staff and managers were informed of the incident, what information was conveyed to these individuals, and what actions they took. We are also identifying what VA electronic data the employee stored at his home, whether the employee had an official need for the data, why he took it to his home, and who in his supervisory chain approved or had knowledge that he had done so.

We have interviewed the employee, his supervisors, project managers, and co-workers; privacy, information security, and VA law enforcement officials; Office of General Counsel attorneys, including the General Counsel; and the VA Chief of Staff. We are also reviewing electronic mail messages pertinent to the incident; notes and memoranda prepared by the employee, General Counsel, and other staff; documentation of the employee's access to VA databases; and other pertinent documentation.

According to the employee, he likely had VA electronic data stolen during the burglary of his residence, but he was not certain of the type and extent of the specific information taken. He said he believed it contained approximately 26.5 million veterans' names, social security numbers, and dates of birth, extracted from a VA database, and possibly other smaller files containing information about individual veterans was also taken. We are currently reviewing the computer discs he used to take data home to determine what other information may have been stolen.

The employee, a data analyst, had an official need to access the records believed to have been stolen. The nature of his work was project-focused and involved manipulating large quantities of data to address certain policy issues. The employee told us he took the data home for work-related purposes. However, none of his supervisors we talked to said they were aware that the employee had taken the file containing approximately 26.5 million veterans' records to his residence.

As part of our investigation, we will determine if the work the employee was performing at home was related to his official duties, and if he had appropriate authorization to take individually-identifiable data to his residence. We will also determine if the employee complied with relevant policies and procedures in taking this information home and properly protecting it. Our report will identify what breakdowns occurred that may have hindered timely notification and follow-up of this incident. Based on our investigation, we will make recommendations for appropriate action, if warranted.

REVIEW OF LAWS, REGULATIONS, AND VA POLICIES AND PROCEDURES ON SAFEGUARDING CONFIDENTIAL INFORMATION

The recent incident raised concerns about whether the VA has adequate policies and procedures in place to protect confidential and privileged information maintained in VA's electronic databases. Our concerns are whether VA policies are adequate to ensure compliance with information security laws, the Privacy Act and other confidentiality laws and regulations, and to identify and take action when there is a violation of law or policy. There are two sets of laws and implementing regulations to protect the integrity of confidential data ? computer security laws and confidentiality statutes. While the intent of both sets of laws is the same ? the protection of information ? the approach is different. Computer security laws ensure that the system infrastructure on which the data is maintained electronically is protected against unauthorized intrusions such as viruses and unapproved access. The Privacy Act and other confidentiality laws and regulations protect information by limiting access, use, and disclosure of records without authorization from the individual about whom the record is maintained.

To address the issues, we initiated a review to determine whether VA has effective policies in place to ensure compliance with computer security laws, the Privacy Act and other confidentiality laws and regulations, whether VA employees are aware of the policies; whether VA has adequate procedures in place to monitor compliance with the policies; and, whether the policies include an effective mechanism for reporting violations and taking appropriate action. Two areas that we are addressing in our review are policies relating to the transfer of electronic information from an employee's VA computer to his home or alternative work site and the impact centralization versus decentralization of VA policy has on ensuring that the integrity of VA computer systems and the information stored on those systems is maintained.

The review includes identifying and reviewing applicable laws, regulations and policies, including Department-wide policies; policies issues by the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and other VA entities, policies issued by local VA facilities; and mandatory training modules. We are also reviewing how policies are disseminated to VA employees; whether VA employees are aware of the policies, and whether

VA procedures for identifying, reporting and taking action when data has been improperly accessed or improperly used are adequate.

This review will identify strengths and weaknesses in VA's policies implementing the provisions of computer security laws and the Privacy Act, and other confidentiality laws. We will also identify strengths and weaknesses in ensuring that VA employees are knowledgeable regarding their obligation to protect VA computer systems and information and that they will be held accountable for violations. We will make recommendations for improvement to ensure that data maintained by VA is protected from unwarranted intrusion and disclosure.

SUMMARY OF OIG REPORTS ADDRESSING INFORMATION SECURITY WEAKNESSES

We have conducted a number of audits and evaluations on information management security and information technology (IT) systems that have shown the need for continued improvements in addressing security weaknesses. My office has reported VA information security controls as a material weakness in its annual Consolidated Financial Statement (CFS) audits since before fiscal year (FY) 2001. Our Federal Information Security Management Act (FISMA) reviews have identified significant information security vulnerabilities since FY 2001 that place VA at risk of denial of service attacks, disruption of mission-critical systems, and unauthorized access to sensitive data. We continue to report security weaknesses and vulnerabilities at VA health care facilities and VA regional offices where security issues were evaluated during our Combined Assessment Program (CAP) reviews.

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

Pursuant to the Chief Financial Officers Act of 1990, the VA consolidated financial statements are audited annually. We contract with an independent public accounting firm to perform this audit. As part of the audit, the contractor follows Government Accountability Office methodology to assess the effectiveness of computer controls. The contractor conducts audits at VA's three information technology centers and selected regional offices and medical centers.

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 of VA systems 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 problems related to VA's control and oversight of access to its information systems. By not controlling and monitoring employee access, not restricting users to only need-to-know data, and not timely terminating accounts upon employee departure, VA has not prevented potential risk. These weaknesses placed sensitive information, including financial data and sensitive veteran medical and benefit information, at risk, possibly without detection of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As a result of these weaknesses, we made recommendations 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. We also recommended that VA 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. Finally, we recommended that VA conform access privileges to the user's level of responsibility and position.

VA has implemented some recommendations for specific locations identified but has not proactively 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.

Evaluations of VA's Information Security Program Have Identified Serious Vulnerabilities for Several Years that Remain Uncorrected

FISMA requires us to annually review the progress of the information technology and security program of the Department and report the results to the Office of Management and Budget. As part of the FISMA review, we conduct scanning and penetration tests of selected VA systems to assess controls for monitoring and accessing systems, and reviews of physical, personnel, and electronic security. We visit all three major IT centers and selected VHA and VBA sites.

In all four audits of the VA Security Program issued since 2001, we reported serious vulnerabilities that remain uncorrected. 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, wireless security, personnel security, and FISMA reporting. Additionally, we have reported significant issues with implementation of security initiatives VA-wide. The status of unimplemented recommendations was discussed in subsequent audits.

The FY 2004 audit once again emphasized the need to centralize the IT security program, implement security initiatives, and close security vulnerabilities. We recognized that the CIO's 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 held the CIO lacked the authority to enforce compliance with the VA information security program as one reason he could not address vulnerabilities. We again recommended that VA fully implement and fund a centralized VA-wide IT security program.

In total, the FY 2004 report included 16 recommendations: (1) centralize IT security programs; (2) implement an effective patch management program; (3) address security vulnerabilities of unauthorized access and misuse of sensitive information and data throughout VA demonstrated during OIG field testing; (4) ensure position descriptions contain proper data access classification; (5) obtain timely, complete background investigations; and complete the following security initiatives on (6) intrusion detection systems, (7) infrastructure protection actions, (8) data center contingency planning, (9) certification and accreditation of systems, (10) upgrading/ terminating external connections, (11) improvement of configuration management, (12) moving

VACO data center, (13) improvement of application program/operating system change controls, (14) limiting physical access to computer rooms, (15) wireless devices, and (16) electronic transmission of sensitive veteran data. As of May 23, 2006, all recommendations from this report remain open.

Finally, in FY 2006, after Congress mandated full centralization of IT security under the CIO, as we advocated in our reports since 2001, VA is now moving out on a truly empowered centralized CIO. We have provided our draft FY 2005 audit report to the Department and are working with the Department to resolve all outstanding recommendations. We have grouped our recommendations into two categories?the CIO's authority under centralization and longstanding vulnerabilities. With a centralized CIO with direct line authority to implement the needed fixes, we believe VA has a unique opportunity to successfully address all the vulnerabilities and weaknesses discussed in our reports since 2001.

We believe centralization is essential because standardization is the key to fixing VA information security weaknesses. As long as three stove-piped administrations and other smaller component organizations are free to operate in the IT environment on their own within VA?accountable not to the CIO but to other line managers who themselves are not accountable to the VA CIO?the vulnerabilities cannot be effectively resolved.

CAP Reviews Continue to Show Information System Security Vulnerabilities Continue to Exist

We continue to identify instances where out-based employees send veteran 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. Consequently, we continue to find these systemic conditions at other sites we visit. For example, between FYs 2000 to 2005 the CAP program identified IT and security deficiencies in 141 of 181 VHA facilities. We identified IT and security deficiencies at 37 of 55 VBA facilities.

CLOSING

In closing, I would like to assure the Committee that this matter will remain a very high priority for the OIG until it is resolved. I will ensure that all the resources that are needed to complete our reviews in a thorough and timely manner will remain dedicated to the goal of recovering the stolen data and protecting our Nation's veterans.

Mr. Chairman, Madam Chairman, and Members of the Committees, thank you again for this opportunity and I would be pleased to answer any questions that you may have.