



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

September 5, 2006



Commemorating 75 Years of Service

The Honorable Tom Davis
Chairman
Committee on Government Reform
U. S. House of Representatives
Washington, DC 25015

Dear Mr. Chairman:

This is in response to your July 10, 2006, letter written in your capacity as Chair of the Committee on Government Reform. You asked the Department of Veterans Affairs (VA) for specific information about incidents that have occurred since January 1, 2003, in which the security and confidentiality of VA individually-identified information was possibly compromised. You also requested information about incidents other than the May 3, 2006, theft of a hard drive containing veterans' personal information from an employee's home.

Enclosed is the information that we have been able to identify as responsive to your request. However, we present the information in the form of two reports for the following reason. Since the May 3, 2006, theft of the hard drive containing veterans' personal information, VA has established a single daily incident report process for reporting potential breaches in the security and privacy of VA's sensitive personal information. Prior to establishing the single reporting process, VA had two incident reporting processes: one for security incidents and one for privacy incidents. Consequently, in order to provide the information that you requested, we enclose two lists; one maintained by the Office of Information & Technology Field Security Operations for security incidents, and one maintained by the Office of E-Government's Privacy Service for privacy incidents. We believe that the two lists contain the information that you requested.

Please note the enclosures contain individually-identified personal information which is protected by the Privacy Act, 5 U.S.C. § 552a. This statute generally limits the Department's ability to publicly disclose the information in an individually-identifiable form. While this information is not protected by the Privacy Act once under the Committee's jurisdiction, it is considered to be of a sensitive nature. You may wish to consider this fact in any decision whether to re-disclose this information. In order to protect the personal privacy of individuals who may be identified from the records provided to the Committee, the Committee may wish to delete any identifying personal information before re-disclosing these records. If the Committee wishes, the Department would be pleased to assist by providing suitably redacted copies for public release.

Page 2


The Honorable Tom Davis

We also provide the following information which may be helpful in the Committee's review of this subject. In accordance with the recent Office of Management and Budget Memorandum M-06-19, dated July 12, 2006, VA now reports all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. In addition, we have taken several other steps to improve the security of VA's individually-identified information. VA has:

- Developed a standard template for reporting security incidents to senior management.
- Expedited completion of cyber security and privacy awareness training for all VA employees.
- Completed an inventory of all positions requiring access to sensitive VA data.
- Directed that sensitive information removed from VA sites or accessed at locations remote from VA sites be encrypted.
- Directed that employees taking or accessing information off site obtain the prior approval of their supervisor and their Information Security Officer.
- Conducted VA-wide Security Awareness Week activities during the last week of June to heighten awareness of security procedures.

VA's mission to serve and honor the Nation's veterans is one that I take very seriously, and we are working diligently to protect veterans and their families from any harm associated with this incident. A similar reply has been sent to Congressman Waxman who co-signed your letter.

Sincerely yours, .



R. James Nicholson

Enclosures



SOCIAL SECURITY

The Commissioner

August 3, 2006

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I received your letter requesting that we provide you with details about incidents involving the loss or compromise of any sensitive personal information held by the Social Security Administration (SSA) or any of our contractors that occurred since January 1, 2003.

I want to take this opportunity to assure you that SSA has always recognized the importance of protecting the privacy of the people we serve. Safeguarding personally identifiable information about individuals is a top priority for all of us at SSA. Our commitment to safeguard and protect personal information began in 1937 as Regulation No. 1 of the Social Security Board and those initial policies were updated in 1939 under the Social Security Act. In addition, our policies and procedures follow the Privacy Act, the Federal Information Security Management Act (FISMA) and other relevant federal laws, regulations and guidance.

While these policies take into account the unavoidable fact that the best systems are subject to human error, and are designed to keep the risk of any breach to an absolute minimum, we continually strive to improve our policies and processes. I have directed my staff to conduct a comprehensive review of our security policies and procedures to identify and immediately address any gaps in assuring the protection of personal information.

I have attached a fact sheet containing the information you requested and I hope this information is helpful to you. I am sending an identical letter to Mr. Waxman. If you have additional questions, please do not hesitate to get in touch with me or have your staff contact Robert M. Wilson, Deputy Commissioner for Legislative and Congressional Affairs at 202-358-6030.

Sincerely,

Jo Anne B. Barnhart

Enclosure



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

The Director

August 3, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Mr. Chairman:

This letter responds to your inquiry of July 10, 2006, requesting information on the Office of Personnel Management's (OPM) data breaches since January 1, 2003. Enclosed is our report. An identical report was provided to Congressman Henry Waxman.

OPM has had a limited number of incidents involving unauthorized access to data, and all were resolved quickly and responsibly. We have provided information on three confirmed incidents that have occurred since January 2003, two of which occurred over 2 years ago.

OPM's Federal Investigative Services Division employs several thousand investigators who conduct hundreds of thousands of background investigations annually. During the course of their daily work, they have access to and carry personally identifiable information (PII) and other sensitive information on subjects of investigation and related sources of information. When identified, we record, review, and follow up on suspected breaches of PII. These include occurrences when our investigators inappropriately lose possession of the case papers or their investigative notes after conducting interviews. Recovery efforts of the potentially breached material are conducted. In total, OPM investigators have conducted over 1.87 million investigations requiring personal interviews or record searches in the field since January 1, 2003. During that time, there were 129 documented instances of mishandled investigative documents, for an incident rate of less than .007%.

I would also like to point out the following:

- No breaches have involved a large volume of sensitive data.
- There have been no reported impacts on any person.

OPM is continuously strengthening its IT security policies and procedures, and is aware of the serious responsibility we all have to protect sensitive PII. OPM has taken steps to reinforce the significance of privacy issues and handling PII data, publicizing the criticality of security, and strengthening the Agency's focus on security concerns such as incident handling procedures and IT security awareness. We will continue to ensure all OPM staff and contractors are regularly reminded of their security and data handling responsibilities.

Sincerely,



Linda M. Springer
Director

Enclosure