Statement of the Honorable R. James Nicholson
Secretary of Veterans Affairs
Before the
Senate Committee on Veterans' Affairs
And
Committee on Homeland Security and Governmental Affairs

May 25, 2006
*

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to appear before you today to explain a devastating situation.

A VA employee, a data analyst, took home electronic data files from VA. He was not authorized to do so.

These data contained identifying information including names and dates of birth for up to 26.5 million veterans and some of their spouses. In addition, that information, plus social security numbers, was available for some 19.6 million of those veterans. Also possibly included were some numerical disability ratings and the diagnostic codes which identify the disabilities being compensated.

It is important to note that the data did not include any of VA's electronic health records. Neither did it contain explicit financial information, although knowing of a disability rating could enable one to compute what that implied in terms of compensation payments.

On May 3, the employee's home was broken into in what appears to local law enforcement to have been a routine breaking and entering, and the VA data were stolen. The employee has been placed on administrative leave pending the outcome of an investigation with which I understand he is cooperating.

I am outraged at the loss of this veterans' data and the fact an employee would put it at risk by taking it home in violation of VA policies. However, the employee promptly reported the theft to the local police and to the Department of Veterans Affairs. But it was not until May 16th that I was notified. I am gravely concerned about the timing of the Department's response once the burglary became known. I will not tolerate inaction and poor judgment when it comes to protecting our veterans.

Appropriate law enforcement agencies, including local police, the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items stolen because of any knowledge of the data contents. It is possible that the thieves remain unaware of the information they possess or of how to make use of it. Because of that, we have attempted to describe the equipment stolen, the location from which it was stolen and other information in very general terms. We do not want to provide information to the thieves that might be informative as to the nature of what they have stolen. We still hope that this was a common theft, and that no use will be made of the VA data.

From the moment I was informed, VA began taking all possible steps to protect and inform our veterans.

In our post-disclosure assessment, we have seen the gaps between what we said and the way we are seen.

VA has begun a top to bottom examination of our business, policies, and procedures to find out how we can prevent something like this from happening again. We will stay focused on the problems until they are fixed. In addition, we will take direct and immediate action to address and alleviate veterans' concerns and to regain their confidence.

I have taken the following actions so far:

- I have directed all VA employees to complete the annual "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by June 30, 2006.

- This includes:

    - The Privacy Act;

    - Unauthorized disclosing or using, directly or indirectly, information obtained as a result of employment in VA, which is of a confidential nature or which represents a matter of trust, or other information so obtained of such a character that its disclosure or use would be contrary to the best interests of the VA or veterans being served by it; and,

    - Loss of, damage to, or unauthorized use of Government property, through carelessness or negligence, or through maliciousness or intent.

- I have also directed that all VA employees sign annually an Employee Statement of Commitment and Understanding which will also acknowledge consequences for non compliance.

In addition the Department will immediately begin to conduct an inventory and review of all current positions requiring access to sensitive VA data. The inventory will determine whether positions in fact require such access. We will then require all employees who need access to sensitive VA data to do their jobs to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required and the responsibilities associated with their position.

And I have directed the Office of Information & Technology to publish, as a VA Directive, the revisions to the Security Guidelines for Single-User Remote Access developed by the Office of Cyber and Information Security. I have asked that this be done by June 30, 2006. This document will set the standards for access, use, and information security, including physical security, incident reporting and responsibilities.

VA is working with members of Congress, the news media, veterans' service organizations, and numerous government agencies to help ensure that those veterans and their families are aware of the situation and of the steps they may take to protect themselves from misuse of personal information.

VA is coordinating with other agencies to send individual notifications to those individuals whose social security numbers were stolen, instructing them to be vigilant in order to detect any signs of possible identity theft and telling them how to protect themselves. In the meantime, veterans can also go to www.firstgov.gov for more information in this matter. This is a federal government website capable of handling large amounts of web traffic.

Additionally, working with other government agencies, VA has set up a manned call center that veterans may use to get information about this situation and learn more about consumer-identity protections. That toll free number is 1-800-FED INFO (333-4636). The call center is operating from 8:00 am to 9:00 pm (EDT), Monday-Saturday as long as it is needed. The call center is able to handle up to 20,000 calls per hour (260,000 calls per day). Through the end of the day on Tuesday, concerned veterans had made a total of 105,753 calls to this number.

I want to acknowledge the significant efforts of numerous government agencies in assisting VA to prepare for our announcement on May 22nd.

Agencies at all levels of the federal government pitched in to ensure that our veterans had information on actions they could take to protect their credit. Hundreds of people worked around the clock writing materials to inform the veterans and setting up call centers and a website to ensure maximum dissemination of the information. I want to personally thank each of those agencies and those individuals for their selfless efforts on behalf of our veterans.

The three nationwide credit bureaus have established special procedures to handle inquiries and requests for fraud alerts from veterans.

Experian and TransUnion have placed a front-end message on their existing toll-free fraud lines, bypassing the usual phone tree, with instructions for placing a fraud alert. Equifax has set up a new toll-free number for veterans to place fraud alerts. The new Equifax number is 1-877-576-5734. The new procedures became operational on Tuesday. The bureaus report a spike in phone calls (171% of normal) and in requests for free credit reports through the annual free credit report web site (annualcreditreport.com). The Federal Trade Commission also experienced high call volumes about the incident earlier this week.

On Monday, the Office of Comptroller of the Currency notified its examiners of the theft. On Tuesday, OCC posted an advisory on an internal network available to its banks and instructed the examiners to direct their banks to the advisory. It explains what happened and asks the banks to exercise extra diligence in processing veterans' payments. The advisory also reminds the banks of their legal obligations to verify the identities of persons seeking to open new accounts and to safeguard customer information against unauthorized access or use. It also includes a summary of relevant laws and regulations.

I briefed the Attorney General and the Chairman of the Federal Trade Commission, co-chairs of the President's Identity Theft Task Force, shortly after I became aware of this occurrence.

Task Force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report they are entitled to under the law. Additionally, the Task Force met on Monday to coordinate the comprehensive Federal response, recommend further ways to protect affected veterans, and increase safeguards to prevent the recurrence of such incidents.

On Monday, following the announcement of this incident, I also issued a memorandum to all VA employees. The purpose was to remind them of the public trust we hold and to set forth the requirement that all employees

complete their annual General Privacy Training and VA Cyber Security Awareness training for the current year by June 30.

As technology has advanced, it has become possible to store vast quantities of data on devices no larger than one's thumb. All of us carry a cell phone, a BlackBerry or a Personal Digital Assistant, and each of these contains vast quantities of data. Someone intent on taking such data and using it inappropriately would have many opportunities to do that.

I can promise you that we will do everything in our power to make clear what is appropriate and inappropriate use of data by our employees. We will train employees in those policies, and we will enforce them. We have already begun discussions regarding the immediate automatic encryption of all sensitive information.

We will also work with the President's Task Force on Identity Theft, of which I am a member, to help structure policies that will be put in place throughout the government to ensure that situations such as this do not occur at other agencies.

VA's mission to serve and honor our nation's veterans is one we take very seriously and the 235,000 VA employees are deeply saddened by any concern or anxiety this incident may cause to those veterans and their families. We honor the service our veterans have given their country and we are working diligently to protect them from any harm as a result of this incident.

Department of Veterans Affairs

Office of Public Affairs
Media Relations

Washington, DC 20420
(202) 273-6000
www.va.gov

Statement

FOR IMMEDIATE RELEASE
May 22, 2006

A Statement from the Department of Veterans Affairs

The Department of Veterans Affairs (VA) has recently learned that an employee, a data analyst, took home electronic data from VA, which he was not authorized to do. This behavior was in violation of our policies. This data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. Importantly, the affected data did not include any of VA's electronic health records nor any financial information. The employee's home was burglarized and this data was stolen. The employee has been placed on administrative leave pending the outcome of an investigation.

Appropriate law enforcement agencies, including the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items because of any knowledge of the data contents. It is possible that they remain unaware of the information which they possess or of how to make use of it. However, out of an abundance of caution, VA is taking all possible steps to protect and inform our veterans.

VA is working with members of Congress, the news media, veterans service organizations, and other government agencies to help ensure that those veterans and their families are aware of the situation and of the steps they may take to protect themselves from misuse of their personal information. VA will send out individual notification letters to veterans to every extent possible. Veterans can also go to www.firstgov.gov to get more information on this matter. This website is being set to

Statement from the Department of Veterans Affairs // 2

handle increased web traffic. Additionally, working with other government agencies, VA has set up a manned call center that veterans may call to get information about this situation and learn more about consumer identity protections. That toll free number is 1-800-FED INFO (333-4636). The call center will be open beginning today, and will operate from 8 am to 9 pm (EDT), Monday-Saturday as long as it is needed. The call center will be able to handle up to 20,000 calls per hour (260,000 calls per day).

Secretary of Veterans Affairs R. James Nicholson has briefed the Attorney General and the Chairman of the Federal Trade Commission, co-chairs of the President's Identity Theft Task Force. Task Force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report they are entitled to under the law. Additionally, the Task Force will meet today to coordinate the comprehensive Federal response, recommend further ways to protect affected veterans, and increase safeguards to prevent the reoccurrence of such incidents. VA's mission to serve and honor our nation's veterans is one we take very seriously and the 235,000 VA employees are deeply saddened by any concern or anxiety this incident may cause our veterans and their families. We appreciate the service our veterans have given their country and we are working diligently to protect them from any harm as a result of this incident.

# # #

VA's Notification to Veterans

Dear Veteran:

The Department of Veterans Affairs (VA) has recently learned that an employee took home electronic data from VA, which he was not authorized to do and was in violation of established policies. The employee's home was burglarized and this data was stolen. The data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. As a result of this incident, information identifiable with you was potentially exposed to others. It is important to note that the affected data did not include any of VA's electronic health records or any financial information.

Appropriate law enforcement agencies, including the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items because of any knowledge of the data contents. It is possible that they remain unaware of the information which they possess or of how to make use of it.

Out of an abundance of caution, however, VA is taking all possible steps to protect and inform our veterans. While you do not need to take any action unless you are aware of suspicious activity regarding your personal information, there are many steps you may take to protect against possible identity theft and we wanted you to be aware of these. Specific information is included in the attached question and answer sheet. For additional information, VA has teamed up the Federal Trade Commission and has a website (www.firstgov.gov) with information on this matter or you may call 1-800-FED-INFO (1-800-333-4636). The call center will operate from 8 a.m. to 9 p.m. (EDT), Monday-Saturday, as long as it is needed.

We apologize for any inconvenience or concern this situation may cause, but we at VA believe it is important for you to be fully informed of any potential risk resulting from this incident. Again, we want to reassure you we have no evidence that your protected data has been misused. We will keep you apprised of any further developments. The men and women of VA take our obligation to honor and serve America's veterans very seriously and we are committed to seeing this never happens again. Sincerely, R. James Nicholson Secretary of Veterans Affairs

Sincerely,
R. James Nicholson
Secretary of Veterans Affairs

Department of Veterans Affairs

Office of Public Affairs
Media Relations

Washington, DC 20420
(202) 273-6000
www.va.gov

F A Qs

FOR IMMEDIATE RELEASE
May 22, 2006

Frequently Asked Questions on VA's Letter to Veterans

1- I'm a veteran, how can I tell if my information was compromised?
At this point there is no evidence that any missing data has been used illegally. However, the Department of Veterans Affairs is asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved and contact the Federal Trade Commission for further guidance.

2- What is the earliest date at which suspicious activity might have occurred due to this data breach?
The information was stolen from an employee of the Department of Veterans Affairs during the month of May, 2006. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that veterans may notice suspicious activity during the month of May.

3- I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?
The Department of Veterans Affairs strongly recommends that veterans closely monitor their financial statements and visit the Department of Veterans Affairs special website on this, www.firstgov.gov or call 1-800-FED-INFO (1-800-333-4636).

4- Should I reach out to my financial institutions or will the Department of Veterans Affairs do this for me?

The Department of Veterans Affairs does not believe that it is necessary to contact financial
institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

5- ***Where should I report suspicious or unusual activity?***
The Federal Trade Commission recommends the following four steps if you detect suspicious
activity:
Step 1 – Contact the fraud department of *one* of the three major credit bureaus:
Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

-More-

Frequently Asked Questions // 2

Step 2 – Close any accounts that have been tampered with or opened fraudulently

Step 3 – File a police report with your local police or the police in the community where the
identity theft took place.

Step 4 – File a complaint with the Federal Trade Commission by using the FTC's Identity Theft
Hotline by telephone: 1-877-438-4338, online at www.consumer.gov/idtheft, or by mail at
Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW,
Washington DC 20580.

6- I know the Department of Veterans Affairs maintains my health records electronically;
was this information also compromised?
No electronic medical records were compromised. The data lost is primarily limited to an
individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of
potential use to identity thieves and we recommend that all veterans be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7- What is the Department of Veterans Affairs doing to insure that this does not happen
again?
The Department of Veterans Affairs is working with the President's Identity Theft Task Force,
the Department of Justice and the Federal Trade Commission to investigate this data breach and
to develop safeguards against similar incidents. The Department of Veterans Affairs has directed all VA employees complete the "VA Cyber Security Awareness Training Course" and complete the separate "General Employee Privacy Awareness Course" by June 30, 2006. In addition, the Department of Veterans Affairs will immediately be conducting an inventory and review of all current positions requiring access to sensitive VA data and require all employees requiring access to sensitive VA data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the

Federal Bureau of Investigation and the Inspector General of the Department of Veterans Affairs, have launched full-scale investigations into this matter.

8- Where can I get further, up-to-date information?

The Department of Veterans Affairs has set up a special website and a toll-free telephone
number for veterans which features up-to-date news and information. Please visit www.firstgov.gov or call 1-800-FED-INFO (333-4636).