rec'd 06/07/06

THE SECRETARY OF VETERANS AFFAIRS

WASHINGTON

Dear Veteran:

The Department of Veterans Affairs (VA) has recently learned that an employee took home electronic data from the 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.

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 enclosed question and answer sheet. For additional information, the VA has teamed up with the Federal Trade Commission and has a Web site (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.

Beware of any phone calls, e-mails, and other communications from individuals claiming to be from VA or other official sources, asking for your personal information or verification of it. This is often referred to as information solicitation or "phishing." VA, other government agencies, and other legitimate organizations will not contact you to ask for or to confirm your personal information. If you receive such communications, they should be reported to VA at 1-800-FED-INFO (1-800-333-4636).

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 the VA take our obligation to honor and serve America's veterans very seriously and we are committed to ensuring that this never happens again.

In accordance with current policy, the Internal Revenue Service has agreed to forward this letter because we do not have current addresses for all affected individuals. The IRS has not disclosed your address or any other tax information to us.

Sincerely yours,

R. James Nicholson

Enclosure

May 2006

Answers to Frequently Asked Questions

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

(Continued on reverse.)

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

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 ensure 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 (1-800-333-4636).