

DISTRICT OFFICE:

534 BROADHOLLOW ROAD, SUITE 302
MELVILLE, NY 11747
PHONE: (631) 777-7391
PHONE: (516) 505-1448
PHONE: (718) 875-1675
FAX: (631) 777-7610



Congress of the United States
House of Representatives

STEVE ISRAEL
Third District, New York

WASHINGTON OFFICE:

2457 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
PHONE: (202) 225-3335
FAX: (202) 225-4669
www.house.gov/israel
Twitter: @RepSteveIsrael

March 8, 2013

Secretary Eric K. Shinseki
U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington DC 20420

Dear Secretary Shinseki:

Today I write to you about a troubling matter that threatens our nation's veterans and the security of their personal information. Yesterday, George Opfer, the Inspector General of the Department of Veterans Affairs (VA), released a "Review of Alleged Transmission of Sensitive VA Data Over Internet Connections." This report validated previous allegations that the VA has transmitted veterans' data and sensitive information in some regions over unsecured networks that are susceptible to both hackers and wrongdoers. I believe this assessment must be taken seriously and addressed swiftly.

It is our moral obligation as Americans to provide the best healthcare available to American veterans, but in doing so we need to protect their electronic health records and must not transmit those documents over unsecured networks. In January 2013, the Department of Homeland Security reported that the number of cyber attacks launched against U.S. infrastructure in 2012 increased by over 50 percent. Knowing this, the federal government must take every precaution available to prevent attacks and protect against vulnerabilities.

Specifically, the Office of the Inspector General (OIG) found that the "VA typically transferred unencrypted sensitive data, such as electronic health records and internal Internet protocol addresses, among certain VA medical centers and outpatient clinics using an unencrypted telecommunications carrier network. OIT management acknowledged this practice, accepting the security risk of potentially losing or misusing the sensitive information exchanged via a waiver. However, the use of a system security waiver was not appropriate. Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems." This is unacceptable.

American veterans deserve better. In getting top notch healthcare services, they shouldn't have to worry about fraud or hackers getting their private information to scam them. The Inspector General's report also noted that this "sensitive VA data could be used to perpetrate various types of fraud, including tax fraud." In the first nine months of 2012 alone, the IRS identified almost 642,000 incidents of tax identity theft. Considering this factor and that identity theft annually tops the list of consumer complaints being

reported to the Federal Trade Commission and local law enforcement, this problem must be fixed immediately.

In conclusion, the OIG recommended that the "Assistant Secretary for Information and Technology identify the VA networks transmitting sensitive data over the unencrypted carrier networks and implement configuration controls to ensure encryption of such data." The current unsecured data sharing of veterans' information must be stopped.

I respectfully request an update on the status of these security reforms and your thorough review as they are put in place swiftly. I look forward to working with you to ensure our veterans and their personal information are protected and treated with the highest quality care and concern. Thank you again for your urgent attention to this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "S. Israel", written over the printed name.

Steve Israel
Member of Congress