Department of Veterans Affairs

Office of Inspector General

MANAGEMENT LETTER:

Review of Department of Veterans Affairs Activities to Collect, Review, and Use Information That Identifies Individuals Who Access the Department's Internet Sites

Report No.: 00-02797-78
Date: May 21, 2001

Office of Inspector General
Washington, DC 20420

Department of Veterans Affairs

Memorandum

Date: MAY 21, 2001

From: Assistant Inspector General for Auditing (52)

Subj: Review of Department of Veterans Affairs Activities to Collect, Review, and Use Information That Identifies Individuals Who Access the Department's Internet Sites (Report No. 00-02797-78)

To: Chairman, Subcommittee on Treasury and General Government, Committee on Appropriations, United State Senate

Chairman, Subcommittee on Treasury, Postal Service and General Government, Committee on Appropriations, United States House of Representatives

1. Purpose

The Department of Veterans Affairs (VA) Office of Inspector General (OIG) conducted a review of VA Internet web sites in accordance with Section 646 of the Omnibus Appropriations Act (H.R. 4577) and Office of Management and Budget (OMB) guidelines. The OIG is required by the Act to provide a report to Congress disclosing the agency's activity relating to the collection of data about individuals who access any VA Internet site.

2. Background

To ensure Federal agencies protect an individual's right to privacy when collecting personal information, OMB issued Memorandum M-99-18, Privacy Policies on Federal Web Sites, in June 1999. This memorandum requires each agency to post clear privacy policies on World Wide Web sites and to any other known, major entry point to the site. These privacy policies must also be posted to any web page where substantial personal information is collected from the public. In addition, privacy policies must be clearly labeled and easily accessed when someone visits a web site. The guidance requires that agencies can only use "cookies" or other automatic means of collecting information if they give clear notice of those activities. Cookies are small bits of software placed on a web user's hard drive that help web servers identify their users or track browsing habits.

On June 22, 2000, OMB issued Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites. The purpose of the memorandum is to remind each agency they are required by law and policy to establish clear privacy policies for its web activities and to ensure full adherence with stated privacy policies. This memorandum states that due to the unique laws and traditions about government access to citizens' personal information, the presumption should be that cookies are not to be used at Federal web sites. However, in addition to clear and conspicuous posted notice, cookies can be used if the following conditions are met: (1) a compelling need to gather the data on the site exists, (2) appropriate and publicly disclosed privacy safeguards for

handling of information derived from cookies exist, and (3) personal approval is granted by the head of the agency. OMB's Office of Information and Regulatory Affairs Administrator subsequently issued a letter on September 5, 2000, to the Chief Information Officer (CIO), Department of Commerce explaining that OMB did not intend to include session cookies[1] in the requirements of M-00-13.

3. Scope and Methodology

We reviewed 988 VA Internet web sites to determine compliance with OMB Memoranda M-99-18 and M-00-13. These web sites were reviewed for: (1) information being collected on visitors through the use of persistent cookies, and (2) appropriate privacy policy notices posted on the home page or at major entry points to the web site as required. To identify the presence of cookies on a web site, we used a utility program that cleaned the hard drive of all accumulated cookies. We then activated the system to provide a prompt whenever a cookie was detected. After a review of each of these 988 web sites, detailed listings were compiled of: (1) sites using persistent cookies, and (2) sites that did not post adequate privacy act notices to major entry points. We contacted VA's CIO to determine if approvals had been granted allowing the use of persistent cookies on any VA Internet web site.

4. Results

Of the 988 web sites reviewed, 22 sites did not provide privacy policy notices posted at the home page or at a major entry point to the web site. In addition, there were 29 sites identified with persistent cookies. The sites with persistent cookies did not indicate in the privacy statement what information was being collected or why it was being collected, nor had approvals been granted for the use of cookies as required by OMB. Upon completion of the web site reviews we provided the results to the Office of Automation and Network Support Division, the Acting Principal Deputy Assistant Secretary for Information and Technology, and to the webmasters of those sites needing corrective actions.

Research conducted by the Network Support Division into all sites containing persistent cookies, with the exception of one site, revealed the cookies were automatically created as a result of default settings in the web design software. The responsible offices did not realize that setting the defaults would result in the creation of a persistent cookie. The one site that is using a persistent cookie to track user information during navigation between screens was developed prior to the release of OMB's guidance on the use of cookies. Efforts are currently underway by VA to determine if a session cookie could effectively be used to track the required data within this application.

5. Conclusion

The appropriate webmasters of the sites needing corrective action are now correcting these sites to ensure compliance with OMB guidelines. The site that is using a persistent cookie to track user information during navigation between screens is being reviewed by VA to determine if a session cookie could effectively be used to track the required data. Should it be determined the

[1] Session cookies are short-lived and survive only during a single browsing session. Persistent cookies specify an expiration date and remain stored on the client's computer until that expiration date.

use of the persistent cookie is needed; VA advised us that steps would be taken to procure the necessary approval.

In order to gain better control of VA's compliance with OMB policies, the Acting Principal Deputy Assistant Secretary for Information and Technology has requested that each VA office perform a compliance review of all web sites under their responsibility. VA plans to make this an annual requirement and related VA directives and handbooks will be updated to include this policy.

If you have any questions regarding our audit, please contact me or Stephen L. Gaskell, Director, Central Office Operations, at 202-565-4098.

(Original signed by)

MICHAEL SLACHTA, JR.

Cc: Acting Principal Deputy Assistant Secretary for Information and Technology (005)
Special Assistant to the Secretary (00)
Associate Deputy Assistant Secretary for Cyber Security (045A2)
Chief Information Officer, Veterans Health Administration (19)
Chief Information Officer, Veterans Benefits Administration (20S)
Director, Information Systems Service, National Cemetery Administration (402C)
Veterans Benefits Administration OIG Liaison (24)
U.S. General Accounting Office
Department of Defense Office of Inspector General
Ranking Member, Subcommittee on Treasury and General Government, Committee on Appropriations, United States Senate
Ranking Member, Subcommittee on Treasury, Postal Service, and General Government, Committee on Appropriations, United States House of Representatives