2011-01620-IQ-0103

Memorandum to the File
Case Closure

Alleged Security Violation
VISN 1, VA New England Healthcare System, Bedford, Massachusetts
(2011-01620-IQ-0103)

The VA Office of Inspector General Administrative Investigations Division investigated an allegation that [redacted] Veterans Integrated Service Network 1, Bedford, Massachusetts, violated VA policy when he stored VA sensitive information on removable electronic storage devices and then used that information on a laptop at his home. To assess this allegation, we interviewed [redacted] and [redacted] We also reviewed network and computer logs, e-mail records, inventory reports, as well as, relevant Federal laws, regulations, and VA policy. (b) (7)(C)

VA Policy states that all VA employees who have access to and store VA sensitive information must have permission from a supervisor and ISO to use removable storage media/devices to store sensitive information. VA Handbook 6500, Part C, Para. 4(a). It further states that all staff who have access to and store VA sensitive information must have written approval from their respective VA supervisor and ISO, before sensitive information can be removed from VA facilities/operating units and that VA sensitive information, to include all sensitive information entrusted to VA, must be in a VA protected environment at all times, or it must be encrypted. Id. at 4(c) and (d). VA policy states that VA sensitive information may not reside on other non-VA owned Other Equipment (OE) unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver issued by VA's CIO. Id. at 4(J).

Background:

A Zip drive is a removable disk storage system of medium capacity and depending on disk size, will store various amounts of data. A USB flash drive, often called "thumb drive" or "jump drive," is a data storage device that connects to a computer's Universal Serial Bus (USB) and is easily removable. Sanctuary Management Console is a software application that detects, blocks, and audits plug-and-play devices, such as removal storage devices, i.e. USB flash and Zip drives. This software application is deployed on VA systems in order to protect VA information from unauthorized removal. The Citrix Access Gateway (CAG) is a Virtual Private Network (VPN) that provides secure remote access to a virtual desktop through a web browser.

Alleged Security Violation

[redacted] told us that he was not issued a USB flash drive while in his current position and that he never used a Zip drive or external hard drive. Bedford VA Medical Center equipment records reflected that [redacted] was not issued any external storage devices, such as USB flash drives, zip drives, or external hard drives. (b) (7)(C)

[redacted] told us that he was not aware of his office issuing any non-encrypted storage devices to [redacted] told us that he did not connect any personal, non–government issued, USB flash drives, zip drives, or external storages devices to his VA-issued computers, and Sanctuary Management Console logs reflected that [redacted] did not connect any unauthorized devices to his VA-issued computers. [redacted] said that he was not aware of any security violations involving [redacted] further said that his VA-issued computer did not have the ability to safe information to compact disc (CD). (b) (7)(C)

Equipment inventory records reflected that [redacted] had a VA-issued laptop, and [redacted] told us that he used this laptop to work at home afterhours and on weekends. [redacted] and [redacted] both told us that the laptop was encrypted, and [redacted] said that [redacted] was current on all removal authorizations. [redacted] also said that he accessed VA systems from his personal computer using VPN and the Citrix Access Gateway (CAG) as part of a pilot program and that by using this system he accessed patient records and his VA-assigned email. [redacted] told us that [redacted] was authorized to use the CAG from his personal computer, and VPN records reflected that between October 2, 2010, and July 4, 2011, [redacted] connected to VA systems remotely using VPN 204 times. (b) (7)(C)

We did not substantiate the allegation that [redacted] stored VA sensitive information on removable electronic storage devices and then used that information on his personal laptop. Although we found that [redacted] accessed VA sensitive information from his home computer, he did so though an authorized pilot program and through the use of secured VPN access. Furthermore, Office of Information Technology records reflected that [redacted] was not issued any external storage devices and that his VA-issued computers contained software that protects the computer from unauthorized information removal. This case is being closed without issuing a formal report or memorandum. (b) (7)(C)

Prepared By: [redacted]

9/15/11
Date

Approved By: [redacted]

9/15/11
Date