Department of Veterans Affairs

Memorandum

Date: March 26, 2015

From: Director, Information & Technology and Security Audit Division (52CT)

Subj: Hotline Review of Alleged Unapproved Software Installation at Wichita KS VAMC (Project # 2014-05166-CT-0005)

To: Executive Assistant to the Assistant Inspector General for Audits and Evaluations (52)

Thru: Deputy Assistant Inspector General for Audit and Evaluations (52B)

1. On August 19, 2014, the OIG Hotline received a complaint from (b) (3) IG ACT, (b) (3) IG ACT. The complaint alleged that the station Chief Information Officer (CIO) installed unapproved software on VA computers.

2. To determine the merits of the allegation, we reviewed relevant Office of Information Technology (OIT) documentation, VA's software compliance report, and conducted interviews with the complainant and Network Security Operations Center (NSOC) staff. Based on the information provided, we substantiated that Wichita OIT staff, not the CIO, installed unapproved Malwarebytes software on VA computers. However, we also noted that OIT had taken steps to address this issue and a prior OIG audit recommendation in this area. (For more information, see Recommendation No. 25 in the OIG Report, *Federal Information Security Management Act for Fiscal Year 2013*, Report No. 13-01391-72.) More specifically, OIT has developed a listing of approved software and is implementing continuous monitoring processes to identify and prevent the use of unauthorized applications on its networks. Results of a network scan performed subsequent to the allegation showed no instances of the unapproved software on the Region 5 network.

3. In August 2014, (b) (3) IG ACT received an email that contained a listing of computers on the VA network that were infected with either malware or malicious code. The list originated from the NSOC and provided the name of the affected facility, the specific device name, and security incident tracking numbers. Subsequently, (b) (3) IG ACT emailed the Wichita CIO to inquire about the status of the infected machine. The Wichita CIO then contacted one of his staff to have him address (b) (3) IG ACT inquiry. The staff member responded stating that the infected machine had been cleaned and provided a screen shot indicating that Malwarebytes anti-virus software was used to remove the computer infection. However, (b) (3) IG ACT noted that Malwarebytes was not an approved application within VA's Technical Reference Model (TRM) and later submitted a security ticket with the NSOC. As part of the OIT's Enterprise Architecture, VA programs and projects must comply with VA's TRM, which

provides a listing of assessed technologies and standards used to develop and maintain enterprise applications.

4. The Network ISO subsequently contacted the Region 5 Network CIO and requested a response to the security ticket. The Region 5 Network CIO explained that an OIT employee had used the Malwarebytes software to remove a computer infection after unsuccessfully using a VA approved McAfee anti-virus software to eradicate the virus. The Network CIO also wrote that the OIT employee had removed the Malwarebytes software and was instructed to use the security ticket escalation process if approved software was not effective. The Network ISO requested that (b) (3) IG close the security ticket based on the Network CIO's response.

5. Since the time of the complaint, OIT has initiated an unauthorized software removal process that will reportedly detect and ultimately prevent the installation of unauthorized software on its networks. Further, VA has developed a Technical Reference Model and is implementing continuous monitoring processes to ensure compliance with set standards. This effort consists of multiple steps, including utilization of network scanning tools to identify instances of unauthorized and the creation of security incident tickets as appropriate. OIT's Field Security Service will then work with respective facility staff to monitor the removal of unauthorized software and find approved alternatives if necessary.

6. While we partially substantiated the hotline allegation, VA has on-going efforts to remediate this issue and address a prior OIG audit recommendation in this area. Accordingly, we have no new recommendations for improvement and are closing the project without further action. If you have questions or wish to discuss these issues, please contact me at (b) (6).

Michael Bowman
Director—Information Technology and Security Audits (52 CT)