Department of
Veterans Affairs

Memorandum

Date: August 20, 2014

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

Subj: Review of Alleged Redirected Inbound Email (PII) (Project Number: 2014-02790-CT-0146)

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

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

1. In April 2014, the VA OIG Hotline received an allegation from an anonymous complainant regarding VA system configuration and user credential information passing through unauthorized Internet connections. More specifically, the complainant alleged that Veterans Health Information Systems and Technology Architecture (VistA) and Computerized Patient Record System (CPRS) login information and Internet Protocol addresses were discovered within the unencrypted network transmissions that utilized Amazon Web Services, a private cloud service provider.

2. In May 2014, we initiated a review of this complaint and requested relevant system information from the VA Enterprise Systems Engineering staff and the Veterans Health Administration's (VHA) Innovations Program Office. We also conducted interviews and reviewed current documentation, processes, and controls related to the allegation.

3. We did not substantiate this Hotline allegation. Rather, we found the system configuration information identified in the complaint, including passwords and Internet Protocol addresses, was not for accessing VistA production systems but rather for accessing developmental servers hosted within the Amazon cloud environment. Specifically, during our review, we noted that Amazon Web Services was providing VA Sandbox Cloud (VASC) development and test environments for system developers to create enhancements and improve functionality of the VistA suite of applications. Although the VASC environment was hosted within the same Regional Data Center as some VistA production systems, its network environment was isolated from VistA production systems. More specifically, separate Internet connections were utilized so external partners could access VASC test and development environments hosted at the Regional Data Center. VHA also utilized Amazon commercial cloud services to deliver additional developmental resources that cannot be provided at the Regional Data Center.

4. We noted that only fictitious patient information was used in the test and development environments and no sensitive Protected Health Information or Personally Identifiable Information was provided to VASC developers. The entire VistA development application as reviewed by the Office of Information and Technology's Product Development Open Source, Configuration & Tools Management Division to ensure that only appropriate proprietary software, internal source code, system configurations, and

fictitious patient information were used. The VistA test application had only limited functionality within the test environment.

5. Because this hotline complaint was unsubstantiated, we will not pursue this matter further. We have no recommendations for improvement and are closing the project. If you have questions or wish to discuss these issues, please contact me at (b) (6) [redacted].

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