DEPARTMENT OF VETERAN AFFAIRS

Memorandum

Date: April 23, 2013

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

Subj: Review of Alleged Inappropriate Use of System Authority to Operate (Project # 2013-01419-CT-0088)

To: Director, Hotline Division (53E)

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

1. We did not substantiate allegations that Office of Information Technology (OIT) senior managers circumvented Federal Information System Management Act (FISMA) requirements and exposed VA information systems to increased security risks. On January 13, 2013, we received a Hotline complaint from an anonymous source alleging that OIT's intent to perform cursory system testing and provide eight-month Authority to Operate (ATO) extensions for approximately 600 VA information systems was inappropriate. Specifically, the complainant alleged: (1) OIT's abbreviated testing process was truly fraud, waste, and abuse of senior management responsibility as VA could not effectively test 50-100 systems a day; (2) Senior management's actions weakened VA system security and gave a false sense that systems were secure; and (3) OIT did not conduct adequate evaluation and testing of IT security controls to validate re-authorization (i.e., ATO) of VA information systems.

2. To assess the merit of these allegations, we interviewed selected OIT officials, including the current and former Deputy Assistant Secretaries for Information Security, the Associate Deputy Assistant Secretary for Information Security, and the Executive Director of Quality, Performance, and Oversight. These officials provided us with supporting documentation and a basic understanding of VA's current process for providing ATO extensions. We also reviewed a limited sample of system certification and accreditation documents within VA's central data repository (SMART) to determine whether the ATO process met National Institute of Standards and Technology (NIST) guidelines.

3. Based on the work performed, we did not substantiate the three allegations. Specifically, we determined:

- OIT's abbreviated testing process and supporting documentation met minimum FISMA requirements for system security risk assessment prior to re-authorization. VA's continuous monitoring program also will entail periodic testing of all systems throughout the year to ensure systems security risks are effectively mitigated. In this context, senior management took appropriate actions to extend the system ATOs, which were needed to reauthorize prior system certifications and accreditations due to expire at various dates from December 2012 to February 2013.

- OIT senior management's reliance on continuous monitoring and periodic systems security assessments was intended to strengthen information security; we found no evidence that these actions weakened VA system security controls. VA continues to implement certain aspects of its continuous monitoring program. For example, the Department plans to deploy a Governance, Risk, and Compliance tool over the next several months to improve its current capability.

- OIT's high-level reviews of system security controls and reliance on continuous monitoring to evaluate system security risks met minimum NIST and FISMA requirements. Because the continuous monitoring program was not fully implemented, OIT directed system owners to also perform the high-level system security control reviews before formally extending system ATOs through August 31, 2013. As part of this process, OIT management directed system owners to determine whether appropriate security controls could be maintained through the ATO extensions. As of March 25, 2013, VA had completed the extension process for just over 50 percent of its existing information systems. OIT anticipates that its continuous monitoring program will be fully implemented by August 2013.

4. In the May 23 2012 report, we did not substantiate a similar complaint that VA circumvented information security requirements by suspending system security control testing and granting extensions for information systems to operate based on existing continuous monitoring controls.[1] The complainant suggested that continuous monitoring alone could not fulfill FISMA testing requirements. As a result of our review to assess the merits of the allegation, we reported that VA did not circumvent FISMA certification and accreditation requirements by extending ATO for information systems. We reported that VA planned to leverage its continuous monitoring program to assess information system security and identify risks. As a basis for our conclusions, we pointed out that NIST guidelines also promoted continuous monitoring of existing systems.[2] We noted, however, that the continuous monitoring approach did not relieve VA from ensuring the implementation of adequate controls to secure its mission-critical systems.

5. Our FY 2012 FISMA audit identified a number of areas for improvement, such as access controls, configuration management, and continuity of operations, that resulted in an IT material weakness reported as part of our annual consolidated financial statement audit.

[1] *Review of Alleged Circumvention of Security Requirements for System Certifications and Apple Mobile Devices*, VA OIG Report No. 12-00089-182 May 23, 2012.
[2] NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.*

However, as part of this audit we identified no significant issues related to the certification and accreditation of VA's information system and nothing to preclude OIT from extending system ATOs as necessary. We will continue to evaluate the effectiveness of VA's continuous monitoring program and information security controls as part of our annual FISMA assessments.

6. Because we did not substantiate any of the allegations, we have no recommendations for improvement. If you have questions or wish to discuss these issues, please contact Neil Packard, IT Specialist, at (b) (6), or me at (b) (6).

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