VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Circumvention of Security Requirements for System Certifications and Apple Mobile Devices

May 23, 2012
12-00089-182

To Report Suspected Wrongdoing in VA Programs and Operations:
Telephone: 1-800-488-8244
E-Mail: vaoighotline@va.gov
(Hotline Information: http://www.va.gov/oig/contacts/hotline.asp)

DEPARTMENT OF VETERANS AFFAIRS

Memorandum

Date: May 15, 2012

From: Assistant Inspector General for Audits and Evaluations (52)

Subj: Final Report: Review of VA's Alleged Circumvention of Security Requirements for System Certifications and Apple Mobile Devices

To: Assistant Secretary for Information Technology (005)

1. In September 2011, we received a confidential Hotline complaint that VA was circumventing Federal Information Security Management Act of 2002 (FISMA), Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) requirements for certification and accreditation of VA information systems. The complainant specifically alleged that VA was circumventing certification and accreditation requirements because VA had suspended security control testing and granted waivers for existing information systems formally authorized to operate and suggested that continuous monitoring alone could not fulfill the testing requirement. The complainant also alleged that VA was using Apple mobile devices without adhering to Federal Information Processing Standards, *Security Requirements for Cryptographic Modules* (FIPS 140-2), to protect sensitive information stored on the devices. In October 2011, we received a similar inquiry from Senator Jon Kyl regarding the extent to which VA planned to deploy Apple mobile devices (such as iPhones and iPads) without using FIPS 140-2 certified hardware encryption. Senator Kyl requested that we evaluate whether VA's approach of only storing sensitive data in FIPS 140-2 compliant software applications hosted on the mobile devices would meet FISMA requirements.

2. We did not substantiate the allegation that VA was circumventing FISMA certification and accreditation requirements by suspending security control testing and granting operational waivers for existing systems that are formally authorized to operate. We partially substantiated the allegation regarding VA's use of Apple mobile devices without the FIPS 140-2 hardware encryption needed to protect sensitive information stored on them. Specifically, we determined that VA's approach for allowing only FIPS 140-2 certified applications to access sensitive data or storing encrypted data on the mobile device met FISMA information security requirements for data protection. However, we noted that VA could improve security controls and systems management by ensuring an accurate inventory and consistent configuration for the mobile devices deployed enterprise-wide.

3. Use of mobile devices has gained broad acceptance in the private sector and offers access to many specialized applications. Recognizing the potential benefits, in 2011, VA began piloting a limited number of Apple mobile devices that leveraged applications for enhanced medical clinician productivity and email support. For example, clinicians tested the use of the VAi2 iHealth application to access patient data in the Veterans Health Information Systems and Technology Architecture system and provide mobile health care delivery in

real world settings. Although VA's greatest business demand for the Apple mobile devices is in health care, the Department's infrastructure is being expanded to support a wide variety of mobile devices that will serve VA's business needs. Since the pilot began, VA has deployed more than 200 mobile devices at medical and administrative facilities in Washington, DC; Albany, NY; Chillicothe, OH; and Battle Creek, MI.

4. To conduct our review of the mobile device program, we examined FISMA, OMB, and NIST guidelines; FIPS 140-2 standards; and VA policy to identify applicable information systems security requirements. We interviewed relevant personnel within the Office of Information Technology (OIT) to determine compliance with the requirements. We reviewed project artifacts and documents to gain an understanding and timeline for the Department's management and deployment of Apple mobile devices. Additionally, we evaluated whether VA performed appropriate testing and implemented effective security management controls before deploying mobile devices throughout the enterprise. We conducted our review in accordance with Quality Standards for Inspection and Evaluation published by the Council of the Inspectors General on Integrity and Efficiency. We planned and performed the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

5. OMB provides guidance to agencies on meeting FISMA requirements. In April 2010, OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, recommends Federal agencies move toward a risk-based approach for assessing information system security. OMB advised that agencies use automated tools to monitor systems operations continuously to gain enterprise-wide awareness of their information security risks. NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, also promotes continuous monitoring of existing systems. Based on the NIST publication, which states organizations may choose to eliminate system authorization termination dates if their continuous monitoring programs are sufficiently robust to ensure that continued operations are acceptable based on identified risks, VA initiated a continuous monitoring program.

6. In August 2011, in response to the revised OMB guidance, VA's Deputy Assistant Secretary for Information Security issued a memorandum suspending formal systems security assessments and granting 16-month extensions for existing systems formally authorized to operate. For the future, VA planned to leverage technology initiatives, such as "Visibility to the Desktop/Server," to continuously monitor system security and identify risks. We determined that VA's continuous monitoring approach complied with FISMA requirements and supporting OMB and NIST guidance. However, this continuous monitoring approach did not relieve VA from also ensuring the implementation of adequate controls to secure its mission critical systems. We will continue to evaluate the effectiveness of VA's continuous monitoring program and information security controls as part of our annual FISMA assessments.

7. In response to the second allegation and the Senator's inquiry, we partially substantiated that VA is using Apple mobile devices without the FIPS 140-2 hardware encryption needed to protect sensitive information stored on the devices. The manufacturer's documentation accompanying the mobile devices states that hardware is always encryption enabled and cannot be disabled by the user. The mobile devices come with hardware encryption, using a 256-bit Advanced Encryption Standard (AES) algorithm to protect data stored on the devices. As of March 2012, the NIST Cryptographic Module Validation Program was still working to validate the 256-bit AES; however, it had not certified that the encryption module was FIPS 140-2 compliant. Our iPad testing during the pilot project indicated that hardware encryption on the devices was functioning as intended. Additionally, we confirmed that end users could not make configuration changes to disable the hardware encryption.

8. Although the mobile devices were hardware encrypted, VA deployed more than 200 Apple iPhones and iPads with encryption that was not FIPS 140-2 certified. Compliance with the FIPS 140-2 standard is mandatory when agencies specify they will use cryptographic-based security systems to protect sensitive or valuable data. As a compensating control, VA used a FIPS 140-2 certified security application named "Good" from Good Technology to encrypt application data such as emails, calendars, and contacts residing on the mobile devices. "Good" also required that mobile device users provide complex passwords to connect to the VA network, enforcing a strong password policy. VA approved the use of other mobile device applications that are FIPS 140-2 certified to connect to VA systems, however mobile device users can access VA sensitive data through encrypted applications such as virtual private networks, but they cannot store the data on their mobile devices.

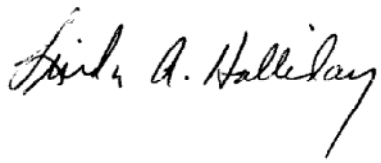
9. Based on our results and in response to Senator Kyl's additional request, we determined that VA's approach of allowing only FIPS 140-2 certified applications to access or store sensitive encrypted data on the mobile device met FISMA requirements for data protection. The manufacturer's default hardware encryption controls have further minimized the risk of unauthorized disclosure of sensitive data while the 256-bit AES undergoes FIPS 140-2 certification testing.

10. We also identified deficiencies regarding VA's information security controls and management of mobile devices. Specifically, VA did not have an accurate inventory of the mobile devices deployed across the enterprise. OIT provided us three iPads to use and evaluate during VA's mobile device pilot test program. Two of the three devices were delivered without the "Good" security application installed and contained factory default settings. Without the "Good" installation, VA could not accurately inventory the mobile devices on the network, or centrally manage and configure device settings through the use of the "Good" Mobile Device Management tool. An accurate inventory and central device management are critical to identify and disable stolen mobile devices as appropriate. The configuration setting on the third device, which had the "Good" security application installed, did not ensure encryption of the device backup files. Malicious users can use text editing programs to view exported backup files of sensitive information stored on the mobile devices.

11. Further, VA did not ensure a consistent security configuration for all mobile devices deployed across the enterprise. VA had three clusters of mobile devices maintained by servers at Hines, IL; Albany, NY; and Washington, DC. Each cluster was configured to different security standards and had a different functionality, resulting in inconsistent security profiles and risks. Our testing revealed that mobile devices supported by the server in Washington, DC had the default copy, paste, and backup to the Internet functionality still enabled. However, mobile devices supported by Albany, NY had this default functionality disabled as VA intended.

12. Inconsistent security configurations occurred because VA had not fully implemented minimum baseline security standards for its mobile devices. FISMA Section 3544 requires each agency to establish minimally acceptable system configuration requirements and ensure compliance. Similarly, NIST Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle: A Security Life Cycle Approach*, states that configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system. By not implementing minimum baseline configuration settings to establish a consistent security posture for each device, VA is placing sensitive data at risk of unauthorized disclosure.

13. We recommended the Assistant Secretary for Information Technology implement minimally acceptable baseline security configuration requirements for VA mobile devices in accordance with FISMA. We also recommended the Assistant Secretary centrally manage the distribution of VA mobile devices to ensure they are accurately inventoried and configured in accordance with minimum-security standards. The Assistant Secretary concurred with our findings and recommendations and stated that OIT has created a security baseline standard for mobile devices that will continue to evolve as the technology matures. Further, VA will centrally manage all mobile devices against minimally acceptable baseline security requirements by June 2012. We consider this response acceptable and will monitor implementation of the corrective action plans.



LINDA A. HALLIDAY

Appendix A Assistant Secretary for Information and Technology Comments

Department of Veterans Affairs **Memorandum**

Date: April 27, 2012

From: Assistant Secretary for Information Technology (005)

Subj: Draft Report: Review of Alleged Circumvention of Federal Information Security Management Act of 2002 Requirements and Deploying Mobile Devices Enterprise-Wide

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

Thank you for the opportunity to review the subject draft OIG report. The Office of Information Technology concurs with the findings and submits the attached written comments for each recommendation. If you have questions, please contact me at 202-461-6910 or have a member of your staff contact Gary Stevens, Director, Officer of Cyber Security (005R2), at 202-632-7538.

(original signed by:)

Roger W. Baker

Attachment

Attachment

Office of Information Technology
Response to Draft OIG Report,
"Review of Alleged Circumvention of FISMA Requirements and Deploying Mobile Devices Enterprise-Wide"

OIG Recommendation 1: ***We recommend the Assistant Secretary for Information and Technology implement minimally acceptable baseline security configuration requirements for VA mobile devices in accordance with FISMA.***

OIT Comment*:* Concur. OIT has created and published a security baseline standard for mobile devices and will continue to evolve that baseline as the technology matures. As the minimum standard has already been posted for these devices, implementation is considered complete. We recommend closure of this recommendation.

OIG Recommendation 2: ***We recommend the Assistant Secretary centrally manage the distribution of VA mobile devices to ensure they are accurately inventoried and configured in accordance with minimum security standards.***

OIT Comment*:* Concur. OIT currently uses "GOOD for Enterprise" to manage all OIT purchased mobile devices. This provides inventory and configuration enforcement for mobile devices. All production GOOD servers will be under one GOOD instance run out of Hines, IL by June 30, 2012.

****

OIT Technical Comments to OIG Findings in the draft report: None

Appendix B OIG Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720
Acknowledgments	Michael Bowman, Director Carol Buzolich Mike Miller Gordon Snyder

Appendix C Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG Web site for at least 2 fiscal years.