DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

VA's Management of Mobile Devices Generally Met Information Security Standards

AUDIT | **REPORT #18-04608-212** | **OCTOBER 22, 2019**

The mission of the Office of Inspector General is to serve veterans and the public by conducting effective oversight of the programs and operations of the Department of Veterans Affairs through independent audits, inspections, reviews, and investigations.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

VA's Office of Information and Technology (OIT) manages over 50,000 mobile devices that store, process, and transmit veteran information and require protection at all times. VA centrally manages mobile devices accessing VA networks through an enterprise-wide mobile device management (MDM) system. A centralized, enterprise-wide MDM system can provide consistent management, configuration, security, and continuous monitoring of VA mobile devices. The VA Office of Inspector General (OIG) contracts with an independent public accounting firm to conduct an annual audit of VA's information security program and practices to determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute for Standards and Technology (NIST) information security guidelines.[1] However, the FISMA audit focuses on selected major applications, and VA's MDM system is not one of the applications evaluated. The OIG conducted this audit to determine whether OIT is implementing policies and procedures to mitigate information security weaknesses associated with mobile devices being used in VA's network infrastructure.

What the Audit Found

The audit team found OIT's security practices for mobile devices generally mitigated security control weaknesses within VA's network infrastructure. The Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) has five general categories of information technology controls—security management, access controls, segregation of duties, contingency planning, and configuration management.[2] OIT's information technology controls in four of the five categories met OMB, NIST, and VA security standards for VA mobile devices.

However, the audit team did find vulnerabilities associated with configuration management. Specifically, OIT did not enforce blacklisting of applications as required by VA policy.[3] Blacklisting blocks the use of applications to prevent the execution of malicious, vulnerable, or flawed applications. According to OIT's director of mobile technology and endpoint security

[1] NIST is an agency of the Department of Commerce that has the responsibilities under the Federal Information Security Management Act of 2002 to develop mandatory standards and guidelines for federal agencies' information and information systems.

[2] GAO-09-232G, February 2, 2009. FISCAM provides a methodology for performing information systems control audits of federal entities in accordance with professional standards.

[3] VA Handbook 6500.10, *Mobile Device Security Policy*, February 15, 2018.

engineering, OIT decided not to implement blacklisting due to the workload associated with vetting applications. OIT would need to individually assess the security risks to VA data of over two million applications, and OIT would also need to add the applications that were considered high risk to the blacklist in the MDM system. Because OIT has not implemented blacklisting, users can download applications that are not authorized on VA mobile devices, such as cloud-based applications. Cloud-based applications could allow users to transfer locally stored VA data into uncontrolled storage, increasing the risk of lost VA data. According to OIT, it has started implementing application-vetting tools that have a similar capacity to blacklisting.

Training is one mitigating control VA uses in the absence of blacklisting, but the audit team also found VA does not validate whether users of mobile devices are completing the required annual *Mobile Training: Security of Apps on iOS Devices*. A separate training, the *VA Privacy and Information Security Awareness and Rules of Behavior*, is required and validated through the Talent Management System, but does not address prohibited applications on mobile devices. Furthermore, OIT has no way to validate the effectiveness of annual information security training because OIT cannot check mobile devices that are not in supervised mode to see what applications users may have installed from a source other than the VA application store—i.e., Apple's application store.[4]

Finally, the audit team found VA does not use configuration management tools to control and automate updates for its mobile devices and applications. According to FISCAM, configuration management controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended. The audit team found users of mobile devices were responsible for managing the updates of their applications and operating systems. Prior to the Apple iPhone Operating System (iOS) 12 update, the audit team found that notifications from OIT advising users not to update applications and devices were sent after users had experienced issues as a result of installing updates. The audit team found 12,298 out of 50,618 mobile devices had unapproved operating systems.

According to OIT's director of mobile technology and endpoint security engineering, OIT decided not to use configuration management tools, as with blacklisting, due to the workload associated with using supervised mode. To enforce supervised mode, OIT administrators would need to physically connect each individual mobile device to an Apple computer for configuration. Enforcing supervised mode would also require a wide distribution of Apple computers to administrators and would add tasks to the implementation process, which would require more time to issue the devices.

[4] Supervised mode allows administrators to centrally manage and control Apple iOS devices.

As a result of not using the tools, VA is unable to prevent users from updating the operating system or applications before testing can be accomplished. The lack of configuration management tools has resulted in VA users experiencing loss of use of their applications due to installing device updates before application updates were tested and approved by OIT. In addition, relying on users to perform updates could result in security vulnerabilities if updates are untimely. Furthermore, premature or untimely updates by users impact the usability of their devices—for example, interfering with their access to VA email, contacts, and calendars. OIT has now awarded a contract to Lookout for a new application-vetting tool, but as of the time of this report, it was not available for review by the audit team.

What the OIG Recommended

The OIG made three recommendations to mitigate information security weaknesses associated with mobile devices being used in VA's network infrastructure. Recommendations include enforcing blacklisting or formally assessing and documenting the approach of using training as the mitigating control, using configuration management tools to prevent premature or late updating, and validating that users are completing the required annual mobile device training.

Management Comments

The principal deputy assistant secretary for information and technology and deputy chief information officer concurred with Recommendations 1−3. Regarding Recommendation 1, the principal deputy assistant secretary stated OIT is working on two approaches to address the recommendation. The first approach involves deploying the Lookout application to VA mobile endpoints to ensure mobile applications are not malicious. The second approach involves implementing a process to ensure mobile users are trained in appropriate and inappropriate use of VA sensitive data applications prior to receiving mobile devices.

In response to Recommendation 2, the principal deputy assistant secretary stated OIT is working to transition all mobile devices to supervised mode. OIT can delay operating system updates for a maximum of 90 days for mobile devices in supervised mode but cannot indefinitely prevent application updates due to the Apple App Store model. For VA-specific applications, OIT will implement a process to look for any updates, test them, and confirm there are no issues. If issues are identified, a bulletin will be released to all mobile users to refrain from updating until the issues are resolved. The principal deputy assistant secretary reported that OIT will provide target completion dates and additional details on corrective actions for Recommendations 1 and 2 when they respond to the OIG's 90-day follow-up memorandum.

Regarding Recommendation 3, the principal deputy assistant secretary stated VA will fully implement a process by June 30, 2020, to ensure mobile training is provided before users receive devices. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Executive Summary i

Abbreviations vi

Introduction 1

Results and Recommendations 6

Finding 1: OIT Security Practices Generally Mitigated VA's Mobile Device Security Weaknesses 6

Finding 2: Configuration Management Vulnerabilities Existed 13

Recommendations 1–3 18

Appendix A: Scope and Methodology 20

Appendix B: Management Comments 22

OIG Contact and Staff Acknowledgments 24

Report Distribution 25

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
iOS	Apple iPhone Operating System
MDM	mobile device management
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
PIV	personal identity verification

Introduction

The VA Office of Inspector General (OIG) conducted this audit to determine whether the Office of Information and Technology (OIT) has implemented policies and procedures to mitigate information security weaknesses associated with mobile devices used in VA's network infrastructure. OIT manages over 50,000 mobile devices that store, process, and transmit veteran information and require protection at all times.

VA centrally manages mobile devices accessing VA networks through an enterprise-wide mobile device management (MDM) system. A centralized, enterprise-wide MDM system can provide consistent management, configuration, security, and continuous monitoring of VA mobile devices. The OIG contracts with an independent public accounting firm to conduct an annual audit of VA's information security program and practices to determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA).[5] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[6] However, the FISMA audit focuses on selected major applications, and VA's MDM system is not one of the applications evaluated.

Federal Information System Controls Audit Manual

To accomplish the objective, the audit team assessed VA's information security program related to mobile devices by aligning risk areas with the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual*'s (FISCAM) five general categories of information technology controls. FISCAM provides a methodology for performing information systems control audits of federal entities in accordance with generally accepted government auditing standards. The following are the five categories of information technology controls:

- Security management controls provide reasonable assurance that security management is effective.
- Access controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals.
- Configuration management controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended.

[5] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[6] NIST is an agency of the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

- Segregation of duties controls provide reasonable assurance that incompatible duties are effectively segregated.
- Contingency planning controls provide reasonable assurance for protection of information resources, minimize the risk of interruptions, and provide recovery of critical operations should interruptions occur.

National Institute of Standards and Technology's Mobile Device Guidelines

A NIST special publication defines the characteristics of a mobile device as being small; having network access, built-in data storage, and applications that can be accessed through a web browser; and lacking a desktop or laptop operating system.[7] The publication also states that mobile devices need to support multiple security objectives—confidentiality, integrity, and availability—and secure against a variety of threats. According to the publication, this could be accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise information technology infrastructure.

According to the NIST special publication, organizations should create a mobile device security policy. The policy should address what types of resources may be accessed by mobile devices, the degree of access for different classes of devices, and how configuration and administration of devices should be handled—e.g., how centralized mobile device management servers are administered and updated. The policy should be consistent with and complement nonmobile security policy. Organizations should use threat modeling to identify any threats that are unique to mobile devices.

The publication also states that the nature of mobile devices makes them more susceptible to being lost or stolen than other devices, so their data are at a higher risk of compromise. Mobile device security policies and controls should be created with the assumption that the devices will be acquired by malicious parties who will attempt to recover sensitive data either from the devices or by using the devices to remotely access organizational data. The publication recommends a layered approach to mobile device security. The first layer is to use an authentication method more robust than a personal identification number, such as token-based authentication, network-based device authentication, and domain authentication. The second layer involves protecting sensitive data either by encrypting the devices or by not storing data on them.

[7] Department of Commerce, NIST, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* by Murugiah Souppaya and Karen Scarfone. Special Publication 800-124, Revision 1, sec. 2.1, June 2013.

The publication recommends application management to restrict which application stores may be used. Agencies should consider conducting an application inventory, verifying digital signatures of applications to ensure trust, and using dedicated distribution of organizational applications. Recommended operation and maintenance practices for mobile devices include checking upgrades and patches, keeping an active inventory of devices and applications, providing user training specific to mobile devices, revoking or deleting applications when an increase in risk is identified, and deleting data from a mobile device before reissuing it.

VA's Mobile Device Security Policy

VA Handbook 6500.10, *Mobile Device Security Policy*, provides policy and procedures for securing VA mobile devices, which are the only mobile devices that can be connected to the VA network or used to store or transmit VA data. The handbook defines which types of mobile devices are permitted to access VA resources; what degree of access is permitted; how provisioning and development should be handled; how VA will select, implement, and use centralized mobile device management technologies; and what responsibilities relate to mobile device security.

Government Accountability Office Mobile Device Vulnerabilities and Recommendations

Vulnerabilities

According to GAO, mobile devices are subject to numerous security vulnerabilities. The following is a list of some vulnerabilities found on mobile platforms.

- Mobile devices often do not have passwords enabled, meaning mobile devices often lack passwords to authenticate users and control access to data stored on the devices.
- Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. Using static passwords for authentication rather than two-factor authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or obtained through eavesdropping.
- Wireless transmissions are not always encrypted, and as a result, information such as emails sent by a mobile device are usually not encrypted while in transit.
- Mobile devices may contain malware, and users could download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application.
- Mobile devices often do not use security software because many mobile devices do not come already installed with security software to protect against malicious applications, spyware, and malware-based attacks.

- Operating systems may be out-of-date as security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner.
- Mobile devices often do not limit internet connections because many mobile devices do not have firewalls to limit connections.
- Communication channels may be poorly secured leaving those channels, such as Bluetooth, "open" or in "discovery" mode.

Recommendations

GAO outlines security controls that can be enabled on mobile devices to help protect against common security threats and vulnerabilities.[8] As previously discussed, mobile devices and many mobile applications do not always encrypt data on their own before transmission. Other network communications such as Wireless Personal Area Networks, which are short range networks that require little or no infrastructure, are left unsecured and discoverable. Bluetooth can be used to establish Wireless Personal Area Networks. Malware is prevalent in mobile applications due to the ability of the malware to be easily concealed in a seemingly valid application.

The following are security controls identified by GAO to combat common threats and vulnerabilities:

- Enable user authentication.
- Enable two-factor authentication.
- Validate application authenticity.
- Install antimalware.
- Install firewall.
- Receive prompt security updates.
- Remotely disable lost or stolen devices.
- Enable encryption for data stored on the device.
- Implement a virtual private network.
- Enable, obtain, and analyze device log files.

GAO also recommends turning off or setting Bluetooth to nondiscoverable, limiting the use of public Wi-Fi, minimizing unnecessary applications, configuring web accounts for secure connections, and limiting storage of sensitive information on the device. In addition, GAO

[8] GAO, *Better Implementation of Controls for Mobile Devices Should Be Encouraged*, GAO-12-757, September 2012. According to GAO, this is not a comprehensive list but is consistent with recent studies and guidance.

recommends establishing mobile device security policy, providing mobile device training, performing risk assessments, and performing configuration control for mobile devices.

VA's Assessment

In January 2017, OIT published *Staff-Facing Mobile Devices and Applications Security*, which included MDM within VA. The document identified three hurdles to the success of securing VA's mobile devices. First, OIT was not using enterprise mobility management to manage and secure VA mobile devices.[9] Second, there was an authentication gap for users with only personal identity verification (PIV) cards for credentials that prohibited them from using MobilePASS for remote access.[10] Last, OIT identified a lack of mobile device backup. OIT also determined it was using multiple MDM solutions to manage an array of devices, such as Blackberry, Apple, and Android. The use of multiple MDM solutions adds complexity and configuration issues and subsequent security vulnerabilities. VA also did not have Federal Information Processing Standard-compliant encryption on all mobile devices.[11]

[9] Enterprise mobility management is a holistic approach to securing and managing mobile devices. It typically includes some combination of mobile device, application, and data management capabilities.

[10] MobilePASS provides two-factor authentication for remote Citrix Access Gateway (VA virtual services) users by generating a onetime password.

[11] Department of Commerce, NIST, *Security Requirements for Cryptographic Modules,* Federal Information Processing Standard 140-2, May 25, 2001.

Results and Recommendations

Finding 1: OIT Security Practices Generally Mitigated VA's Mobile Device Security Weaknesses

The audit team found OIT's security practices for mobile devices generally mitigated security control weaknesses in VA's network infrastructure. OIT's information technology controls in four of the five FISCAM categories—security management, access controls, segregation of duties, and contingency planning—met OMB, NIST, and VA security standards for VA mobile devices.

What the OIG Did

The audit team examined VA-managed mobile devices and applications and reviewed risk assessment documentation and configuration settings to assess the security of VA's mobile devices. The audit team conducted interviews with OIT's director of mobile technology and endpoint protection, system administrators, and the acting director of the Office of Cyber Security to determine the sufficiency of information technology security oversight for mobile devices. In addition, the audit team interviewed the senior technical lead for the identity management team, which supports VA's Enterprise Public Key Infrastructure solution, to determine the sufficiency of certificate management and authentication of users and mobile devices. The audit team also interviewed contracting officer's representatives and the training manager for the contracted administrators to determine the adequacy of their training.

The audit team reviewed policy and risk assessment documentation associated with mobile device management. The audit team also reviewed configuration files for mobile devices. In addition, the audit team examined OIT spreadsheets showing device inventories, configurations, and user profiles to determine if unapproved devices and software were being managed by OIT. This finding discusses security management, access controls, segregation of duties, and contingency planning.

Security Management

Overall, VA met NIST and VA security standards for security management. OIT's move to a single-vendor (Apple) mobile device resulted in a single MDM solution, and VA's approach not to use antivirus protections was congruent with standard security practices. Also, OIT had the required risk assessment documentation. According to FISCAM, security management controls are those that provide reasonable assurance that security management is effective. An entity-wide security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for

assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. The audit team specifically reviewed security management controls in the areas of multiple MDM solutions, antivirus implementation, and risk analysis.

Multiple MDM Solutions

The audit team found that OIT's *Staff-Facing Mobile Devices and Applications Security* assessment revealed a concern related to multiple MDM solutions. Multiple management platforms create a larger attack surface and divide administrator security efforts, resulting in higher risk and less ability to prepare and respond. In July 2016, VA's chief information officer issued guidance requiring users to transition from Android devices to Apple devices by November 17, 2016. All users were required to have VA-furnished Apple devices. The audit team reviewed the device inventory list in VA's MDM application, which revealed only 15 non-Apple iPhone Operating System (iOS) devices out of 50,618. This is consistent with interviews provided by the Tier IV administrator and the director of mobile technology and endpoint security engineering.[12] The audit team found that the transition resulted in a single-vendor environment and consequently a single MDM solution.

Antivirus Protection

The audit team found that the nonuse of antivirus applications was congruent with normal security practices. VA exclusively uses iOS for VA mobile devices. According to the director of mobile technology and endpoint security engineering, VA does not use antivirus software on its mobile devices. Devices using iOS have security provided in layers to ensure that applications are signed, verified, and "sandboxed" to protect user data.[13] Once iOS starts, it controls which processes and applications can be run, ensuring that all applications come from known and approved sources and have not been tampered with. The Apple application store submission process works to further shield users from risks by reviewing every iOS application before it is made available. If a virus does affect an application, sandboxing makes it very difficult for an infected application to spread the virus to another application.

In addition, the use of antivirus applications consumes resources on the device, slowing processing. The audit team reviewed iOS security and commercial antivirus providers' documentation. Antivirus for iOS is not available from several reputable commercial antivirus providers. The audit team also interviewed a Tier IV administrator and the director of mobile technology and endpoint security engineering to assess VA's approach of not using antivirus software.

[12] The Tier IV administrator manages the design of the MDM system.

[13] According to NIST, a sandbox is a restricted, controlled execution environment that prevents potentially malicious software from accessing any system resources except those for which the software is authorized.

Risk Analysis

The audit team found that the security risk documentation was sufficient. OIT is required to assess security risks to its systems and document its approach to providing security for the system. The documentation for the assessment and mitigations for VA is stored in VA's Governance, Risk, and Compliance RiskVision System. Security documents such as assessments, control lists, and plans of action and milestones are used to determine if vulnerabilities to the system are being mitigated. The audit team reviewed the security documentation and compared it to federal and VA requirements to determine if VA's risk assessment and security plan for MDM were up-to-date and complete.

Access Controls

VA met OMB, NIST, and VA security standards for access controls. According to NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification Credentials*, the use of PIV cards with mobile devices has proven to be challenging. Due to the cards' impracticality, Special Publication 800-157 provides an alternative to the use of PIVs through the use of derived PIV certificates. Derived PIV certificates leverage the current investment in PIV infrastructure while achieving a substantial cost savings. VA uses derived certificates for two-factor authentication to mitigate the inability to use PIV authentication. The audit team interviewed an OIT Tier IV administrator, as well as the program director and the senior technical lead for identification and authentication management, to assess VA's PIV posture. The audit team also reviewed PIV and derived certificate publications, OIT procedures, and VA's MDM and enterprise service applications for compliance settings for certificate management.

The audit team found that VA's use of a two-factor authentication solution, instead of PIV cards, met OMB's policy through the NIST Special Publication 800-157 alternative. The audit team also found VA uses FIPS-compliant encryption on its mobile devices and, according to a system administrator, is limiting iCloud access to device recovery and non-VA user data. According to FISCAM, access controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals. Access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. FISCAM also stated that without adequate access controls, unauthorized individuals, including intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or withdraw data or execute changes that are outside their span of authority.

Inadequate access controls diminish the reliability of computerized data and increase the risk of the data's destruction or inappropriate disclosure. The audit team assessed access controls by reviewing PIV compliance, device encryption, cloud storage usage, and blacklisting. The audit

team found OIT does not enforce blacklisting of applications as required by VA's Handbook 6500.10, which is discussed in Finding 2.

PIV Compliance

The PIV credential is the sole identity credential for VA employees, contractors, and affiliates. User authentication confirms the identity of individuals accessing enterprise resources. The PIV credentials are used to access VA resources that require authentication and authorization and provide digital signature capability. VA does not use PIV authentication to meet the requirements of OMB Memo M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*, for mobile devices.[14] According to NIST Special Publication 800-157, the use of PIV cards was geared toward traditional computing devices with an integrated smartcard reader. A PIV sled (card reader) on mobile devices is a method for accessing VA data that requires an Active Directory authentication.[15]

However, NIST Special Publication 800-157 provides an alternative which can be implemented and deployed directly with mobile devices. The PIV credential associated with this alternative greatly improves the usability of electronic authentication from mobile devices to remote information technology resources. Instead of using PIV smartcard credentials as required by OMB Memorandum M-11-11, VA implemented a two-factor authentication solution to meet the Special Publication 800-157 alternative. According to OIT officials, they decided not to use PIV sleds due to cost and lack of practicality. However, according to OIT's director of mobile technology and endpoint protection, no formal cost analysis or documented approach was conducted to make this determination. Furthermore, the decision not to use PIV sleds was also based on a lack of standards for the sleds themselves and functional limitations of the sleds with applications.

Device Encryption

NIST Special Publication 800-124, Revision 1, recommends that agencies encrypt stored data on mobile devices. Device encryption protects data on a device by making it more difficult to interpret if it is obtained by unauthorized personnel. When a passcode is enabled on an Apple device, it is automatically encrypted at FIPS 140-2 level. On March 9, 2018, Apple achieved

[14] OMB Memo M-11-11 (February 3, 2011) is the continuation policy for use of a common identification standard and requires that all new systems be enabled to use PIV credentials prior to being made operational.

[15] Active Directory is a hierarchical structure that stores information about objects on the network and provides methods for storing directory data and making data available to network users and administrators. For example, Active Directory stores information about user accounts, such as names, passwords, and phone numbers, and enables other authorized users on the same network to access this information.

FIPS 140-2 encryption validation, which is the standard for federal encryption.[16] According to OIT's *Mobile Technology and Endpoint Security Engineering Activation Guide*, users are required to establish a passcode when performing initial setup of their mobile device. VA mobile devices are required to have a passcode enabled prior to being registered with the MDM application.

To validate encryption, the audit team interviewed a Tier IV administrator and reviewed VA policy, Apple security documents, FIPS accreditation documents, and MDM application settings to confirm encryption enforcement. The audit team also reviewed the device inventory to confirm that there were no devices being managed that had non-FIPS-compliant operating systems. Correspondingly, OIG's original concern that VA was using non-FIPS-compliant encryption was resolved in March of 2018, when Apple met the FIPS 140-2 encryption requirements.

Cloud Storage

The audit team determined that the use of cloud storage for device restoration and user data does not present a risk to VA data due to the security controls that are in place. Cloud computing enables the sharing, storage, and accessibility of data through the internet rather than by individual, limited-access hard drives. VA Handbook 6500.10 states that users are prohibited from synchronizing mobile devices with non-VA systems and that blacklisting will be used to block cloud-based applications and applications with known vulnerabilities. Apple's iCloud cloud storage application is embedded in iOS devices and is required for device restoration. There is no capability to back up VA data onto the iCloud drive, and it is not enabled by default. Once a device is registered with VA's MDM application, users are no longer able to turn on iCloud drive backup. If users deregister their devices to turn on iCloud, VA applications are deleted. Furthermore, user training on rules of behavior for mobile devices requires that users not put VA data in non-VA systems or devices. The audit team reviewed Apple security documents and attempted to turn on iCloud backup without success. While VA's mobile devices do use cloud storage, the amount is limited to the device recovery and user data such as user notes, calendars, and reminders.

Segregation of Duties

VA met NIST and VA security standards for segregation of duties. According to FISCAM, segregation of duties provides reasonable assurance that incompatible duties are effectively segregated through formal operating procedures, supervision, and review. Work responsibilities should be segregated so that one individual does not control all critical stages of a process. Often,

[16] FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module within a security system protecting sensitive but unclassified information.

segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

The audit team interviewed an OIT Tier IV administrator, the director of mobile technology and endpoint security engineering, and contract managers to assess how duties were separated within MDM. According to the director of mobile technology and endpoint security engineering, OIT segregation of duties for MDM is based on VA's Active Directory structure. For example, user access to MDM is limited to individual and organizational email accounts established within the Active Directory structure. Also, OIT uses a tiered approach to system administration. Tier I-IV administrators' access is restricted based on their roles and responsibilities to meet organizational needs and provide user support. The audit team found that there was a low risk of segregation of duties vulnerabilities for MDM.

Contingency Planning

VA met NIST and VA security standards for contingency planning. According to OIT's Tier IV administrator, VA does not provide mobile device backup capabilities, but OIT does allow users to manually back up their own data to a personal or VA computer with USB access if they choose to do so. According to VA Handbook 6500.10, no VA data should be on the device, so there is no risk of loss of VA data. FISCAM states that contingency planning provides reasonable assurance that protects information resources, minimizes the risk of interruptions, and provides recovery of critical operations should interruptions occur. Adequate contingency planning controls will prevent the loss or incorrect processing of data that could result in financial losses, expensive recovery efforts, and inaccurate or incomplete information. VA's approach to contingency planning for mobile devices is that since no VA data reside on the devices, there is no reason to back up the devices.

Although OIT's *Staff-Facing Mobile Devices and Applications Security* assessment found the lack of mobile device backup was an issue. VA applications retrieve data from VA systems where backup takes place. Therefore, VA data are backed up to a central system. As stated in VA Handbook 6500.10, VA data should not be used in non-VA systems and devices. Consequently, there would be no threat of VA data loss. The only risk of data loss would be from user data stored on non-VA systems and devices. However, according to a Tier IV administrator, users can back up their local data for convenience. OIT allows users to manually back up their devices. Therefore, the audit team determined this process is not automated or centralized. Further, the Tier IV administrator explained that backups are encrypted due to passcode enforcement, even though encryption is not required for non-VA data. Once a passcode is enabled on the device, it is encrypted, and any backups that are generated from the device are encrypted as well.

To confirm device backup capabilities, the audit team interviewed OIT personnel with program management, security, and administrative responsibility for MDM. The audit team also reviewed configuration settings, profiles, and Apple security documentation for mobile devices managed by OIT. In addition, the audit team compared settings, profiles, and documentation to VA and federal security requirements. OIT's concern regarding device backups for continuity has been mitigated based on implemented controls that are in place.

Conclusion

The OIG found OIT's security practices for mobile devices generally mitigated security control weaknesses associated with mobile devices used in VA's network infrastructure. OIT's information technology controls within FISCAM security management, access controls, segregation of duties, and contingency planning categories met OMB, NIST, and VA security standards for VA mobile devices. However, the OIG did find vulnerabilities associated with configuration management, which are discussed in Finding 2.

Finding 2: Configuration Management Vulnerabilities Existed

The audit team found configuration management vulnerabilities existed associated with mobile devices. Specifically, OIT does not enforce blacklisting of applications as required by VA's Handbook 6500.10, *Mobile Device Security Policy*. Blacklisting disallows the use of specified applications to prevent the execution of malicious, vulnerable, or flawed applications. Because OIT has not implemented blacklisting, users can download applications that are not authorized on VA mobile devices, such as cloud-based applications (Dropbox, Google Drive, etc.). Cloud-based applications could allow users to transfer locally stored VA data into uncontrolled storage, increasing the risk of lost VA data. According to VA Handbook 6500.10, users are prohibited from synchronizing mobile devices with non-VA systems, and blacklisting will be used to block cloud-based applications and applications with known vulnerabilities.

The OIG also found training is one mitigating control in the absence of blacklisting, but the audit team found OIT does not validate whether users of mobile devices are completing the required annual *Mobile Training: Security of Apps on iOS Devices*. A separate course, the *VA Privacy and Information Security Awareness and Rules of Behavior*, is required and validated through the Talent Management System, but does not address prohibited applications on mobile devices. Additionally, OIT has no way to validate the effectiveness of annual information security training because OIT staff cannot check to see what applications users have installed from Apple's application store for mobile devices that are not in supervised mode.

Finally, VA does not use configuration management tools to control and automate update releases for mobile devices and applications. Instead, users of mobile devices are responsible for managing the updates of their applications and operating systems. As a result, VA is unable to prevent users from updating the operating system or applications before testing can be accomplished. The lack of configuration management tools has resulted in VA users experiencing loss of use of their applications due to installing updates before they were tested and approved by OIT. Furthermore, relying on users to perform updates can lead to untimely updates, which could result in security vulnerabilities. Also, premature or untimely updates by users can impact the usability of their devices—for example, interfering with their access to VA email, contacts, and calendars.

What the OIG Did

The audit team examined VA-managed mobile devices and applications and reviewed configuration settings to assess the security of VA's mobile devices. The audit team conducted interviews with OIT's director of mobile technology and endpoint protection and system administrators to determine the sufficiency of IT security oversight for mobile devices. The audit team also interviewed contracting officer's representatives and training developers for the contracted administrators to determine the adequacy and proficiency of their training. In addition, the audit team reviewed policy and documentation associated with mobile device

management and configuration files for the mobile device manager to identify inconsistencies in the application of settings. To test whether blacklisting was being enforced, the audit team downloaded cloud-based applications to VA-managed mobile devices.[17] The audit team also examined OIT spreadsheets showing device inventories, configurations, and user profiles to determine if unapproved devices and software were being managed by OIT. This finding discusses the purpose of configuration management, the lack of configuration management, and the reliance on users for configuration management.

Purpose of Configuration Management

According to FISCAM, configuration management controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended. Configuration management also involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. At an entity-wide-level, management develops security policies that establish the entity's configuration management process and may establish the configuration settings for the organization. Policy enforcement applications can be used to help administrators define and perform centralized monitoring and enforcement of an entity's security policies.

Lack of Configuration Management

VA is not managing the configuration of its mobile devices in terms of blacklisting, validating security training, and using configuration management tools.

Blacklisting of Applications Not Enforced

The audit team downloaded cloud-based applications to VA-managed mobile devices and found OIT is not enforcing blacklisting of applications. While some of the downloaded applications did not work when the mobile device was connected to the VA wireless network, they did work on both cellular and non-VA networks. Three OIG auditors used their VA mobile devices that were managed by OIT's MDM to download Dropbox and Box applications through public wireless or cellular networks. Dropbox and Box are well-known public cloud file-sharing applications that should be blacklisted. Unauthorized applications could allow users to transfer locally stored VA data into uncontrolled storage, increasing the risk of lost VA data. VA Handbook 6500.10 requires blacklisting to prevent undesired applications from being installed on a device and

[17] The OIG acknowledges that VA Handbook 6500.10, sec. 2(k), states that, due to statutory independence, the OIG manages its own mobile devices with support from VA in accordance with the Inspector General Act of 1978. However, during the audit, OIG mobile devices were managed by VA OIT and utilized the same security profiles as the VA. Therefore, the OIG determined that testing OIG devices managed by VA was sufficient for meeting the audit objective and would produce the same results as testing VA devices.

provides policy and procedures for securing VA mobile devices that can be connected to the VA network or used to store or transmit VA data.

According to VA Handbook 6500.10, mobile devices have the potential to synchronize with other systems, putting VA's data at risk of being stored in an unsecured location outside of VA's control or of transmitting malware from device to device. The handbook also states that VA will use blacklisting to block cloud-based applications and applications with known vulnerabilities. NIST Special Publication 800-124, Revision 1, recommends federal agencies use blacklisting. According to Special Publication 800-124, Revision 1, organizations deploying mobile devices should consider the merits of each security service, determine which services are needed for their environment, and then design and acquire one or more solutions that collectively provide the necessary services. While VA Handbook 6500.10 requires blacklisting, OIT instead uses training as a mitigating control to prevent users from downloading non-VA-approved applications and entering VA data into these applications, according to a Tier IV administrator.

According to OIT's director of mobile technology and endpoint security engineering, OIT decided not to implement blacklisting due to the workload associated with vetting applications. In VA's chosen vendor environment of Apple iOS, there are a multitude of available applications. According to the director, Apple iOS devices require administrators to use supervised mode to enforce blacklisting. To enforce supervised mode, OIT administrators would need to physically connect each individual mobile device to an Apple computer for configuration.[18] Enforcing supervised mode would also require a wide distribution of Apple computers to administrators and would add tasks to the implementation process, which would require more time to issue the device. The Apple application store has over two million applications that require individual validation. OIT would need to individually assess the security risks to VA data of each application according to OIT's director of mobile technology and endpoint security engineering. Administrators would then need to add the applications that were considered high risk to the blacklist in the MDM system. However, OIT has started implementing application-vetting tools that have similar capability to blacklisting, such as AirWatch and Lookout, according to the director.

In September 2018, OIT awarded a contract to Lookout for a new application-vetting tool that will work with the AirWatch enterprise mobility management tool.[19] Lookout contains application-vetting and scanning capabilities that interact with applications upon installation and assess any associated risks. According to OIT's director of mobile technology and endpoint security engineering, if there is a risk to VA, the application will be removed. The application-vetting tool will provide a similar control to blacklisting and will be automated. As implementation of Lookout was not complete during our on-site review, the audit team did not

[18] Supervised mode allows administrators to centrally manage and control Apple iOS devices.

[19] AirWatch is the enterprise mobility management tool that allows centralized configuration management.

assess whether the enterprise mobility management tool prevents undesired applications from being installed on a VA-furnished mobile device. According to OIT's director, Lookout is currently going through the authority-to-operate process with AirWatch.

Mobile Device Security Training Not Validated

The audit team determined security training for VA-furnished mobile device users is not being validated. The former acting assistant secretary for OIT issued a policy memo, *Security of Apps on iOS Devices Training*, on August 16, 2016, that mandated the completion of annual mobile device security training for all users of VA-furnished mobile devices. According to the memo, the training, *Mobile Training: Security of Apps on iOS Devices (WBT),* can be found on the Talent Management System. According to a Tier IV administrator, OIT does not validate whether this specific training is being accomplished. According to both OIT's director of mobile technology and endpoint security engineering and a Tier IV administrator, training is enforced at the local level but not validated before account creation.

Users of VA-issued mobile devices must also complete the *VA Privacy and Information Security Awareness and Rules of Behavior* training before receiving the device and must refresh their training each year. According to VA, the completion of this annual training meets the recertification requirement for users of VA-issued mobile devices. However, the audit team found the information security awareness training is not consistent with the 2016 policy memo. For example, the security awareness training does not specifically address the security of applications on iOS devices. The security awareness training does not state that downloading unapproved applications on VA mobile devices is prohibited. Furthermore, OIT has no way to validate the effectiveness of annual information security training because OIT staff cannot check to see what applications users have installed from Apple's application store for mobile devices that are not in supervised mode.

Configuration Management Tools Not Used

The audit team found VA does not use configuration management tools to control and automate updates for its mobile devices and applications. According to OIT's director of mobile technology and endpoint security engineering, OIT decided not to use configuration management tools, as with blacklisting, due to the workload associated with using supervised mode. Instead, OIT is relying on mobile device users to manage updates of their applications and operating systems. This process can lead to premature or late updates, unusable applications, or lingering security vulnerabilities. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support their missions. According to FISCAM, effective configuration management prevents unauthorized changes to information system resources, such as software programs and hardware configurations, and provides reasonable assurance that systems are configured and operating securely.

VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, requires that OIT centrally test updates on inactive systems prior to deployment. This is necessary to ensure that OIT fully understands the impact of configuration updates and that the loss of security protection resulting from changes to risk status is mitigated. VA Handbook 6500.10 also requires that VA use an MDM system to centrally install, update, and remove applications and notify users of noncompliance. The MDM system must also automate removal of access features of the mobile device, which will severely limit the user's ability to leverage the device. Configuration management tools centrally control and automate patch and remediation updates. Enforcing configuration management of devices uses supervised mode in the same manner as blacklisting.

Reliance on Users for Configuration Management

Without centralized management of mobile devices, responsibility for configuration management falls on local chief information officers and system administrators, who rely on users for initiating updates of their devices. OIT uses emails to notify users not to install updates upon release and when applications or updates are approved for installation. Approved operating systems have been tested by OIT to confirm they perform correctly. Prior to the iOS 12 update, the audit team found that notifications from OIT advising users not to update applications and devices were sent after users had experienced issues as a result of installing updates. However, with the iOS 12 update, OIT did notify users before release that updating would impact applications. The audit team also assessed OIT spreadsheets showing mobile device inventory lists to identify the presence of unapproved operating systems. The audit team found 12,298 out of 50,618 mobile devices had unapproved operating systems.

NIST Special Publication 800-53A, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires that organizations identify, report, and correct system flaws and test software and firmware updates related to remediation for effectiveness and side effects before installation. According to OIT's director of mobile technology and endpoint security engineering, OIT awarded a contract to AirWatch for a follow-on enterprise mobility management tool that will allow centralized configuration management. Also, VA has approximately one-half of its devices in supervised mode, which allows OIT to automatically prompt the device to download the update. The director also stated that for the remaining devices, OIT plans to bring those devices under supervised mode and plans to test with the latest iOS 12 update.

Conclusion

The audit team found OIT is not using blacklisting, configuration management tools, or validating mobile device training for security of applications. Instead, OIT is using training as the only mitigating control to prevent users from downloading non-VA-approved applications and entering VA data into these applications. OIT is also relying on mobile device users to

update their applications and operating systems. Furthermore, OIT is not validating whether required mobile device training is being completed.

Recommendations 1–3

1. The OIG recommended the assistant secretary for the Office of Information and Technology enforce blacklisting or formally assess and document the approach of using training as the mitigating control to prevent users from downloading and using non-VA-approved applications.
2. The OIG recommended the assistant secretary for the Office of Information and Technology use configuration management tools to prevent premature or late updating of mobile devices or develop proactive policies and procedures to ensure users do not update mobile devices and applications until after the mobile device management team has conducted testing.
3. The OIG recommended the assistant secretary for the Office of Information and Technology validate that users of mobile devices are completing the required annual *Mobile Training: Security of Apps on iOS Devices* before user accounts are activated.

Management Comments

The principal deputy assistant secretary for information and technology and deputy chief information officer concurred with Recommendations 1−3. In response to Recommendation 1, the principal deputy assistant secretary stated OIT is working on two approaches. The first approach is to deploy the Lookout application to VA mobile endpoints. The Lookout application is a technical solution that will ensure mobile applications are not malicious. The second approach is to implement a process to ensure mobile users are trained in appropriate and inappropriate use of VA sensitive data applications prior to receiving mobile devices.

In response to Recommendation 2, the principal deputy assistant secretary stated OIT is working to transition all mobile devices to supervised mode. OIT can delay operating system updates for a maximum of 90 days for mobile devices in supervised mode. However, OIT cannot indefinitely prevent application updates due to the Apple App Store model. According to the principal deputy assistant secretary, application updates provide functional changes and security updates. For VA specific applications, OIT will implement a process to look for any updates, test, and confirm there are no issues. If issues are identified, a bulletin will be released to all mobile users to refrain from updating until the issues are resolved. The principal deputy assistant secretary reported that OIT will provide target completion dates and additional details on corrective actions for Recommendations 1 and 2 when they respond to the OIG's 90-day follow-up memorandum.

In response to Recommendation 3, the principal deputy assistant secretary stated VA will fully implement a process by June 30, 2020, to ensure mobile training is provided before users receive devices.

OIG Response

The corrective actions planned by the principal deputy assistant secretary for information and technology and deputy chief information officer are responsive to the intent of the recommendations. The OIG will monitor implementation of planned actions and will close the recommendations when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the responses from the principal deputy assistant secretary is included in Appendix B.

Appendix A: Scope and Methodology

Scope

The audit team performed this audit from May 2018 to August 2019 to determine whether OIT has implemented policies and procedures to mitigate information security weaknesses associated with mobile devices being used in VA's network infrastructure. Specifically, the audit team focused on VA mobile devices, the mobile device manager, and mobile enterprise service applications that are within the VA infrastructure for proper authentication, backup, restoral, device protection, account management, and update and configuration management. NIST Special Publication 800-124, Revision 1, defines a mobile device as being small with network access but not having a full desktop or laptop operating system.

Methodology

To achieve the objective, the audit team reviewed mobile device policies, configurations, and risk assessment documentation and also interviewed officials from OIT's Information Technology Operations, Office of Cyber Security, identity management team, and contracted help desk. Mobile device policies and configurations were obtained from the OIT's Information Technology Operations mobile device team. Risk assessment documentation was compared with the Governance, Risk, and Compliance RiskVision System. VA mobile device policies were compared to NIST and OMB guidelines and standards.

The audit team interviewed administrators and observed their interaction with the MDM and enterprise service delivery systems. The audit team also interviewed the director of mobile technology and endpoint security engineering, who was responsible for operations of the mobile device environment, and OIT's acting director of the Office of Cyber Security, who was responsible for validating the reasonableness of the security approach used by the mobile technology team. In addition, the audit team conducted interviews with trainers and the contracting officer's representatives responsible for ensuring administrators were properly trained to provide support. Furthermore, the audit team interviewed the senior technical lead for the identity management team, who provides authentication and validation services for mobile devices used in VA.

Fraud Assessment

The audit team assessed the risk that fraud, violations of legal and regulatory requirements, and abuse could occur during this audit. The audit team did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The audit team obtained computer-generated items for this audit. Specifically, the team obtained spreadsheets from OIT showing device inventory lists. The team also obtained several OIT information security documents. To test for reliability, the audit team determined whether any data were missing from key fields, included any calculation errors, or were outside the time frame requested. Further, the audit team compared the information security documents to those maintained in the VA's Governance, Compliance, and Compliance RiskVision System. Testing of the data disclosed that they were sufficiently reliable for the audit objective.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on audit objectives. The OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

Appendix B: Management Comments

Department of Veterans Affairs Memorandum

Date: September 18, 2019

From: Principal Deputy Assistant Secretary for Information and Technology and Deputy Chief Information Officer (005A)

Subj: OIG Draft Report, Audit of VA's Information Security Management of Mobile Devices – Project Number 2018-04608-DV-0001

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

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, *Audit of VA's Information Security Management of Mobile Devices* (Project No. 2018-04608-DV-0001). The Office of Information and Technology (OIT) concurs with the OIG's findings and recommendations and submits the attached written comments. For questions regarding OIT's comments on the draft report, please contact Martha Orr, Deputy Chief Information Officer for Quality, Performance, and Risk at (202) 461-5139.

(Original signed by)

Dominic Cussatt

Attachment

Enclosure

Department of Veterans Affairs (VA) Comments to
Office of Inspector General (OIG) Draft Report,
VA's Information Security Management of Mobile Devices
(Project No. 2018-04608-DV-0001)

OIG Recommendation 1: The OIG recommended the Assistant Secretary for the Office of Information Technology enforce blacklisting or formally assess and document their approach of using training as the mitigating control to prevent users from downloading and using non-VA approved applications.

Comments: Concur. The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) is working on two approaches which will address the recommendation. The first approach is a technical solution using the application Lookout to ensure mobile applications are not malicious. Lookout is deployed to VA mobile endpoints. The second approach will be to implement a process to ensure mobile users have the proper training before receiving a mobile device. The mobile training includes information on what activities are appropriate and inappropriate for VA sensitive data applications.

Target Completion Date: VA will provide a target completion date and additional details on the technical and process solutions at the time of the report's 90-day follow-up.

OIG Recommendation 2: The OIG recommended the Assistant Secretary for the Office of Information Technology use configuration management tools to prevent premature or late updating of mobile devices or develop proactive policies and procedures to ensure users do not update mobile devices and applications until after the Mobile Device Management team has conducted testing.

Comments: Concur. OIT can delay Operating System updates for a maximum of 90 days, but this requires that mobile devices are in supervised mode. OIT is working to transition all VA mobile devices to supervised mode. OIT cannot indefinitely prevent application updates due to the app store model that Apple utilizes. These updates provide functional changes, as well as security updates. For VA specific applications, OIT will implement a process to look for any updates, test, and confirm there are no issues. If any issues are identified, a bulletin will be released to all mobile users to refrain from updating the application until the identified issues are resolved.

Target Completion Date: VA will provide a target completion date and additional details at the time of the report's 90-day follow-up.

OIG Recommendation 3: The OIG recommended the Assistant Secretary for the Office of Information Technology validate that users of mobile devices are completing the required annual Mobile Training: Security of Apps on iOS Devices before user accounts are activated.

Comments: Concur. OIT will develop a process to ensure that mobile training is provided to users before they receive a device.

Target Completion Date: VA will fully implement said process by June 30, 2020. VA will provide additional details at the time of the report's 90-day follow-up.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Audit Team	Al Tate, Director Francis Hoang Robin Morse Robert Skaggs Adam Sowells

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Additional Directors

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and 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

OIG reports are available at www.va.gov/oig.