Fairfax County Internal Audit Office

Department of Information Technology
Mobile Device Management Audit
Final Report

March 2019

NOTE: ***Selected sensitive and confidential Airwatch system operational and security information has been omitted from public disclosure, based on the Virginia Freedom of Information Act (FOIA) Va. Code Ann. 2.2-3705.2(14)(b). This information, if disclosed, would subject the County to potential computer network security risks.***

"promoting efficient & effective local government"

Background Information

The Department of Information Technology (DIT) is primarily responsible for the management of County mobile devices. DIT uses Airwatch, a mobile device management software, to help secure and manage mobile devices. DIT enrolls County mobile devices into Airwatch and serves as the County Airwatch system administrator. Airwatch allows DIT to establish mobile device security settings and compliance policies, and generate reports used for monitoring mobile device security and overall device management. There are approximately 3,900 smart phones and 180 iPads issued by the County enrolled in Airwatch. DIT orders and distributes mobile devices for most of the County agencies, based on agency requests and authorizations. Agencies send their requests for mobile devices to DIT Mobility Center and the center orders, receives, and distributes the devices to the requesting agencies/staff. Most of the devices enrolled in Airwatch use Apple iOS platforms.

Executive Summary

Our audit focused on determining whether adequate policies and procedures were established for mobile device management and security. We also focused on determining whether controls were in place to ensure the Airwatch system was properly configured for effective mobile device security. We reviewed the controls over ordering devices, distributing mobile devices, and accounting for lost or stolen devices. Finally, we reviewed controls over Airwatch user access to ensure it was based on a business need and only allowed access rights necessary for staff to perform their job responsibilities. We noted the following areas where internal controls could be strengthened:

- [redacted]

- [redacted]

- Documentation to support the approval and distribution of County mobile devices was inadequate. There was no documentation provided to support the distribution of mobile devices by the DIT Mobility Center for 17 out of 30 transactions tested. Also, no documentation was provided to support the approval or distribution for two of the devices tested.

- There was no documentation provided to evidence that DIT was performing periodic reviews of Airwatch exception reports to monitor mobile devices to ensure County mobile devices were not compromised and were in compliance with security policies established in Airwatch.

- There were no formal written procedures by DIT for the periodic review of Airwatch system users to validate if their system access was appropriate for their job responsibilities, nor was a user access request form used for granting access and documenting access approval. The Airwatch users consisted of 18 system administrators with various access levels. Three of DIT users had the ability to grant access to all application users; configure and change Airwatch device security and management settings.

Scope and Objectives

This audit was performed as part of our fiscal year 2018 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of January 1, 2017, through December 31, 2017. The audit scope included only County mobile devices enrolled in Airwatch, which were subject to DIT oversight. The scope did not include mobile devices not enrolled in Airwatch or enrolled in other mobile device management systems. Therefore, mobile devices used by the Sheriff's Office, and some of the mobile devices used by Fire and Rescue and Police departments were not included in the audit scope. The objectives of the audit were to determine whether:

- Adequate written policies and procedures existed for mobile computing devices.
- There were adequate controls over the request, approval, distribution and enrollment of mobile devices.
- If Mobile Device Management Software (MDMS) configuration settings for mobile devices complied with DIT Information Security Policy and were properly approved.
- There were adequate user access controls for the Airwatch application**.**
- There were adequate controls for tracking lost, stolen or returned mobile devices.

Methodology

Our audit approach included reviews of Information Technology Security Policy 70-05.01, and DIT procedural memorandum to gain an understanding of the management and security requirements for County mobile devices. We interviewed department management and staff responsible for mobile policies and procedures; authorization and distribution of devices; Airwatch system user access; and protection of sensitive or confidential device data. We selected a sample of enrolled devices to test for proper authorization and distribution. We reviewed Airwatch device setting for compliance with County security policy. In addition, we performed user access rights test for sample of Airwatch users to ensure user rights are assigned based on their job responsibilities.

Findings, Recommendations, and Management Response

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. Controls Over Request, Approval and Distribution of Mobile Devices

Controls over approval and distribution of mobile devices issued by the DIT Mobility Center were inadequate. We tested 30 enrolled devices and found that; no request documentation was provided for two of the devices; and Device Responsibility

Statements (DRS) used by DIT as proof of distribution could not be obtained for 17 of the items.
As a result, we could not determine whether the devices were properly disbursed.

Per DIT Procedural Memorandum Mobility, “Agency directors are responsible for approving use of wireless devices by their staff based on the agencies’ business requirements. In addition, DIT *Information Technology Security Policy*, 70-05 01 - Section 2. 8 *User Security,* states that “Agencies should have County employees and contractors sign agreements defining the acceptable use of information systems and information protection requirements to assist in deterring the unauthorized disclosure of County confidential, sensitive, and Internal Use information and mitigating risk to County information systems. “

Improper approval and distribution documentation for mobile devices increases the risk of unauthorized use of devices and the distribution of mobile devices to unauthorized employees. Additionally, failure to obtain signed DRS forms increases the risk that employees are unaware of their responsibilities for use of devices and information security. These could lead to security breaches and waste of county resources.

While DIT has developed an automated process for ordering, approval and distribution of devices that captures approval and distribution information, it was not fully implemented to all agencies/departments. This process has been implemented for only one agency. For all other agencies ordering devices from DIT, there was no formal procedure to document the approval and distribution of mobile devices to county staff. Most of this was done informally through emails to the Mobility Center that may or may not be maintained. The DIT iPhone Order Form is available for ordering mobile phones, but we noted only three agencies used the form. There was no form available for ordering other mobile devices.

Recommendation: To the extent possible, DIT should implement their automated process for ordering, approval and distributing mobile devices. For the agencies/departments in the county where the automated process has not been implemented, a form should be used to request a mobile device. The form should be signed by agency directors or authorized agency telecom contacts to provide written authorization for employees’ use of mobile devices. We recommend DIT consider enhancing the existing iPhone Order form for use to request all mobile devices. The DIT Mobility center should maintain a copy of each device user’s DRS as the user’s acknowledgement of their responsibilities and to document employee receipt of the device. Additionally, a copy of the completed DRS form should be provided to the mobile device user to inform them of their responsibilities.

Management Response: DIT had already built the asset management system at the time of the audit and will complete and go-live in FY 2019. DIT plans to include the DRS statement within the workflow of the ordering form. In concert with the county’s directive to reduce paper processes when possible, DIT will send electronic copies to end users. We note that agencies are authorized and accountable for acquiring devices and paying from their agencies’ budgets. The anticipated completion date is June 1, 2019.

4. Periodic Review of Airwatch Reports

There was no documentation provided to evidence that DIT was performing periodic reviews of Airwatch exception reports to monitor mobile devices. Per discussions with DIT, they informally review exception reports on their screens for potentially threatening situations, such as device inactivity. Additionally, per DIT staff, automated, actionable, compliance policies are configured into the system. However, there was no formal procedure to document this review. Airwatch produced reports that allowed monitoring of mobile devices that were not in compliance with set policies or believed to be compromised.

DIT PM 70-04 Revised, Section 2.4, *Mobile Communication Devices,* states that DIT is responsible for the centralized management of County mobile devices on County provided networks and carrier networks.

Inadequate written procedures on the utilization of Airwatch reports essential to security and overall management of mobile devices increases the risks of device noncompliance with county policies; insufficient tracking of noncompliant devices; devices susceptible to security breaches and viruses; and unauthorized disclosure of confidential or sensitive data.

Recommendation: DIT should document their procedures for review of information/reports provided by the Airwatch system to effectively manage mobile devices, including information/reports used for tracking devices, device compliance and information security. Also, the written procedures should state how often this information should be reviewed (daily, monthly, quarterly, etc.) Some of the information/reports that DIT should consider for regular review are Device Compliance, Device Compromise and Profile Compliance. Controls should be developed by DIT to ensure accountability for the timely performance of these reviews.

Management Response: DIT will create automated reports in conjunction with the already automated compliance policies and develop an internal procedure document as requested. The anticipated completion date is June 1, 2019.

5. User Access Controls

Airwatch application user access controls were not adequate. There were no formal written procedures by DIT for the periodic review of Airwatch system users to validate their system access was appropriate; nor, was a user access request form used for granting access and documenting access approval. The Airwatch users consisted of 18 system administrators with various levels of access. Three DIT users had the ability to grant access to all application users and, configure and change Airwatch device security and management settings.

DIT Security Policy 70-05 01 Section 3.5.2 *Account Administration* states: “Requests for County information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions.”

In addition, the Policy states that “User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Agency Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications.”

Inadequate controls over user access increases the risk of improper, unauthorized system use by unauthorized users. In addition, failure to perform periodic reviews of user access increases the risk of inappropriate system use and unauthorized access to sensitive or confidential system information.

Recommendation: DIT and other agencies with Airwatch system administrator users should establish procedures requiring the appropriate staff to periodically review the Airwatch role based access (RBA) user lists and notify DIT Airwatch system administrators when an employee is terminated, transferred or no longer authorized to use the system. Additionally, a RBA user access request form should be sent to a designated DIT Airwatch system administrator to request RBA access. The user access request form should be signed and dated by the employee’s supervisor, noting the business purpose and any access term limits. The form should be maintained on file by DIT.

Management Response: DIT has this capability in ServiceNow and will extend it to AirWatch. The anticipated completion date is June 1, 2019.