County of San Diego Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

MOBILE DEVICE MANAGEMENT – COUNTYWIDE AUDIT

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Ron Cosey, CGAP

Report No. A15-026

April • 2016

Intentionally Left Blank

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF AUDITS & ADVISORY SERVICES
5530 OVERLAND AVENUE, SUITE 330, SAN DIEGO, CA 92123-1261
Phone: (858) 495-5991

JUAN R. PEREZ
CHIEF OF AUDITS

April 18, 2016

TO: Mikel Haas, County Information Officer
County Technology Office

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: MOBILE DEVICE MANAGEMENT – COUNTYWIDE AUDIT

Enclosed is our report on the Mobile Device Management – Countywide Audit. We have reviewed your response to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Ron Cosey at (858) 495-5679.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:RC:aps

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Damien Quinn, Group Finance Director, Finance and General Government Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of the County of San Diego (County) Mobile Device Management. The objective of the audit was to assess the adequacy of mobile device management practices and security procedures to determine their operating effectiveness.

Background

Mobile device management (MDM) is a term for the administration of mobile devices in the workplace such as smartphones, tablets, laptops and cellular phones. MDM software is a type of security software used to deploy, secure, monitor and manage mobile devices across multiple mobile service providers such as Verizon, AT&T and Sprint, and operating systems such as iOS, Android and Windows. The County contracts HP Enterprise Services, LLC (HP) to administer MDM services via the IT Telecommunications Service Agreement ("The IT Agreement"). HP sub-contracts AT&T to manage these services using an MDM software solution called AirWatch. These services enable AT&T to centrally manage and control mobile devices, platforms and applications from a single unified console. AirWatch deploys configuration policies to County owned and employee owned mobile devices upon enrollment that automatically apply County-defined settings, policies and restrictions, such as encryption and access passcodes.

AirWatch continuously monitors enrolled mobile devices to ensure configuration settings on devices remain compliant with established County policy.

AirWatch has the ability to remotely lock a device if necessary, remotely remove data on the device that has been lost or stolen, and apply profiles that limit the number of incorrect device passcode attempts before removing all data on the device.

At the time of the audit, the County had approximately 3,365 County-owned mobile devices and two employee-owned devices enrolled in AirWatch. These mobile devices managed by AirWatch only had access to emails on the County network from their device, with one exception. When development of the application is complete, employees from the Probation department will also have access to a new mobile application named the Probation Officer Utility & Mobile Application (PUMA) from their device.

The County has a "bring your own device" (BYOD) program that allows employees to enroll employee-owned mobile devices in AirWatch. Employees in the BYOD program must comply with specific operating system requirements, observe the County BYOD policy, and sign the Employee-Owned Device User Consent and Waiver Agreement.

A key aspect of BYOD policies is containerization, also known as "sandboxing". The purpose of containerization is to allow users to manage business data without intermingling it with the user's personal data and applications. Business applications in the "container" can communicate with each other but cannot exchange data with external applications. The container also protects the business data with layered security, including encryption.

Audit Scope & Limitations

The scope of the audit covered FY 2014-15 to current and included a review of:

- IT governance over mobile device management.
- Security controls for mobile device management.
- Mobile device purchases and provisioning.
- Mobile device asset management.
- Mobile device decommissioning and salvage.

Our review included both County-owned and employee-owned mobile devices purchased by County departments and managed by HP through AT&T. County laptops were excluded from the scope of our review since HP purchases and manages the administration and security of laptops under the IT Agreement and are not enrolled in AirWatch.

Five County departments were selected for review using a judgmental sampling approach based on the number of mobile devices in the departments.

- Assessor/Recorder/County Clerk (ARCC)
- Child Welfare Services (CWS)
- Environmental Health (DEH)
- General Services (DGS)
- Public Health Services (PHS).

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

The scope of the review was based on the IT Governance Institute's Control Objectives for Information and Related Technologies (COBIT) related to MDM.[1]

Methodology

OAAS performed the audit using the following methods:

- Reviewed County Administrative polices related to data, mobile devices, and IT security.

[1] COBIT is a framework developed by the Information System Audit and control Association (ISACA) for developing, implementing, monitoring and improving information technology governance and management control practices.

- Reviewed the IT Agreement, Schedule 4.3, Section 4.11 - Mobile Device Management.
- On a sample basis, inspected mobile devices and compared them to department inventory listings to verify accuracy.
- Interviewed sampled department management regarding mobile device procurement, provisioning, and decommissioning processes.
- On a sample basis, inspected County employee termination reports provided by sampled department's DHRO and wireless provider invoices to verify mobile device service disconnection.
- Reviewed and assessed the adequacy of the County's BYOD policy and related consent and waiver agreements.
- Reviewed MDM software configuration profiles for mobile devices to verify County-defined settings, policies, and restrictions.
- On a sample basis, inspected mobile phones for verification of factory reset by departments when devices are de-commissioned.
- Interviewed HP and AT&T personnel regarding operational procedures for administering County mobile devices.
- On a sample basis, inspected Computer Service Request Form (CSRF) submissions and department approvals for mobile devices.
- Reviewed department's salvage procedures for inactive mobile devices.

AUDIT RESULTS

Summary: While the mobile device management practices and security procedures were satisfactory overall, OAAS identified opportunities for improvement in certain areas including governance over mobile device management practices; asset management; decommissioning mobile devices; and IT security controls.

Finding I: **There is No Overall Mobile Device Policy**

While the CTO has developed a BYOD policy for employee-owned devices, there is no overall mobile device policy to provide guidance to departments that manage County-owned mobile devices.

Mobile Device Asset Management Process Needs Improvement – None of the five departments sampled were maintaining a complete and accurate inventory of their mobile devices, because their inventory list excluded inactive mobile phones.

- DEH had an inventory listing of 277 active mobile phones. However, OAAS found 105 inactive mobile phones that were not on the department's inventory listing. Most of the phones were unsecured.

- PHS had an inventory listing of 241 active mobile phones. However, OAAS found 42 inactive mobile phones that were not on the department's inventory listing.

- DGS had an inventory listing of 302 active mobile phones. However, OAAS found 430 inactive mobile phones that were not on the department's inventory listing.

- CWS had an inventory listing of 302 active mobile phones. However, OAAS found two inactive mobile phones that were not on the department's inventory listing. In addition, most of the International Mobile Equipment Identification (IMEI) numbers were inaccurately recorded on the inventory listing due to a processing error.

- ARCC had an inventory listing of 61 mobile devices. However, OAAS found two inactive mobile phones that were not on the department's inventory listing.

Discussions with department personnel revealed that the departments were using the wireless provider's invoice to track their mobile devices. When a device becomes inactive due to an employee transfer or termination, the department notifies the wireless provider to remove the device from the invoice. The departments then stop tracking the device.

County Administrative Manual 0400-05 states that an asset inventory shall be maintained to account for all workstations. A workstation is defined as a computing device (e.g., desktop PC, laptop, tablet, or handheld device) that is pre-configured with a standard operating system, a suite of standard application software, and connected to the County network.

Without a complete list of active and inactive mobile devices, County assets may be susceptible to misappropriation or loss and not properly accounted for.

Mobile Devices are Not Properly Salvaged – Departments were not sure how to properly salvage inactive mobile devices and were not certain if all data was removed from the device when they performed a factory reset. Also, because the devices are County property, there was some confusion whether departments could trade-in devices to wireless providers for credit. As a result, inactive devices that the departments are no longer using or tracking have not been salvaged.

If all data is not removed from an inactive device, an unauthorized person may gain access to and misuse County information on the device.

The Mobile Device Decommissioning Process Needs Improvement – Two of the five departments OAAS tested did not always disconnect wireless service for employees who terminated employment.

- OAAS tested five mobile phones in DEH where the user had terminated employment. Of the five phones tested, four had active wireless service. For three of the four phones, the service was active for three or more months after the employee left the department and the phone had not been reassigned, including one that was active for seven months.

- OAAS tested three mobile phones in PHS where the user had either transferred or terminated employment. Of the three phones tested, one had active wireless service for two months after the change in employment.

In some cases, departments stated that because the wireless provider's invoice was used to track the mobile devices, the service was kept active to facilitate reassignment of the device to future employees.

If the service is not disconnected timely, unnecessary service charges may be incurred.

County Administrative Policy 0400-07 states "If an authorized mobile phone user transfers or terminates employment with the County and their mobile phone will not be reassigned, services should be discontinued immediately".

In addition, two of the five departments OAAS tested did not remove all County and user data from the mobile phones when employees transferred, terminated employment or upgraded their device.

- Of three ARCC's mobile phones OAAS tested, one contained a prior user's emails.

- Of five DEH's mobile phones OAAS tested, one contained text messages, call history and contact information from the prior user who had terminated employment.

Board Policy A-111 requires departments to protect their data. In addition, wiping mobile phones before disposing of them is a general security best practice, which prevents unauthorized access to any sensitive data stored on devices.

Recommendation:

The CTO should coordinate the development of comprehensive mobile device guidance to assist departments responsible for managing the devices. At a minimum, the CTO guidance should address the following:

1. A method of tracking all mobile devices, both active and inactive, other than the wireless provider's invoice.

2. Procedures to salvage mobile devices including the method of removing existing data before salvaging the devices.

Finding II: **The Encryption Security Setting was Not Enabled for All Mobile Devices**

Although AT&T enabled the AirWatch encryption setting for iOS devices, they disabled the same setting for Android devices. Per discussions with the CTO, AT&T was directed to disable the encryption setting on Android devices because the setting was negatively affecting the functionality of the devices.

County Administrative Policy 0400-05 states, "All County portable workstations and devices are to be encrypted, per the County's adopted standard". The policy defines a workstation as a computing device (e.g. a desktop PC, laptop, tablet or handheld device) that is preconfigured with standard operating system, a suite of standard application software and connected to the County network.

If mobile devices are not encrypted, an unauthorized person may be able to access County information if devices are lost or stolen resulting in possible harm to the County, its customers or employees.

Recommendation: To comply with County policy, the CTO should work with HP and AT&T to identify and implement a workable solution for securing the Android mobile devices.

Finding III: **Insufficient Procedures to Ensure Business and Personal Data Are Separated on BYOD Devices**

The CTO was unable to provide documented evidence of containerization to ensure that County data are segregated from employees' personal data on employee-owned mobile phones.

County Administrative Policy 0400-06 states, storing of County information on a privately-owned computer or other device is strictly prohibited.

In addition, the IT Agreement's Section 4.11 states that HP will provide all MDM test services and produce documentation to support the results. Furthermore, it is the County's responsibility to review and approve HP test documentation and results.

Absent containerization, employees' personal applications may access County data and allow users to transfer County information outside of the County's network. In addition, it may allow for unauthorized access to employees' personal information in violation of the user's privacy.

Recommendation: The CTO should ensure that:

1. HP implements one of the container solutions that are available in AirWatch for employee-owned devices.

2. As needed, HP tests that County data cannot be transferred to employees' personal devices and is adequately secured.

3. HP provides documentation of test results.

Finding IV: **Insufficient Procedures to Ensure Compliance with MDM Policies**

Procedures that define HP's responsibility if an AirWatch enrolled mobile device is not compliant with the IT Agreement's MDM policies have not been developed by HP or approved by the County.

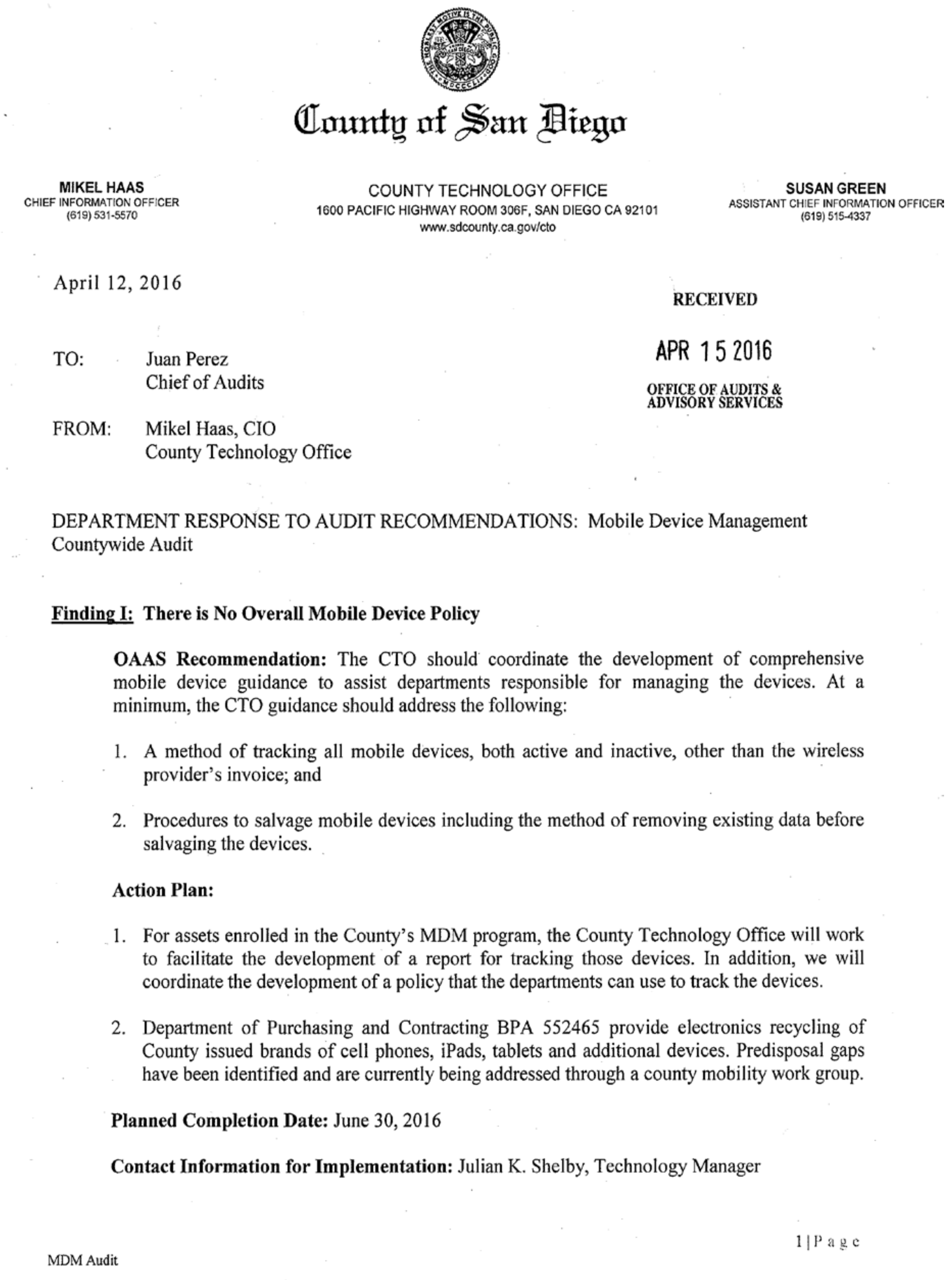
The AT&T Administrator who manages the centralized AirWatch console stated that he was not certain how to handle mobile devices that are out of compliance with MDM policies.

Per the IT Agreement Section 4.11 - Mobile Device Management, HP is required to submit MDM operational policies and procedures including escalation procedures for any mobile device that is not in compliance with MDM policies.

Mobile devices that are out of compliance with MDM policies may be vulnerable to data leakage and unauthorized access.

Recommendation: The CTO should work with HP to develop, document, and implement operating procedures for handling noncompliant mobile devices, including escalation.

DEPARTMENT'S RESPONSE



County of San Diego

MIKEL HAAS
CHIEF INFORMATION OFFICER
(619) 531-5570

COUNTY TECHNOLOGY OFFICE
1600 PACIFIC HIGHWAY ROOM 306F, SAN DIEGO CA 92101
www.sdcounty.ca.gov/cto

SUSAN GREEN
ASSISTANT CHIEF INFORMATION OFFICER
(619) 515-4337

April 12, 2016

TO: Juan Perez
Chief of Audits

FROM: Mikel Haas, CIO
County Technology Office

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: Mobile Device Management Countywide Audit

Finding I: **There is No Overall Mobile Device Policy**

OAAS Recommendation: The CTO should coordinate the development of comprehensive mobile device guidance to assist departments responsible for managing the devices. At a minimum, the CTO guidance should address the following:

1. A method of tracking all mobile devices, both active and inactive, other than the wireless provider's invoice; and

2. Procedures to salvage mobile devices including the method of removing existing data before salvaging the devices.

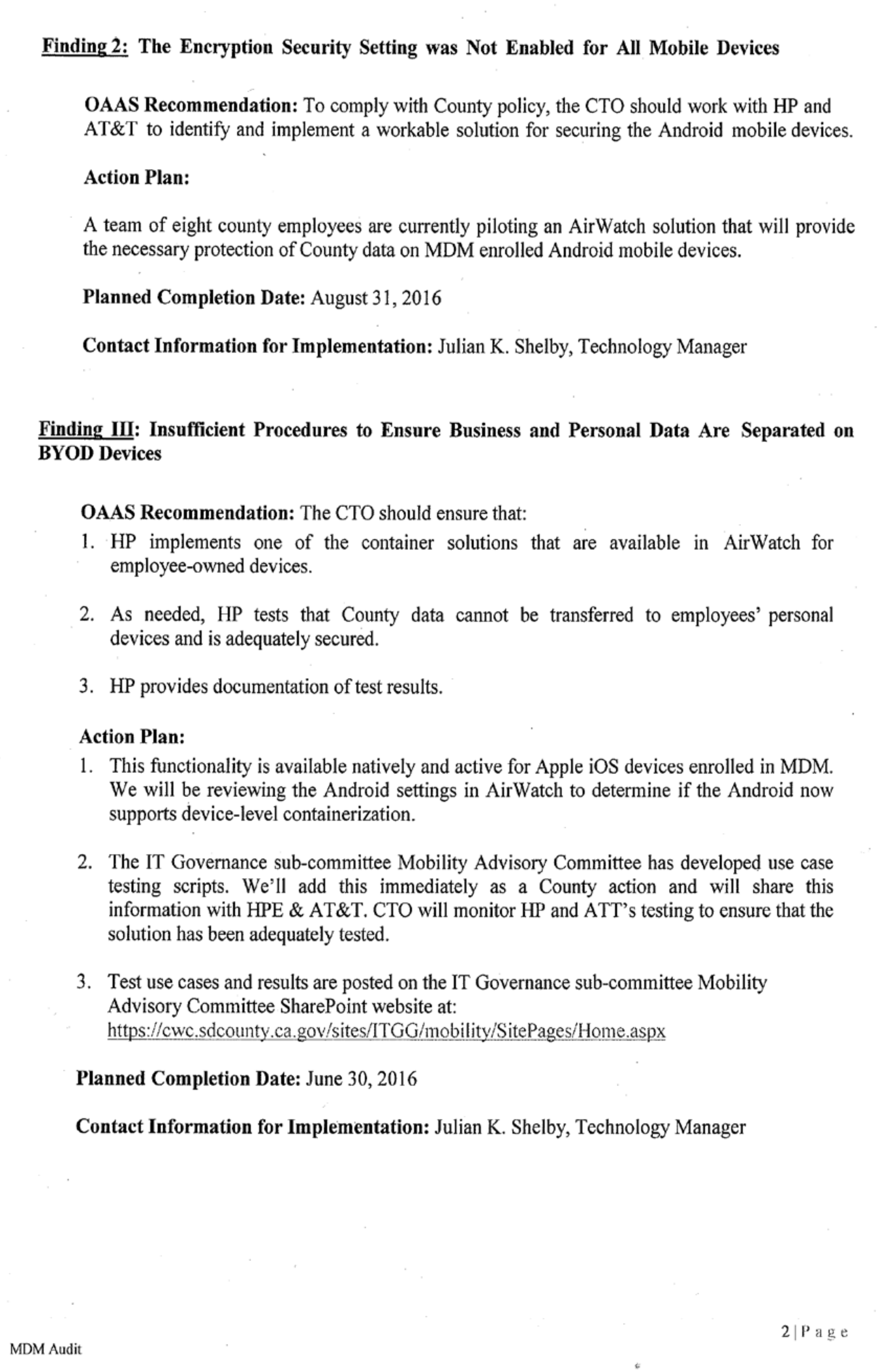
Action Plan:

1. For assets enrolled in the County's MDM program, the County Technology Office will work to facilitate the development of a report for tracking those devices. In addition, we will coordinate the development of a policy that the departments can use to track the devices.

2. Department of Purchasing and Contracting BPA 552465 provide electronics recycling of County issued brands of cell phones, iPads, tablets and additional devices. Predisposal gaps have been identified and are currently being addressed through a county mobility work group.

Planned Completion Date: June 30, 2016

Contact Information for Implementation: Julian K. Shelby, Technology Manager



Finding 2: The Encryption Security Setting was Not Enabled for All Mobile Devices

OAAS Recommendation: To comply with County policy, the CTO should work with HP and AT&T to identify and implement a workable solution for securing the Android mobile devices.

Action Plan:

A team of eight county employees are currently piloting an AirWatch solution that will provide the necessary protection of County data on MDM enrolled Android mobile devices.

Planned Completion Date: August 31, 2016

Contact Information for Implementation: Julian K. Shelby, Technology Manager

Finding III: Insufficient Procedures to Ensure Business and Personal Data Are Separated on BYOD Devices

OAAS Recommendation: The CTO should ensure that:

1. HP implements one of the container solutions that are available in AirWatch for employee-owned devices.

2. As needed, HP tests that County data cannot be transferred to employees' personal devices and is adequately secured.

3. HP provides documentation of test results.

Action Plan:

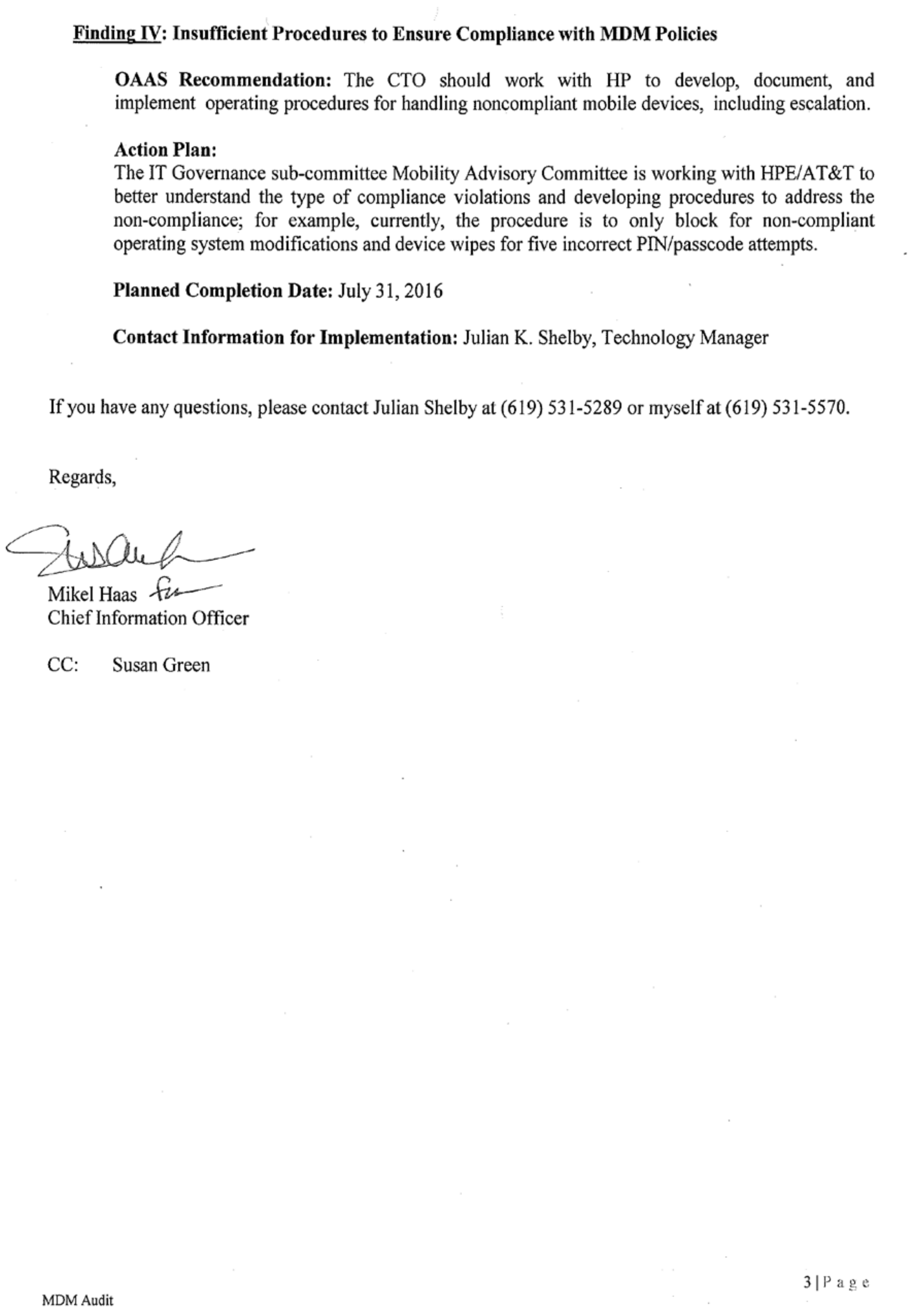
1. This functionality is available natively and active for Apple iOS devices enrolled in MDM. We will be reviewing the Android settings in AirWatch to determine if the Android now supports device-level containerization.

2. The IT Governance sub-committee Mobility Advisory Committee has developed use case testing scripts. We'll add this immediately as a County action and will share this information with HPE & AT&T. CTO will monitor HP and ATT's testing to ensure that the solution has been adequately tested.

3. Test use cases and results are posted on the IT Governance sub-committee Mobility Advisory Committee SharePoint website at: https://cwc.sdcounty.ca.gov/sites/ITGG/mobility/SitePages/Home.aspx

Planned Completion Date: June 30, 2016

Contact Information for Implementation: Julian K. Shelby, Technology Manager



Finding IV: Insufficient Procedures to Ensure Compliance with MDM Policies

OAAS Recommendation: The CTO should work with HP to develop, document, and implement operating procedures for handling noncompliant mobile devices, including escalation.

Action Plan:
The IT Governance sub-committee Mobility Advisory Committee is working with HPE/AT&T to better understand the type of compliance violations and developing procedures to address the non-compliance; for example, currently, the procedure is to only block for non-compliant operating system modifications and device wipes for five incorrect PIN/passcode attempts.

Planned Completion Date: July 31, 2016

Contact Information for Implementation: Julian K. Shelby, Technology Manager

If you have any questions, please contact Julian Shelby at (619) 531-5289 or myself at (619) 531-5570.

Regards,

Mikel Haas
Chief Information Officer

CC: Susan Green