The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver’s government. He also chairs the City’s Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

<table>
<thead>
<tr>
<th>Dennis Gallagher, Chair</th>
<th>Robert Bishop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maurice Goodgaine</td>
<td>Jeffrey Hart</td>
</tr>
<tr>
<td>Leslie Mitchell</td>
<td>Timothy O’Brien, Vice-Chair</td>
</tr>
<tr>
<td>Rudolfo Payan</td>
<td></td>
</tr>
</tbody>
</table>

Audit Staff

<table>
<thead>
<tr>
<th>Audrey Donovan, Deputy Director, CIA, CGAP, CRMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Pierce, IT Audit Supervisor, CISA, CISSP</td>
</tr>
<tr>
<td>Shannon Kuhn, Lead IT Auditor, CISA</td>
</tr>
<tr>
<td>Nicholas Jimroglou, Senior IT Auditor</td>
</tr>
<tr>
<td>Jakki Boline, Senior IT Auditor</td>
</tr>
</tbody>
</table>

You can obtain copies of this report by contacting us at:

**Office of the Auditor**

201 West Colfax Avenue, Department 705 • Denver CO, 80202

(720) 913-5000 • Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at:

www.denvergov.org/auditor
Mr. Frank Daidone, Chief Information Officer  
Technology Services  
City and County of Denver  

Dear Mr. Daidone:

Attached is the Auditor’s Office Audit Services Division’s report of the audit of Mobile Devices. The purpose of the audit was to assess the economy and efficiency of mobile device management and administration, and to assess the effectiveness of internal controls used by Technology Services to manage mobile devices with access to City systems and data.

We examined Technology Services’ mobile device policies and procedures, provisioning and de-provisioning mobile device access to City computer resources, mobile device management software configurations, and the propriety of payments for wireless services.

We identified several areas related to Information Technology Governance where controls need to be improved. Our recommendations address improvements to policies and procedures, enhancements to mobile device security, increased monitoring of payments for wireless services and software licenses, and more effective use of existing monitoring tools.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5000.

Sincerely,

Dennis J. Gallagher  
Auditor

DG/rp

cc: Honorable Michael Hancock, Mayor  
Honorable Members of City Council  
Members of Audit Committee  
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer  
Ms. Janice Sinden, Chief of Staff  
Mr. David P. Edinger, Chief Performance Officer  
Mr. Scott Martinez, City Attorney  
Ms. Beth Machann, Controller  
Ms. Janna Young, City Council Executive Staff Director  
Mr. Stephen Coury, Chief Information Security Officer  
Mr. L. Michael Henry, Staff Director, Board of Ethics  
Mr. Alena Gouveia, Manager of IT Governance  

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people.  
We will monitor and report on recommendations and progress towards their implementation.
AUDITOR’S REPORT

We have completed an audit of Mobile Devices. The purpose of the audit was to assess the effectiveness of internal controls used by Technology Services to manage mobile device usage and access to City systems and data.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, 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.

The audit found that the City does not have an adequate mobile device management governance structure in place to ensure the: 1) security of sensitive information stored on mobile devices, 2) propriety of payments for wireless services, and 3) effective use of software used to manage mobile devices. This report makes a number of specific recommendations that will strengthen the governance surrounding these issues and ensure that mobile devices are effectively and economically managed.

We extend our appreciation to Technology Services and the personnel who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CRMA
Director of Audit Services
Background

Mobile devices are wireless portable devices that allow users to access data and information on the City's network. Cell phones, smart phones, and tablets are all mobile devices. The City hosts nearly 3,000 smart phones and more than 500 tablets for business use. The wireless voice and data usage budget for mobile devices managed by Technology Services is $1.3M for 2014.

Purpose

The purpose of the audit was to assess the effectiveness of Citywide mobile device administration and management, including determining whether: 1) performance measures are developed, implemented, monitored, and aligned with best practices; 2) mobile device access provisioning and de-provisioning is effectively performed; 3) security requirements are enforced; 4) lost and stolen devices are disabled and City data is deleted; and 5) wireless service payments are monitored and appropriate.

Highlights

The audit found that improvements need to be made to the City's mobile device management governance with regard to financial monitoring, mobile device administration, and effective use of technology. Specifically we identified the following:

- Technology Services could improve efficiency and security by:
  - Providing training and using the security features available in the City's mobile device management software
  - Removing City data from devices that are lost, stolen, or belong to former employees
  - Incorporating best practices, legal opinions on privacy, regulations and standards into mobile device policies

- Technology Services and agency liaisons could realize cost savings by:
  - Improving monitoring of usage, device inactivity, and payments
  - Reviewing wireless detail reports for accuracy
  - Monitoring under-utilized City-owned devices and suspending wireless service to those devices not being used, where applicable
  - Suspending wireless accounts for terminated employees timely
  - Preventing employees from receiving stipends for business use of personal mobile telephones while concurrently using City-issued mobile telephones
  - Removing unused and former employee devices from the monitoring software to avoid unnecessary license fees
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION &amp; BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>SCOPE</td>
<td>5</td>
</tr>
<tr>
<td>OBJECTIVE</td>
<td>5</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>5</td>
</tr>
<tr>
<td>FINDING</td>
<td>7</td>
</tr>
<tr>
<td>Governance over Mobile Device Management Needs To Be Improved to Increase Security and Reduce Costs</td>
<td>7</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>14</td>
</tr>
<tr>
<td>AGENCY RESPONSE</td>
<td>16</td>
</tr>
</tbody>
</table>
INTRODUCTION & BACKGROUND

Mobile Devices in the City and County of Denver

In a post for Forbes.com, Juniper Networks CEO and presidential appointee to the National Security Telecommunications Advisory Committee, Kevin Johnson, said, “In a world of 7 billion people, there are now 5.9 billion mobile-phone subscribers. Here in the U.S., we have more mobile-phone subscriptions than people. The mobile Internet that we’ve come to rely on — for everything from financial transactions to business operations to emergency-response procedures — is increasingly vulnerable.”

This perspective underscores the importance of mobile device security for all organizations, including the City and County of Denver.

The City and County of Denver’s Mobile Device Policy defines mobile devices as wireless portable devices that allow users to access data and information on the City’s network. Cell phones, smart phones, and tablets are all mobile devices. The City and County of Denver has more than 3,000 mobile devices in use by employees, as shown in Figure 1.

Figure 1: Number of Mobile Devices Used by City and County of Denver Employees

Source: Created by Audit Services Division Staff.

---

City Mobile Device Governance

Within the past year, Technology Services has implemented a shared service model for managing mobile device use. While Technology Services administers and monitors payments to wireless carriers, responsibility for adding and suspending wireless service, as well as monitoring the propriety of mobile device use, lies with City agencies. Agency liaisons have been appointed in each agency to work with Technology Services, receive and monitor reports from the City’s wireless rate-plan analysis vendor, and order or suspend wireless service for employees.

Technology Services has set up processes and forms for provisioning and de-provisioning mobile devices. Most forms are available on the City's Intranet site, Denver.One.Team (DOT). The forms related to mobile device provisioning and de-provisioning are the Financial Options Form and Computer User Request Form. The Financial Options Form is used by the expending authority in an agency to request mobile device access for City-owned and personal devices. It is also used to process a stipend request through Technology Services and Payroll. The Computer User Request Form is used when an agency needs to add or remove employee access to City information resources upon hire or termination. The form includes directions to agency liaisons to collect former employee badges and equipment.

Bring Your Own Device Programs

Many employers, including the City and County of Denver, have elected to embrace the concept of Bring Your Own Device (BYOD) within the workplace. Gartner, a leading information technology research and advisory firm, defines BYOD as an alternative strategy allowing employees, business partners, and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. A 2012 Gartner study found that 70 percent of corporate respondents already have, or are planning to have, BYOD policies in 2013. Employers can realize substantial productivity gains by embracing BYOD. A CIO magazine article reporting on a Cisco Systems survey states, “Cisco attaches dollars to these extra minutes of work afforded by BYOD. A comprehensive, well-
designed BYOD program can lead to an annual increase of $1,650 per employee.\textsuperscript{5} The City and County of Denver’s BYOD program allows employees to purchase any mobile device they choose and connect it to the City network to gain access to City resources such as email and calendars. BYOD is convenient for employees since they can use one device for both personal and work needs. Technology Services does not track how many employees participate in the City’s BYOD program and that information is not readily available.

Employees who use their personal devices for substantial business use can receive a stipend for reimbursement. An approved Financial Options Form must be submitted to Technology Services and be routed to Payroll to activate the reimbursement.

**Mobile Device Risks in the Workplace**

As with all information technologies, there are risks associated with the use of mobile devices in the workplace. Many mobile device risks relate to sensitive enterprise data being compromised, especially data that is protected by rules and regulations such as the Criminal Justice Information Services (CJIS) Security Policy and the Health Insurance Portability and Accountability Act (HIPAA). Some protected and personally identifiable information could be used for nefarious purposes. Management can reduce the risk of unauthorized access to sensitive data through a sound governance structure by providing policies, standards, procedures, staffing, and training for mobile device administrators and users.

There are also financial risks associated with the use of mobile devices in the workplace. In its Audit of Mobile Device Management and Accountability, the Office of the Multnomah County Auditor in Oregon reported that more than $300,000 was spent in one year on mobile device data and voice plans for unused mobile devices, or for voice and data plan levels that exceeded the business need.\textsuperscript{6}

In addition to financial risks, there are security risks. Mobile devices with outdated software or malware installed could expose the City network to risks. Some mobile device malware copies information about contacts from the mobile device, which could be used to facilitate targeted attacks. Email server settings obtained from a mobile device could be used for unauthorized access to City servers.

Jailbroken or rooted devices allow a mobile device to bypass the factory security settings that have been established by the manufacturer.\textsuperscript{7} This allows an individual to bypass built-in security restrictions so that unauthorized applications can be installed. Users that jailbreak, root, or otherwise modify their device’s operating system expose the mobile device to threats. Additionally, security features that are often used by mobile

---


\textsuperscript{7} Jailbreaking (iPhone) or rooting (Android) is a device hack that provides users with unrestricted access to the entire file system of their mobile devices.
device management software (e.g., remote wiping and password enforcement) can be disabled by a jailbroken or rooted device.

Mobile Device Management Tools

There are a number of mobile device management (MDM) tools available in the marketplace that enforce password and encryption requirements, and allow information security personnel to detect issues with mobile devices and remotely wipe data when devices are compromised. The City selected a cloud-based MDM software package in 2012 that has features to filter websites, enforce City information security, warn administrators and users of risky applications or malware, suspend mobile devices not compliant with City security policy, and remotely remove City data in the event that the mobile device is lost, stolen, or the individual is no longer employed by the City.

Mobile device management tools can remotely wipe data and detect devices that pose a threat to City data. Remote wipe is a security feature that allows an administrator to send a command to a mobile device and delete data. A remote wipe may either delete data in selected folders or delete all data from the device, which would contain both personal and City data. The ability to remotely wipe a mobile device allows administrators to maintain control of City data. Once an individual is no longer employed with the City, or if a device has been lost or stolen, that device can be remotely wiped.

Privacy and Practical Considerations

Thirty years ago when the first mobile telephone was released to consumers, it had one main function: to provide a handheld portable device with which to place voice calls. Since then the mobile telephone has evolved into a handheld personal computer that also happens to include telephone functionality, thus adopting the name “smartphone.” These devices are capable of storing enormous amounts of personal information including pictures, videos, and much more. While employees may find it convenient to have both personal and work data on the same device, there are a number of privacy and practical considerations that must be weighed to effectively implement a BYOD program within an organization. For example, policy writers need to consider what might be the impact to an individual’s personal information in the event the City needs to wipe all data from an employee’s device for security or other reasons.
SCOPE

The audit assessed the efficiency and effectiveness of mobile device governance including: administration, policies and procedures, guidelines, and logical access to systems and data through mobile devices. For logical access, the audit focused on the City-issued and personally owned cell phones and tablets, and configuration of mobile device security within the City’s MDM software.

In accordance with Generally Accepted Government Auditing Standards (GAGAS) the reader should be aware that some details about information security weaknesses are considered sensitive security information and are not disclosed within this report. The details of all findings, however, have been presented to Technology Services management. As part of our regular follow-up for audit issues, we will return at a future date to ensure that all findings have been addressed.

OBJECTIVE

The objective of this audit was to assess the effectiveness of administration and management of mobile devices by Technology Services and agency representatives. Audit objectives also included determining the propriety of payments for City-owned mobile devices, data, and voice plans.

METHODOLOGY

To assess risks associated with MDM at the City and County of Denver, we used a variety of audit methodologies.

- Created queries in the enterprise system of record to identify terminated and current employees, vendors, and payments for testing
- Interviewed agency staff to understand City mobile device administration and management
- Coordinated with Technology Services to conduct a web-based survey to allow mobile device users Citywide to self-assess their mobile device security awareness
- Consulted best practice standards for information security policies and procedures from sources including:
  - Federal Information System Controls Audit Manual (FISCAM February 2009)
  - The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Criminal Justice Information System (CJIS) Security Policy (CJIS August 2013)
  - National Institute of Standards and Technology (NIST) 800-124
• Reviewed the Chief Information Security Officer’s progress in developing and implementing security awareness training
• Reviewed Technology Services Help Desk requests and existing policies and procedures related to mobile device access provisioning and de-provisioning
• Reviewed relevant audits conducted nationwide, such as the mobile device audits for Multnomah County, Oregon, and the U.S. Department of Homeland Security, and the third-party audit of the City’s MDM software vendor
• Obtained reports from the City’s third-party wireless rate-plan analysis service provider and reviewed mobile device usage for appropriate business use and propriety of payments
• Evaluated the City’s structure and internal controls over the administration of mobile devices, which included reviews of manual and automated controls
FINDING

Governance over Mobile Device Management Needs To Be Improved to Increase Security and Reduce Costs

An effective Technology Services governance structure clearly sets forth expectations for City employees, and includes processes and technologies required to provide secure and cost-effective mobile device administration. However, our audit identified several weaknesses related to the City’s mobile device governance structure. Specifically, we found that improvements can be made to the City’s mobile device governance approach in two areas. First, Technology Services can increase the security of City data on mobile devices by improving monitoring and authorization procedures, strengthening and better enforcing relevant policies, and removing City data from mobile devices that are no longer in use. Second, we identified opportunities for cost savings in a number of areas, including software licenses and wireless plans, processing suspensions to wireless accounts, and ensuring accuracy of wireless payment records.

The City’s Mobile Device Governance Approach Can Be Improved to Increase Security of City Data

We found six specific areas of weakness regarding the security of City data on mobile devices. First, certain information security requirements are not being enforced on mobile devices. Second, mobile devices reported lost or stolen and devices belonging to former employees did not have City data removed. Third, internal threats identified by the City’s mobile device management (MDM) software are not monitored and resolved. Fourth, former City employees with mobile device accounts were identified in the MDM software. Fifth, we identified some mobile devices that were connected to the City’s network but not authorized to access City resources. Sixth, the City’s Mobile Device Policy does not take into account certain federal requirements and standards. By addressing these weaknesses, Technology Services can significantly improve the security of City data as accessed through mobile devices.

Technology Services is not enforcing key security features of the Mobile Device Policy – There are many security features installed on mobile devices direct from the factory. One security feature is the optional use of a passcode that prevents access to a mobile device unless the correct digits are entered. An inactivity screen lock is another security feature that causes a mobile device to “hibernate” after a specified amount of inactivity. To access a mobile device that has been locked due to inactivity, a user must correctly enter the passcode of the mobile device. Auto Wipe is a feature which would render the mobile device useless by removing all data and settings from the mobile device after a number of invalid passcode attempts. A mobile device with MDM software installed allows the City to remove data from mobile devices remotely, and allows enforcement of security requirements and suspension of mobile device access.
when users do not implement required security features. The City’s mobile device policy requires mandatory secure password enforcement and approval for Technology Services to remotely wipe or lock data from the device in the case of loss or theft.

The Auditor’s Office conducted an online survey as part of this audit to gauge security awareness of City employees related to mobile devices. This survey indicated that the majority of the 387 respondents have passcodes and screen lock for inactivity enabled on their mobile devices. Additional security requirements are not implemented on user mobile devices because users are not aware that City policy requires their use. Accordingly, Technology Services should reconfigure the City’s MDM software to enforce security requirements of the Mobile Device Policy.

**Lost or stolen mobile devices retained access to City data** – We found that some mobile devices that were reported as lost or stolen, as well as mobile devices belonging to former employees, did not consistently have City data removed. We selected ten mobile devices reported as lost or stolen by City employees and found that six of them (60 percent) did not have City data removed using the Remote Wipe feature available through the City’s MDM software.

In a white paper touting its MDM software, Route1, Inc. poses the following concern: “When an employee is fired or leaves the Enterprise on their own, retrieving Enterprise data from the personal device becomes an issue. It is unclear if an organization has the right to remotely track or wipe an ex-employee’s personal device. Once fired, an ex-employee is just that: no longer employed by the Enterprise and thus potentially not bound by the Enterprise’s BYOD policy. The legality of this scenario remains in a gray area.”

To enforce compliance with federal Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS) Security Policy regulations, the City must be proactive in removing sensitive and protected data from personal devices of employees separating from the City. This can be accomplished in a minimally invasive manner by containerizing City data and wiping or removing only City data from the personal mobile device. If sensitive City data is not containerized, alternate manual methods should be implemented to avoid costly fines for data breaches. Employee exit procedures could include certifying that all City emails are deleted from the employee’s personal mobile device. Technology Services should remove City data from mobile devices that are lost, stolen, or belong to former employees.

---

9 Containerization is the process of separating City from personal data on mobile devices. It allows Technology Services to maintain control over City data while respecting personal data privacy.
Internal threats identified by the City’s MDM software are not monitored and resolved –

The City’s MDM software has several features that help mitigate security threats if used properly. For example, it can be used for suspending mobile access in the event of a security violation, wiping devices that are lost or stolen or that belong to former employees, warning users with devices that are considered vulnerable to malware, and alerting administrators when suspect activity or features are present on a mobile device attached to the City’s network. However, we found that Technology Services mobile device administrators have not been trained on all of the features available through the software and are not monitoring and remediating security threats as they appear on alerts. We recommend that Technology Services develop, document, and implement procedures for mobile device security incident response.

Former City employee mobile device accounts retained MDM software licenses – When an employee with a mobile device account separates from the City, the device should no longer be connected to the City’s network in any way. To test the effectiveness of separation procedures, we reviewed all mobile device accounts with MDM software licenses. We identified seventy-four mobile device accounts for individuals who are no longer employed by the City. The financial impact of failure to remove MDM software licenses is described later in the report. Additional audit work confirmed that compensating controls prevented these individuals from actually accessing email from their mobile devices. However, had those compensating controls failed, it is possible that the individuals could have accessed email when they were no longer authorized to do so. Since mobile devices for former employees are not wiped, previous email messages are retained on the device. We recommend that Technology Services remove mobile device accounts from the MDM software for former employees.

Some mobile devices were connected to the City’s network without authorization – The City’s Mobile Device Policy requires an approved Financial Options Form to be submitted prior to connecting a mobile device to the City’s network. To assess compliance with this policy, we judgmentally selected a sample of thirty mobile devices with access to the City’s network. We found that eight devices, or more than 25 percent, did not have an authorizing Financial Options Form on file.

Additionally, Technology Services allows users a ten-day temporary connection for mobile devices without approval, which conflicts with the City policy that requires the Financial Options Form to be submitted prior to mobile device connection. This configuration allows users to circumvent the policy process and, as such, does not hold users accountable. Technology Services should comply with the City’s Mobile Device Policy by not allowing mobile device access to City resources before receiving an authorized Financial Options Form. To help enforce this requirement, Technology Services should configure the MDM software to prevent mobile device access prior to approval.

The City’s Mobile Device Policy does not take into account certain federal requirements and standards – We analyzed the City’s Mobile Device Policy against applicable federal standards and requirements, including the Federal Information System Controls Audit

---

10 Malware is malicious software which disrupts computer security or functionality.
Manual (FISCAM), the National Institute of Standards and Technology (NIST), HIPAA, and CJIS. We determined that the policy does not incorporate federal requirements for adequate physical security over mobile devices.

There are a number of legal and privacy issues surrounding the City’s use of a Bring Your Own Device (BYOD) policy. While the City wants to position itself to allow employees access to work resources around the clock, it also has a legal responsibility to protect sensitive and protected data. In the case of HIPAA and CJIS information stored on personally owned devices, TS should inform employees of risks associated with storing protected data on mobile devices. Accordingly, in consultation with the City Attorney’s Office, Technology Services should create a Mobile Device Acceptable Use form that clearly states the City’s rights and responsibilities in protecting its data. The form should clearly inform prospective users that their personal mobile device will have its data remotely removed if Technology Services determines that protected or sensitive data might be compromised.

FISCAM, NIST, HIPAA, and CJIS require periodic formal risk assessments to be documented to guide significant security decisions and facilitate internal control design. Technology Services management has not implemented a formal risk assessment program. Technology Services should perform periodic formal risk assessments for mobile devices.

The City’s Mobile Device Governance Approach Can Be Improved to Achieve Cost Savings

In addition to identifying areas of weakness regarding the security of City data on mobile devices, we also identified five areas where the City’s mobile device governance approach could be improved to achieve cost savings. First, we found that Technology Services is not performing sufficient monitoring to identify potential cost savings available through under-used devices. Second, the City is paying software license fees for devices that are no longer in use. Third, some mobile device bills are still being paid for former employees. Fourth, some employees are inappropriately receiving a stipend for business use of personal devices. Fifth, the City’s MDM software is not being used to its full potential. By remediating these weaknesses, Technology Services can realize cost savings and establish stronger stewardship over resources dedicated to the City’s mobile device technology.

Reports are inadequately monitored to identify potential cost savings – Audit work determined that mobile devices with little or no use are not always disabled, resulting in tens of thousands of dollars in monthly charges that potentially could be avoided.

We analyzed low-use wireless accounts using the City’s third-party wireless analysis portal. The total payments for voice and data plans on these low-use mobile devices were more than $136,000 for the eleven-month period.

Although some of these under-utilized devices are for emergency services and other agencies where it is necessary to keep an unused telephone available, a comprehensive review could result in cost savings for the City. The City’s Fiscal
Accountability Rule 7.1 requires employees to be accountable to the citizens of Denver for the appropriate and prudent use of City funds. Technology Services should provide Agency liaisons with low- and zero-usage information at least monthly and liaisons should suspend under-used wireless accounts to eliminate unnecessary costs associated with inactive or low-usage mobile devices. Technology Services delegated monitoring of mobile device usage and payments to agency liaisons in January 2014. Technology Services plans to host quarterly liaison meetings to communicate concerns and best practices, and to provide zero-usage reports to liaisons.

The City continues to pay for MDM software licenses for mobile devices that are no longer in use – As we reviewed MDM software to determine whether mobile device access was authorized and that only active employees have access to City networks, we determined that unused mobile devices are not removed from the MDM software. Once a mobile device connects to the City network to send and receive email, the MDM software activates a monthly license fee. If a user decides not to continue the service, the monthly fee continues to accrue unless Technology Services removes the device from the MDM software registry. We determined that 416 mobile devices were not removed from the registry resulting in nearly $2,500 in unnecessary license fees. Technology Services should perform periodic access reviews for the MDM software and disable inactive accounts after a specified period of inactivity.

Monthly wireless bills were paid for former employees – We queried the Human Resources system of record to identify individuals no longer employed by the City. We then compared wireless payment details to the list of former employees. We found that wireless payments to vendors continued for several months after some employees left the City. When an employee separates from the City, agency liaisons should collect City-owned mobile devices. However, we identified weaknesses with the process for suspending service with the wireless carrier.

Centralized management of mobile devices is relatively new. The City contracted with its wireless rate plan analysis vendor in June 2013, and agency liaisons were assigned in January 2014. Accordingly, many procedures surrounding centralized mobile device administration are new, and in the process of rolling them out, agency liaisons were not made aware that they must suspend wireless accounts through the third-party application when an employee separates from the City. As a result, payments for mobile devices belonging to former employees totaled more than $2,000 for the six-month period tested. We recommend that Technology Services update the Computer User Request Form on the Denver.One.Team web portal (DOT) to include suspending wireless service when employees leave the City. Periodic reviews should be conducted at least monthly to ensure that wireless plans are not paid for former employees.

Employees received stipend payments for business use of personal phones while concurrently using City-owned devices – During our analysis of wireless payments, we were made aware of an employee who received both a stipend for business use of the individual’s personal mobile device and was assigned a City-owned device. To determine whether there were other instances of this type of dual payment, we queried
the Human Resources system of record and compared employees receiving stipends to wireless payments for City-owned devices. We found that seventeen employees who received a stipend for reimbursement for reasonable business use of their personal mobile telephones were concurrently issued City-owned mobile telephones for business use.

We determined that there was no process in place to identify the occurrence of dual payments. Agency liaisons can request payroll reports from Payroll or the Controller’s Office, which show stipends, and compare them to wireless invoices to detect duplicate payments. We recommend that Technology Services prevent employees from having both a City-owned device and a stipend by reviewing existing Financial Options Forms prior to granting an employee a new financial option for mobile device usage. Agency liaisons should perform monthly monitoring to ensure that employees are not receiving dual payments.

**MDM software is not being effectively utilized to address security and payment monitoring** – The City’s wireless rate-plan-analysis company provides an Internet portal and wireless account analysis for the City’s accounts with AT&T, Verizon, and Sprint. The portal allows designated agency liaisons to order new service or suspend wireless services for employees. The portal also supplies numerous administrative reports for tracking spending trends and mobile device inventory management. The City pays $50 per hour to the wireless rate-plan-analysis provider for its analysis and usage monitoring portal. This equates to between $3,000 - $4,000 per month. We found that Technology Services and agency liaisons are not using the monitoring features available on the portal and, accordingly, the City is not receiving all the benefits for which it is paying.

We sought to determine why Technology Services personnel and agency liaisons are not using the monitoring features and found that, due to Technology Services employee turnover, many of the features identified in the project planning phase for MDM software and wireless usage monitoring were not implemented by Technology Services. Training on the software was not provided by outgoing employees, and new employees were informed of the bare minimum information to keep the software running. Many of the administrative tasks for monitoring mobile devices and wireless usage are in the process of being handed off to agency liaisons, so there has been a gap in monitoring mobile devices and wireless payments.

The City pays a mobile device license fee of $2.23 per mobile device per month for use of its MDM software. This cost is on track to approach $70,000 per year for MDM software license fees. Since implementing this MDM software in 2012, Technology Services has not used most of its features. Table 1 provides a comparison of features existing in software tools used by Technology Services.

Some of the features of the MDM software have not been activated, but if activated could help to enforce City information security requirements. Technology Services should evaluate all MDM software features and
implement those that help enforce City information security requirements. Additionally, Technology Services should provide training to MDM administrators to improve the use and effectiveness of MDM software.

Table 1: Comparison of Features in MDM Software and Existing Utility Software

<table>
<thead>
<tr>
<th>Feature within MDM Software</th>
<th>Existing Utility Software Capabilities</th>
<th>City’s Mobile Device Software Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Existing Software Features</td>
<td>$70,000 Annually</td>
</tr>
<tr>
<td><strong>Product Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to access email on a mobile device</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Remote wipe – Allows data to be remotely erased on a mobile device</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Device passcode lock – Requires a passcode to be used each time a mobile device is accessed</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Password complexity – The strength of a password defined by its length, complexity, and unpredictability</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Containerization – The ability to segregate personal and business data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remotely wipe containerized data – The ability to remotely erase containerized business data so that personal data is not affected</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Blacklist/Whitelist Applications for all devices – The ability to block or allow applications on a mobile device</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Monitor and restrict jailbroken or rooted devices – The ability for MDM software to detect and alert administrators if a jailbroken or rooted device attempted to gain access</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Monitor compliance and security</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Manage and enforce a multitude of security features (e.g., disable WiFi, Bluetooth, and GPS; and block web content)</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Detailed security reports</td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

*Source:* Created by Audit Services Division Staff.
RECOMMENDATIONS

We offer the following recommendations to improve governance over mobile device management.

1.1 Technology Services should revise its Mobile Device Policy to meet information security requirements and modify its procedures accordingly.

1.2 Technology Services should immediately begin removing City data from mobile devices reported lost or stolen and from devices belonging to former employees.

1.3 Technology Services should consider enabling the containerization feature in the MDM software to segregate City data from personal information contained on the same device. This would allow removal of City data while preventing personal data from being wiped.

1.4 Technology Services should develop, document, and implement procedures for mobile device security incident response.

1.5 MDM software administrators should disable mobile device accounts for former employees immediately upon departure from the City to ensure security of City devices and eliminate unnecessary costs associated with the former employee’s mobile device.

1.6 Technology Services should, in consultation with the City Attorney’s Office, create a Mobile Device Acceptable Use form that clearly states the City’s rights and responsibilities in protecting its data. The form should clearly inform prospective users that their personal mobile device will have its data remotely removed if Technology Services determines that protected or sensitive data might be compromised. A signed copy of this form should be retained.

1.7 Technology Services should comply with the City’s Mobile Device Policy by not allowing mobile device access to City resources before receiving an authorized Financial Options Form. To help enforce this requirement, Technology Services should configure the MDM software to prevent mobile device access prior to approval.

1.8 Technology Services should update the City’s Mobile Device policy to include critical requirements of standards. End users who work with protected data need direction on how to protect information on their mobile devices to comply with standards, laws, and regulations. Technology Services should document whether or not it is appropriate for employees who work with protected data to download sensitive information to their mobile devices.
1.9 Technology Services should perform formal risk assessments for mobile devices at least annually.

1.10 Technology Services should provide Agency liaisons with low- and zero-usage information at least monthly. Reviews should include data and voice usage for low, as well as, zero usage. Information obtained from these low- and zero-usage reports should be used to communicate deactivations of mobile devices to eliminate unnecessary costs associated with inactive or low-usage mobile devices.

1.11 Technology Services should perform periodic access reviews for the MDM software and disable inactive accounts after a specified period of inactivity.

1.12 Technology Services should update the Computer User Request Form on the Denver.One.Team web portal (DOT) to include suspending wireless service when employees leave the City. Periodic reviews should be conducted at least monthly to ensure that wireless plans are not paid for former employees.

1.13 Technology Services should prevent employees from having both a City-owned device and a stipend by reviewing existing Financial Options Forms prior to granting an employee a new financial option for mobile device usage. Further, Technology Services should direct agency liaisons to perform monthly monitoring to ensure that employees are not receiving dual payments.

1.14 Technology Services should improve training for agency liaisons to ensure that wireless payment monitoring is performed at least monthly to include a review of wireless payments for accuracy and low usage.

1.15 Technology Services should evaluate all MDM software features and implement those that help enforce City information security requirements. Additionally, Technology Services should provide training to MDM administrators to improve the use and effectiveness of MDM software.
July 24, 2014

Mr. Kip R. Menmott, MA, CGAP, CRMA
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. Menmott:

The Office of the Auditor has conducted a performance audit of Mobile Devices.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on July 2, 2014. This response complies with Section 20-276 (b) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING
Governance over mobile device management needs to be improved to increase security and reduce costs.

### RECOMMENDATION 1.1
Technology Services should revise its Mobile Device Policy to meet information security requirements and modify its procedures accordingly.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Aileen Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1

**Response Introduction**

The Mobile Device Audit highlights the inter-relatedness of security policy, financial controls, privacy concerns, legal considerations, operational procedures, staff training, software configuration, process documentation, and operational oversight.

Addressing the identified issues will require a thoughtful and holistic analysis that will include the input of security specialists, technologists, attorneys, and process owners. The software tools also need to be examined closely to ensure they provide the capabilities to address our security and control concerns.

Page 1 of 8
We will be diligent to develop new policies, processes, and tools to ensure we provide a friendly, yet secure, mobile device environment. Although we can make some short term adjustments, resolving all the issues will require significant time to work out, hence our 2015 target dates.

**Response for 1.1**

Technology Services will revise the City’s Mobile Device Policy to meet information security requirements and adjust our procedures.

**RECOMMENDATION 1.2**
Technology Services should immediately begin removing City data from mobile devices reported lost or stolen and from devices belonging to former employees.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alea Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.2**

Within two months, Technology Services will develop, document, and implement a process to immediately remove City data from lost or stolen devices. Removing data from devices belonging to former employees depends on the complete restructure of the Mobile Device Policy and will therefore be completed by December 31, 2015.

**RECOMMENDATION 1.3**
Technology Services should consider enabling the containerization feature in the MDM software to segregate City data from personal information contained on the same device. This would allow removal of City data while preventing personal data from being wiped.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alea Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.3**

Technology Services will analyze the functionality and cost of the containerization feature in the MDM software to determine whether it will sufficiently meet security requirements while addressing privacy issues.
**RECOMMENDATION 1.4**
Technology Services should develop, document, and implement procedures for mobile device security incident response.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>September 30, 2014</td>
<td>Alexa Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.4**
Technology Services will develop, document, and implement procedures for responding to mobile device security incidents.

**RECOMMENDATION 1.5**
MDM software administrators should disable mobile device accounts for former employees immediately upon departure from the City to ensure security of City devices and eliminate unnecessary costs associated with the former employee’s mobile device.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alexa Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.5**
Technology Services will request a report of terminations from Human Resources to be sent to the Service Desk on a weekly basis. This weekly review of the terminations report will begin by September 30, 2014. The Service Desk will use this report to disable any remaining active mobile device accounts belonging to former employees.

We will automate the de-provisioning process by integrating the MDM software with the account de-provisioning tool by December 31, 2015.
RECOMMENDATION 1.6
Technology Services should, in consultation with the City Attorney’s Office, create a Mobile Device Acceptable Use form that clearly states the City’s rights and responsibilities in protecting its data. The form should clearly inform prospective users that their personal mobile device will have its data remotely removed if Technology Services determines that protected or sensitive data might be compromised. A signed copy of this form should be retained.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.6
Technology Services will consult with the City Attorney’s Office to create a Mobile Device Acceptable Use agreement that informs mobile device users of City information security requirements. This agreement will clearly state the City’s rights and responsibilities in protecting its data, including the right to remotely remove data from the user’s mobile device.

RECOMMENDATION 1.7
Technology Services should comply with the City’s Mobile Device Policy by not allowing mobile device access to City resources before receiving an authorized Financial Options Form. To help enforce this requirement, Technology Services should configure the MDM software to prevent mobile device access prior to approval.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>September 30, 2014</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.7
Technology Services will discontinue the practice of allowing a ten day grace period for mobile device users to submit a signed Financial Options Form. Mobile device access to City resources will be granted upon receipt of the authorized form.
**RECOMMENDATION 1.8**
Technology Services should update the City's Mobile Device policy to include critical requirements of standards. End users who work with protected data need direction on how to protect information on their mobile devices to comply with standards, laws, and regulations. Technology Services should document whether or not it is appropriate for employees who work with protected data to download sensitive information to their mobile devices.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alena Guvetea 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.8**
Technology Services will develop usage guidelines based on applicable standards and requirements.

**RECOMMENDATION 1.9**
Technology Services should perform formal risk assessments for mobile devices at least annually.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>July 31, 2015</td>
<td>Alena Guvetea 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.9**
Technology Services will develop, perform, and document formal risk assessments for mobile device management processes annually.

**RECOMMENDATION 1.10**
Technology Services should provide Agency liaisons with low- and zero-usage information at least monthly. Reviews should include data and voice usage for low, as well as, zero usage. Information obtained from these low- and zero-usage reports should be used to communicate deactivations of mobile devices to eliminate unnecessary costs associated with inactive or low-usage mobile devices.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>January 31, 2015</td>
<td>Alena Guvetea 720-913-4964</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 1.10
Our billing vendor is now providing monthly reports to the agency liaisons containing low and zero usage information. Technology Services will instruct the liaisons to review data and voice usage for low and no usage and work with the end users to determine whether the device should be deactivated. Technology Services will evaluate whether the agency liaisons should be responsible for deactivating the mobile devices and if so, ensure that they are properly trained on deactivation procedures.

<table>
<thead>
<tr>
<th>RECOMMENDATION 1.11</th>
<th>Technology Services should perform periodic access reviews for the MDM software and disable inactive accounts after a specified period of inactivity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree or Disagree with Recommendation</td>
<td>Target date to complete implementation activities (Generally expected within 60 to 90 days)</td>
</tr>
<tr>
<td>Agree</td>
<td>August 31, 2014</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.11
Technology Services will evaluate the MDM software rule that automatically disables accounts after a specified period of inactivity. Technology Services will determine the appropriate timeframe of inactivity and enable the rule upon submitting this configuration change through our change management process.

<table>
<thead>
<tr>
<th>RECOMMENDATION 1.12</th>
<th>Technology Services should update the Computer User Request Form on the Denver One Team web portal (DOT) to include suspending wireless service when employees leave the City. Periodic reviews should be conducted at least monthly to ensure that wireless plans are not paid for former employees.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree or Disagree with Recommendation</td>
<td>Target date to complete implementation activities (Generally expected within 60 to 90 days)</td>
</tr>
<tr>
<td>Agree</td>
<td>September 30, 2014</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.12
Technology Services will modify the Computer User Request form to include deactivating wireless service when employees separate from the City. Technology Services will facilitate monthly reviews by agency liaisons of wireless service accounts to ensure that they do not belong to former employees.
RECOMMENDATION 1.13
Technology Services should prevent employees from having both a City-owned device and a stipend by reviewing existing Financial Options Forms prior to granting an employee a new financial option for mobile device usage. Further, Technology Services should direct agency liaisons to perform monthly monitoring to ensure that employees are not receiving dual payments.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 31, 2014</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.13
Technology Services will establish a process to prevent employees from receiving both a stipend and a city-owned device. The process will include monitoring to ensure that employees are not receiving overpayments.

RECOMMENDATION 1.14
Technology Services should improve training for agency liaisons to ensure that wireless payment monitoring is performed at least monthly to include a review of wireless payments for accuracy and low usage.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>January 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.14
Technology Services will include training for wireless payment monitoring into the quarterly liaison meetings. This training will emphasize the importance of the monthly reviews, provide instructions on how to review the reports for accuracy and low usage, and explain the appropriate processes for following up on issues discovered during the review.
RECOMMENDATION 1.15
Technology Services should evaluate all MDM software features and implement those that help enforce City information security requirements. Additionally, Technology Services should provide training to MDM administrators to improve the use and effectiveness of MDM software.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.15
Technology Services will review the features of the MDM software to determine if the application controls would meet and help enforce City information security requirements. Training will be provided to the all administrators to ensure that they gain the necessary skills to effectively manage the tool.

Please contact Alena Gouveia at 720-913-4967 with any questions.

Sincerely,

Frank Daidone
Chief Information Officer

cc:
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
Ms. Janice Sinden, Chief of Staff
Ms. Beth Machanh, Controller
Ms. Audrey Donovan, City Auditor’s Office
Ms. Shannon Kuhn, City Auditor’s Office
Ms. Jacqueline Bolane, City Auditor’s Office
Mr. Nicholas Junrogoul, City Auditor’s Office
Mr. Stephen E. Coury, Chief Information Security Officer
Mr. Alena Gouveia, Manager of IT Governance