CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Office of the City Auditor

Report to the City Council
City of San José

MOBILE DEVICES: IMPROVEMENTS NEEDED TO ENSURE EFFICIENT, SECURE, AND STRATEGIC DEPLOYMENT

Report 16-11
December 2016

CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Office of the City Auditor
Sharon W. Erickson, City Auditor

December 8, 2016

Honorable Mayor and Members
Of the City Council
200 East Santa Clara Street
San José, CA 95113

Mobile Devices: Improvements Needed to Ensure Efficient, Secure, and Strategic Deployment

Mobile devices (cell phones, smartphones, tablets, laptops, and hotspots) have become necessary tools for employees in the City of San José (City) to perform their jobs, typically for work in remote offices or in the field. Mobile devices enhance workplace flexibility, improve communications, and connect workers to City systems for field reporting or outreach. Rapid enhancements in mobile technologies have also contributed to the complexity, risks, and potential costs of managing mobile devices.

Employees with department-identified business needs can be provided either a City-owned mobile device or a monthly stipend to use a personal device for City business. The City owns more than 4,000 mobile devices, with an estimated cost of roughly $3 million. In addition, wireless services cost at least $670,000 annually, and cellular and data stipends for nearly 500 employees cost roughly $250,000 annually. There is also an unknown number of employees who use their own personal devices for work without a stipend.

The objective of this audit was to assess the cost, usage, and management of the growing number of mobile devices used by City employees in light of rapid advancements in mobile technologies and the City's changing technological needs.

Finding 1: Inventory and Cellphone Stipend Management Policies and Practices Can Be Improved. The City has weak controls on mobile device inventories. There is no central inventory of mobile devices in the City; departments are expected to track and manage the mobile devices utilized by their staff. However, most departments did not keep complete inventories of all mobile devices; when records were maintained, they were not in central locations. To protect the City's significant investment in mobile devices and wireless service, the Administration should require departments to maintain current inventories and label City-owned mobile devices. Furthermore, departments can better manage stipends by considering the cost-effectiveness of individual stipends. City policies surrounding stipends have not changed in many years, and should be updated to reflect current costs and business needs. For example, data stipends require multiple levels of review and authorization which can lead to delays.

Finding 2: The City Should Develop a Mobile Device Policy to Reflect Current Technologies and Business Needs. City policies related to mobile devices are outdated and do not provide an efficient or effective framework to achieve the benefits or address the risks of such devices. With up to 17 policies that can apply to the use of mobile devices by City employees, it can be difficult for City staff to understand their roles in the day-to-day management of these tools. We recommend the City consolidate policies related to mobile devices under a *Mobile Device Policy* that encompasses City-owned and personally owned mobile devices that are used for City business. The policy should clarify staff administrative responsibilities, address potential information security risks, and include user-friendly guidelines. Finally, the policy should allow for limited, incidental personal use of mobile devices similar to the allowance for incidental personal use of City desk phones.

Finding 3: The Process for Ordering Mobile Devices Can Be Streamlined. City policies currently require multiple levels of approval and/or review to order tablets, laptops, and smartphones; however, this may unnecessarily slow the process. Further, City policy directs departments to order the most cost-effective device based on business need, but the laptop and tablet price list, which informs such decision-making, is inaccurate and difficult to find. In some instances, it appears the City pays more than retail for some laptops and tablets. Lastly, though hotspots are ordered and billed through the same wireless service purchase orders as cellphones and smartphones, they are not addressed within the City's policies on mobile device procurement. The Administration can streamline the ordering process by delegating approval authority to departments, developing online approval processes, and updating policies.

Finding 4: IT Should Provide Greater Oversight of Mobile Devices to Address Information Security Risks and Control Costs. Currently, the administration of mobile device security controls and the review of mobile device costs and usage are decentralized, with little oversight by the Information Technology Department (IT). This management structure may not be practical today given the changing technical environment of mobile devices. First, IT should implement mobile device management (MDM) software citywide for devices that pose the greatest information security risks for the City. Second, while most departments review wireless service bills to some extent, current processes are inconsistent and ineffective in identifying significant cost savings; IT should provide oversight and clarify the management structure for controlling mobile device costs and appropriate use. As a result, the City could save at least $189,000 per year in costs and minimize risks associated with inappropriate personal use.

Finding 5: Cross-Departmental Coordination Is Needed to Foster Mobile Strategies Citywide. Currently, several departments in the City are working independently to develop mobile processes and applications to improve City services. Rather than relying on individual initiatives, the Administration should establish an interdepartmental working group to serve as a forum to share mobile solutions and processes and facilitate mobile strategies across the City.

This report includes 16 recommendations. We will present this report at the December 15, 2016 meeting of the Public Safety, Finance, and Strategic Support Committee. We would like to thank the Information Technology Department, the City Manager's Office, the Finance Department, and all other departments for their time and insight during the audit process. The Administration has reviewed the information in this report, and their response is shown on the yellow pages.

Respectfully submitted,

Sharon W. Erickson

Sharon W. Erickson
City Auditor

finaltr
SE:lg

Audit Staff: Joe Rois
Michael Tayag
Ani Antanesyan
Stephanie Noble

cc:
Norberto Dueñas
Rob Lloyd
Julia Cooper
Mark Giovannetti
Kip Harkness
Danielle Kenealey
Kathy Lang
Kara Capaldo
Matthew Loesch
Chris Mills
Jennifer Schembri
Allison Suggs
Rick Doyle
Jennifer Maguire
Dave Sykes

This report is also available online at www.sanjoseca.gov/audits.

Table of Contents

Table of Exhibits

Introduction

The mission of the City Auditor's Office is to independently assess and report on City operations and services. The audit function is an essential element of San José's public accountability, and our audits provide the City Council, City management, and the general public with independent and objective information regarding the economy, efficiency, and effectiveness of City operations and services.

In accordance with the City Auditor's Fiscal Year (FY) 2016-17 Work Plan, we have completed an audit of the City's use of mobile devices. We conducted this performance audit 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. We limited our work to those areas specified in the "Audit Objective, Scope, and Methodology" section of this report.

The Office of the City Auditor thanks the City's Information Technology Department, the City Manager's Office, the Finance Department, and all other departments for their time and insight during the audit process.

Background

Employees of the City of San José (City) use mobile devices (cell phones, smartphones, tablets, laptops, and hotspots[1]) for City business, typically for work in a remote office or in the field. Mobile device benefits include: enhancing workplace flexibility, improving communications, and connecting workers to City systems for field reporting or outreach.

If a department identifies a business need for a cellphone or other device, employees can be provided either a City-owned mobile device or a monthly stipend to use a personal cellphone for City business, whichever is more cost-effective. City policies outline requirements for the authorization of City-issued cellphones and stipends, procurement of laptops and tablets, and information security generally.

For the purposes of this audit, we have defined mobile devices as City-issued laptops, tablets, hotspots, cellphones, and smartphones, as listed in Exhibit 1. We also consider cellular and data stipends, which the City offers to reimburse City employees for the use of personal cellphones and smartphones for City business.

[1] For this report, we refer to various standalone devices designed to provide cellular data connections as "hotspots." These include air cards, USB modems, and personal hotspots.

We excluded from analysis ancillary, single-function devices (such as radios, walkie-talkies, standalone cameras, projectors, GPS, wired routers, modems, e-readers, wearable technology, machine to machine (M2M) sensors and routers, and personal mobile devices used without stipends.

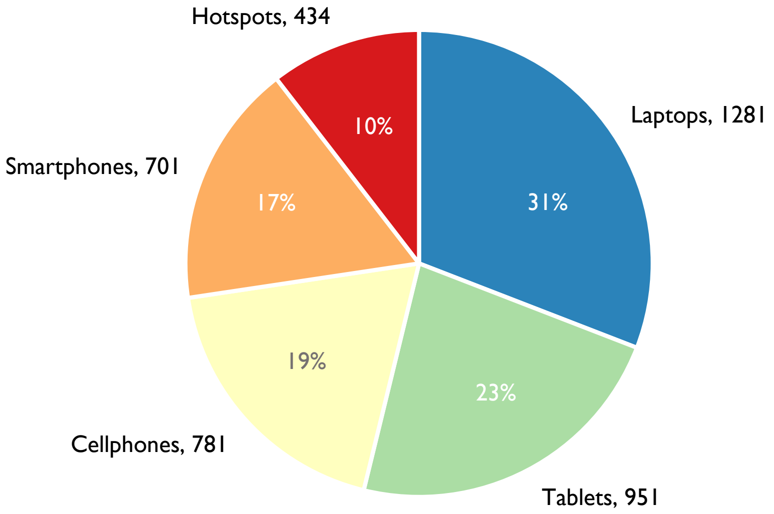
Exhibit 1: Definitions of Mobile Devices

Cellphone	*Portable phone with limited computing power, unable to download and run applications from multiple sources. May have full standard keyboard or touchscreen.*
Smartphone	*Portable computer, designed primarily for telephone conversation, with a full standard keyboard or touchscreen, a limited (non-desktop) operating system, and the ability to download and run applications from multiple sources.*
Laptop	*Portable computer (which may or may not be mounted) with attached, physical keyboard, running a fully-functional desktop operating system. Includes ruggedized laptops (Toughbooks) and Mobile Data Computers (MDCs) used in Police patrol cars.*
Tablet	*Portable computer (which may or may not be mounted) without an attached keyboard, or with detachable keyboard accessory. May be data-enabled to connect to the internet through cellular service, but not primarily designed for telephone conversation. Examples include Apple iPad tablets, Microsoft Surface tablets, and Samsung Galaxy tablets.*
Hotspot	*Single-purpose, portable accessory designed to convert cellular signal into WiFi signal, and typically used to provide internet connection for laptops and non-data enabled tablets.*

Source: Auditor summary based on National Institute of Standards and Technology (NIST) and Government Accountability Office (GAO) definitions

Exhibit 2 shows the breakdown of mobile devices by type across the City based on departmental interviews, invoices, and internal documents. Finding 1 of this report provides more detail on the estimated citywide inventory of devices.

Exhibit 2: Estimated Inventory of Mobile Devices Citywide



Source: Auditor analysis based on invoices, interviews, and internal documents
from June to August 2016

These devices are utilized in a variety of ways across the City. As shown in Exhibit 3, departments commonly use mobile devices for emergency contact, group work, telecommuting, field work, field research, field reporting, communication, community outreach, and recruitment.

Mobile devices enable City employees to work more flexibly and efficiently. Within the Department of Transportation, for example, the sewer, trees and sidewalks, street sweeping, and illegal dumping teams all have devices specially configured for field research and data entry. These field teams have access to City email, documents, maps, customer data, computerized maintenance management systems (CMMS), dispatch, and trees and sidewalk (TWIG) and street sweeping systems. Access to these systems has eliminated the need for data reentry. Using TWIG on a tablet or smartphone, DOT field workers can upload information directly to the City's billing and collections system. They can also manage work orders; upload backup documents, addresses, and contact information; and pull data on property ownership from the City's Application Management and Data Automation (AMANDA) system.

Exhibit 3: Uses of City-Owned Mobile Devices Citywide

	Communication / Emergency Contact	Field Work	Group Work	Business/ Community Outreach	Telecommuting	Recruitment
Airport	✓	✓		✓		
City Attorney	✓				✓	
City Auditor		✓			✓	
City Clerk		✓				
City Manager	✓		✓	✓	✓	
Economic Development	✓			✓		
Environmental Services	✓	✓		✓		✓
Finance		✓	✓		✓	
Fire	✓	✓				
Housing	✓					
Human Resources	✓		✓			
Independent Police Auditor		✓		✓		
Information Technology	✓	✓				
Library	✓			✓		
Parks, Recreation and Neighborhood Services	✓	✓		✓	✓	
Planning, Building and Code Enforcement	✓	✓				
Police	✓	✓				✓
Public Works	✓	✓			✓	✓
Retirement Services		✓			✓	
Transportation	✓	✓			✓	

Source: Interview responses from select department staff

San José seems to be on par with other jurisdictions in terms of mobile device deployment. A 2014 Government Technology/AT&T survey on Emerging Technology Adoption in Local Government found 50 percent of agencies use smartphone and mobile applications, while 26 percent still use voice features only.[2] Furthermore, San José departments have implemented or are implementing projects similar to many of those identified in the 2015 Digital Cities Survey, including mobile field inspections, work order management, and asset control.

[2] "Emerging Technology Adoption in Local Government" Executive Summary, Government Technology, 2014, http://www.corp.att.com/stateandlocal/docs/emerging_technology.pdf.

Various Departments Are Involved in Managing Mobile Devices, Stipends, and Related Processes Citywide

In accordance with City policy, each department is partly responsible for managing its own mobile devices. For example, departments identify the business needs and provide the initial authorization for employees and/or workgroups to receive mobile devices. They also open accounts and lines with wireless service vendors, and directly order network-enabled phones and hotspots from the vendors. Additionally, individual departments are charged with the ongoing management of their mobile devices, including maintaining inventories, paying wireless service bills, and performing annual random reviews of cellphone calls to identify personal use.

In addition to the above duties delegated to all departments, several departments play particular roles in administering mobile device-related business processes citywide:

- The Information Technology Department (IT) is generally responsible for computing and security platforms. It reviews, orders, and configures (upon request) laptops and tablets; approves and establishes remote access on mobile devices; and updates applicable information security policies.
- The City Manager's Office (CMO) approves smartphone purchases and data stipends for employees in job classifications below Division Manager. The newly established Office of Civic Innovation, part of the City Manager's Office, may take on roles related to mobile devices in the future.
- The Finance Department's Purchasing Division (Purchasing) establishes open purchase orders with technology vendors, including wireless service providers. Finance maintains hardcopy records of approved cellphone and data stipends.

The City Has Competitively Bid Laptops and Tablets

All departments in the City, as well as the City Council and Mayor's offices, order laptops and tablets through a central, citywide purchase order with one of four vendors: ComputerLand, TIG, Lehr, and EDX, Inc. Each vendor provides different models, as shown in Exhibit 4. Rather than specify the tablet and laptop models available through the purchase order, IT sets minimum technical specifications, and the vendors determine which models meet those standards. This process is explained in greater detail in Finding 3.

Exhibit 4: Laptop and Tablet Vendors and Brands

Vendor	Laptop/Tablet Brands
ComputerLand	Apple tablets and Microsoft Surface Pro
EDX, Inc.	Samsung Android tablets
TIG	Dell ultraportable and desktop replacement laptops
Lehr	Panasonic semi-rugged laptops

Source: Citywide purchase order matrix

Purchasing initiated the laptop and tablet purchase order in 2015. The purchase order is to be rebid yearly. Departments are required to use these purchase orders, and not allowed to purchase tablets and laptops with procurement cards (p-cards).

The City Participates in Wireless Service Agreements with AT&T, Sprint, and Verizon

To obtain advantageous pricing, the City participates in both state- and national-level master agreements between the National Association of State Procurement Officials' (NASPO) ValuePoint[3] and three wireless service providers—AT&T, Sprint, and Verizon. NASPO ValuePoint creates multi-state contracts to maximize cost avoidance, reduce individual state administrative costs, and encourage market competition and product availability through standard specifications and consolidated requirements. The current agreements run through June 2019.

As part of California's NASPO ValuePoint contracts with AT&T, Sprint, and Verizon, the City can use various discounted voice plans, including a $0.06/minute flat rate plan, unlimited voice plans ranging from $19.99 to $54.99 per month, and unlimited data plans around $38/month (see Appendix A for more details). The City can also take advantage of discounted standard equipment charges, which vary based on the vendor. Currently, the City spends at least $670,000 annually on wireless services for mobile devices.[4]

Prior Audits Have Recommended Mobile Solutions

Past audits have identified ways that departments can improve City services through the strategic use of mobile devices. For example, in 2013, the City Auditor recommended that Code Enforcement review options to replace or enhance its code enforcement database (CES) and include options for mobile units and interfacing with other City databases (Code Enforcement: Improvements are Possible, But Resources Are Significantly Constrained, November 2013), which has

[3] Formerly known as WSCA-NASPO, referring to the Western States Contracting Alliance formed as a subsidiary entity of the National Association of State Procurement Officials.

[4] The City pays additional wireless charges for machine to machine sensors and routers.

been partially implemented as of June 2016. Other open audit recommendations with potential mobile solutions include recommendations related to customer call handling, cash handling, and automated field reporting for auto thefts.

Audit Objective, Scope, and Methodology

The objective of our audit was to assess the cost, usage, and management of the growing number of mobile devices distributed to City employees. We sought to understand the deployment of mobile devices in light of rapid advancements in mobile technologies and the City's own technological needs. We also sought to understand the relevant management controls in place related to mobile device procurement and deployment and performed the following to achieve our audit objective:

- Reviewed sections of the Municipal Code and the City Administrative Manual related to mobile devices.
- Interviewed and surveyed staff in all departments to understand how they procure, manage, deploy, and secure mobile devices and/or cellular and data stipends.
- Solicited and reviewed available departmental policies and procedures related to mobile devices, wireless billing invoices, and mobile device inventories. In a few cases, where departments had an active inventory, we compared inventory assignments to separated employees.
- Reviewed current California NASPO ValuePoint agreements with AT&T, Sprint, and Verizon in which the City participates to understand the terms, pricing, and customer service obligations of the three wireless service vendors.
- Interviewed account managers from Sprint, AT&T, and Verizon to gain insight on the City's account management structure, mobile device plans and pricing, and vendor tools and services.
- Corresponded with customer service representatives from Sprint, AT&T, and Verizon to gain access to cost and usage data associated with City-issued mobile devices, and performed analysis on usage patterns and cost savings using this data.
- Identified high voice, text, and data users through limited testing of three departments. We reviewed their bills to assess whether the level of use appeared appropriate. Based on this review, we identified one case where there appeared to be significant personal use of a City-issued cellphone; we referred this case to the Office of Employee Relations for further investigation.
- Retrieved and analyzed electronic records of cellular and data stipends and a sample of paper authorization forms for cellular and data stipends.

- Reviewed industry reports on mobile device ownership, deployment, and use, including reports from the Pew Research Center and the Center for Digital Government among others.

- Examined the costs and functionalities of various software systems and programs related to data security and telecommunications expense management, including but not limited to AirWatch, Dimension Data, Maas360, ManageMobility, and MobileIron.

- Reviewed best practices related to information security standards and guidelines, including but not limited to:

  Criminal Justice Information Services (CJIS) Security Policy, U.S. Department of Justice (June 2016)

  Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology (June 2013)

  Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged, U.S. Government Accountability Office (September 2012)

  Securing Mobile Devices, Information Systems Audit and Control Association (ISACA) (August 2010)

- Performed gap analysis between information security best practices and the City's current and draft information security policies to identify any gaps in securing mobile devices.

- Benchmarked the City's mobile device management controls with those in other jurisdictions: City and County of Denver, City of Los Angeles, City of Phoenix, City of Portland (OR), City of Oakland, City of Sacramento, City of San Diego, and City and County of San Francisco.

Finding I Inventory and Cellphone Stipend Management Policies and Practices Can Be Improved

Summary

Based on interviews, vendor invoices, and internal documents, we estimate the City owns more than 4,000 mobile devices with an estimated cost of roughly $3 million. To protect this investment, inventory management practices can be improved. Though City policy requires departments to maintain inventories of certain mobile devices and track their assignments, not all departments maintained inventories, and many inventories were incomplete.

Currently, nearly 500 employees receive cellphone or data stipends as an alternative to receiving cellphones at a cost of $250,000 annually. City policies surrounding stipends have not changed in many years and should be updated to reflect current costs and business needs. Additionally, departments can better manage stipends by considering the cost-effectiveness of stipends as opposed to City-issued devices and ensuring stipends are terminated when there is no longer a business need. Finally, the Finance Department, in coordination with the City Attorney's Office, should clarify the rules surrounding taxable and non-taxable stipends.

The City Has More Than 4,000 Mobile Devices with an Estimated Cost of $3 Million

As stated in the Background, the scope of mobile devices for this audit includes cellphones, smartphones, tablets, laptops, and hotspots. The City currently has more than 4,000 mobile devices across departments. Exhibit 5 shows the estimated inventory of City-issued mobile devices as reported by departments and reconciled through available vendor data provided by Sprint, Verizon, and AT&T.

As a general trend, bigger departments tend to have more mobile devices on average per employee than smaller departments. Some departments have pooled devices for use by multiple employees. Exhibit 5 shows the estimated inventory for each department by type of device.

Exhibit 5: Estimated Number of City-Owned Mobile Devices by Department

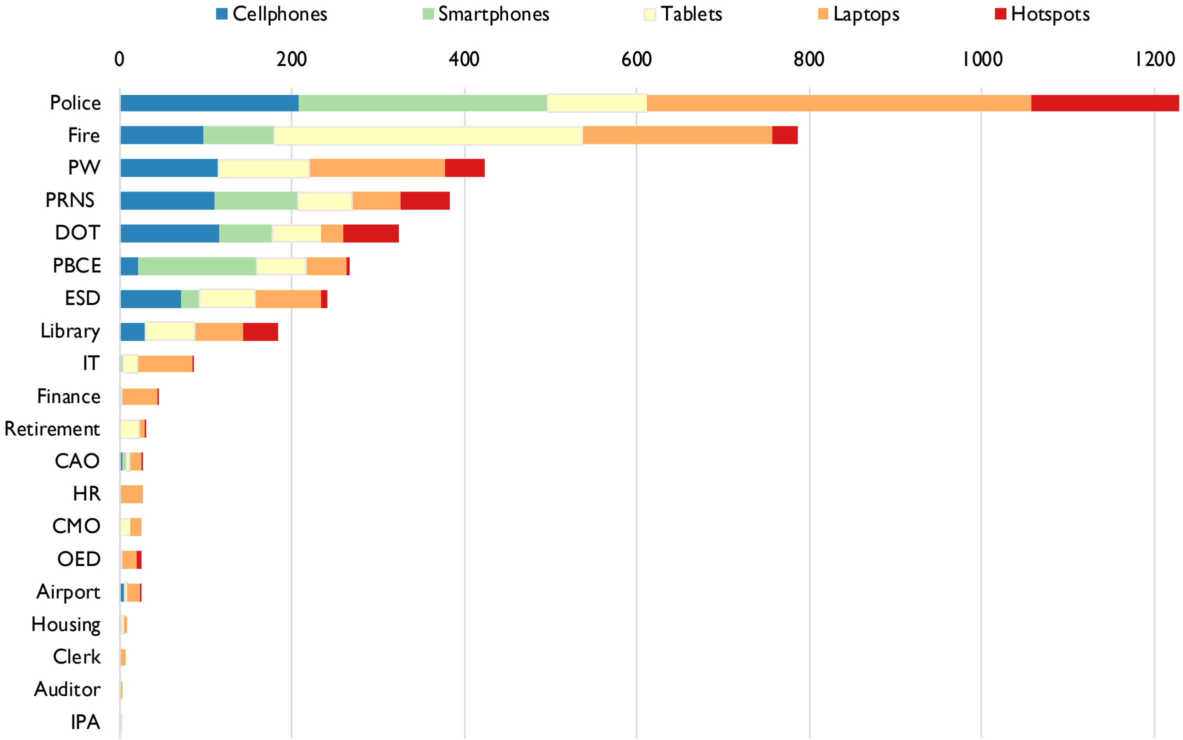
City Department	**Total Inventory**	Cellphones	Smartphones	Tablets	Laptops	Hotspots
Police	**1,228**	207	290	115	446	170
Fire	**787**	98	82	357	220	30
Public Works	**424**	113	1	106	157	47
Parks, Recreation and Neighborhood Services	**383**	111	96	63	56	57
Transportation	**323**	116	61	57	25	64
Planning, Building and Code Enforcement	**267**	21	138	58	46	4
Environmental Services	**241**	72	21	65	75	8
Library	**184**	30	0	58	55	41
Information Technology	**86**	1	4	16	63	2
Finance	**45**	0	0	3	40	2
Retirement Services	**30**	0	0	23	6	1
City Attorney	**28**	4	3	5	14	2
Human Resources	**27**	1	0	1	25	0
City Manager	**25**	0	0	13	12	0
Economic Development	**25**	0	3	1	16	5
Airport	**24**	5	1	3	14	1
Housing	**9**	2	1	3	3	0
City Clerk	**7**	0	0	2	5	0
City Auditor	**4**	0	0	1	3	0
Independent Police Auditor	**1**	0	0	1	0	0
TOTAL	**4,148**	**781**	**701**	**951**	**1,281**	**434**

Source: Auditor analysis based on invoices, interviews, and internal documents from June to August 2016

* Note: Some devices may not be assigned to individual employees or to City staff—for example, some of Retirement Services' tablets are provided to Retirement Board members. Additionally, some devices are specific to vehicles and may be mounted, like the Mobile Data Computers in Police patrol cars.

Police and Fire have the most mobile devices, largely due to their need to equip employees and vehicles with devices that promote fast transmission of information. For instance, the Fire department purchased about 350 tablets in FY 2015-16 that will be installed on fire trucks to support the transmission of patient care data. As shown in Exhibits 5 and 6, departments with large field operations or multiple locations tend to have the next most devices, while centralized, administrative departments tend to have the fewest. Overall, the City had 0.7 mobile devices per full time equivalent (FTE) across departments.

Exhibit 6: Departmental Comparison of City-Owned Mobile Device Deployment



Source: Auditor analysis based on invoices, interviews and internal documents from June to August 2016

As of September 29, 2016, the City list price for tablets ranged between $382.50 and $971.00 per unit; for non-ruggedized laptops, the City list price ranged from $703.55 to $831.05.[5] The Police Department's ruggedized laptops, through the MDC purchase order, cost $3,174.91 per unit.

We estimate the citywide tablet and laptop inventory cost about $2.8 million, based on available invoices from the City's tablet and laptop vendors, departmental inventories, and device replacement costs. Cellphone, smartphone, and hotspot costs are more difficult to estimate because the costs appear as equipment charges on departments' monthly wireless service bill. Based on a range of $0 to $500, cellphone and smartphone costs are estimated to be another $200,000, for a total inventory cost of about $3 million. Cellular equipment and service charges are discussed in greater detail in Findings 3 and 4.

[5] Some of these prices are representative of devices that are configured-to-order, meaning that they may have additional memory or other features needed to meet the City's minimum technical specifications.

Departmental Inventory Controls for Mobile Devices Can Be Improved

The City has weak controls on mobile device inventories. There is no central inventory of mobile devices in the City; departments are expected to track and manage the mobile devices utilized by their staff. However, most departments did not keep complete inventories of all mobile devices; when records were maintained, they were not in central locations.

Although some departments kept active inventories of cellphones and smartphones, these inventories were often based on monthly bills or vendor data, which do not capture physical inventory. For example, a smartphone that has been disconnected from service would not necessarily appear on a bill, and could be excluded from an inventory as a result. This can also be problematic as vendor data was not always updated to reflect turnover or reassignment of phones. In some instances, devices were still assigned to former employees. While most of these devices had been reassigned within the departments, the department inventories had not been updated. At least two departments could not locate a small number of devices that were currently being billed. The departments considered the items lost and disconnected service.

Regarding tablets and laptops, some departments maintained inventories while others did not. More often, larger departments or departments with more mobile devices tended to keep inventories while smaller departments with a few devices did not.

The *Procurement of Laptops and Tablets Policy* (1.7.8) sets inventory requirements for tablets and laptops, stating that:

> *A record should be created and maintained for laptops or tablets purchased in accordance with this policy which includes at the minimum:*
>
> - *The type of device purchased*
> - *The device serial number*
> - *The name of the employee to which the [device] is assigned*
> - *The employee identification number of the employee to which the [device] is assigned*
> - *The date of issue of the device*
> - *The date the equipment is returned (e.g. upon the employee's separation or transfer to a different Department).*

The *Cellular Telephone Policy* (1.7.4) says that departments are responsible for documenting the issuance of cellphones and ensuring that cellphones are returned once the employee changes jobs or is deemed no longer eligible for a City-issued cellphone; however, there are not detailed inventory requirements as in the laptop and tablet policy. Hotspots are not explicitly mentioned in City policies, and few departments kept active inventories of these devices.

Finally, most departments did not label devices to ensure that they can be identified as City property or that asset numbers or device serial numbers are present.

Recommendation #1: To ensure appropriate controls over City-owned mobile devices (including cellphones, smartphones, hotspots, tablets, and laptops), the Administration should require departments to label City-owned mobile devices and maintain current inventories. The inventories should include the type of device, serial number, the name and ID of the employee to whom the device is assigned, the phone number (if applicable), the date of issuance, and the date returned (if applicable).

Nearly 500 Employees Receive Stipends to Use Their Personal Cellphones for City Business, at a Cost of $250,000 Annually

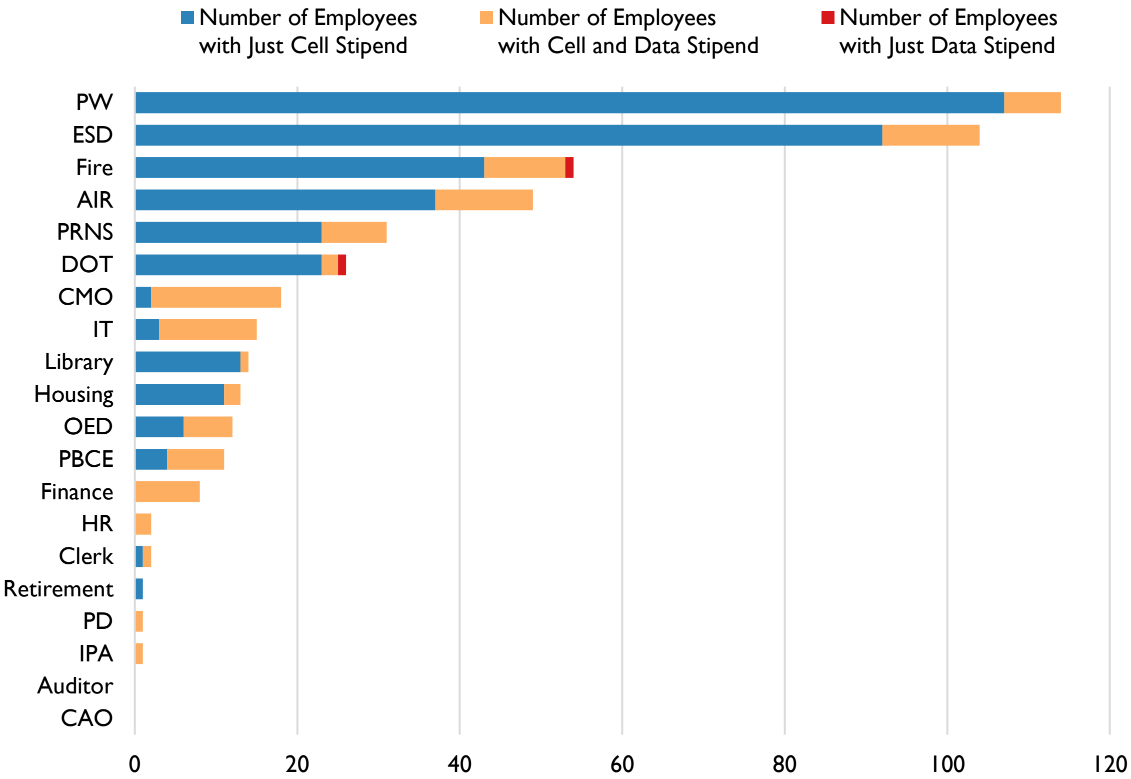
Employees across the City use personal mobile devices for City business. City policy provides for reimbursement in the form of cellphone stipends for voice and/or data to qualifying employees. Currently, nearly 500 City employees receive stipends for using their personal phones for City business.

The current cellphone and data stipends are $35 and $40 per month, respectively. Eligible employees can receive both types of stipends. More than three quarters of employees receive just the cellphone stipend; just over 20 percent, or roughly 100 employees, receive both the cellphone and data stipends.[6] The cost to provide stipends to City employees totals roughly $250,000 annually.

Exhibit 7 shows the distribution of stipends across departments.

[6] The annual cost of an individual cellphone stipend is $35 per month, or $420 per year. The annual cost of cellphone and data stipends together is $75 per month, or $900 per year.

Exhibit 7: Total Number of Employees Receiving Cellular and/or Data Stipends



Source: Auditor analysis of PeopleSoft data on City employees receiving cellphone and data stipends

An Unknown Number of Employees Use Their Personal Phones for City Business

As technology has changed, more employees have access to City computer resources from their personal smartphones. For example, with the implementation of Office 365, employees can access their City email accounts from their home computers or smartphones. Although non-exempt employees are required to file the *Remote Access Authorization Form* with IT to request email access, exempt employees can access Office 365 on their smartphones without the form. Thus, there are an unknown number of employees who may use their personal devices for City business that do not receive stipends and are not covered under the existing *Cellular Telephone Policy*.

The Cellphone and Data Stipend Policies Are Outdated and Oversight Should Be Improved

The City's policies surrounding cellphone and data stipends are outlined in the City's *Cellular Telephone Policy* (1.7.4). The eligibility criteria for a cellphone stipend require that the employee have a business necessity, and the policy states that *"[s]tipends should only be offered in those circumstances where offering the stipend will be more cost effective than issuing a phone."*

Based on the City's wireless service contracts, the breakeven point between offering a City cellphone and providing a cellphone stipend is roughly 580 minutes of calls per month.[7] The breakeven point for individuals with data stipends is more difficult to calculate because employees are commonly offered an unlimited data plan.

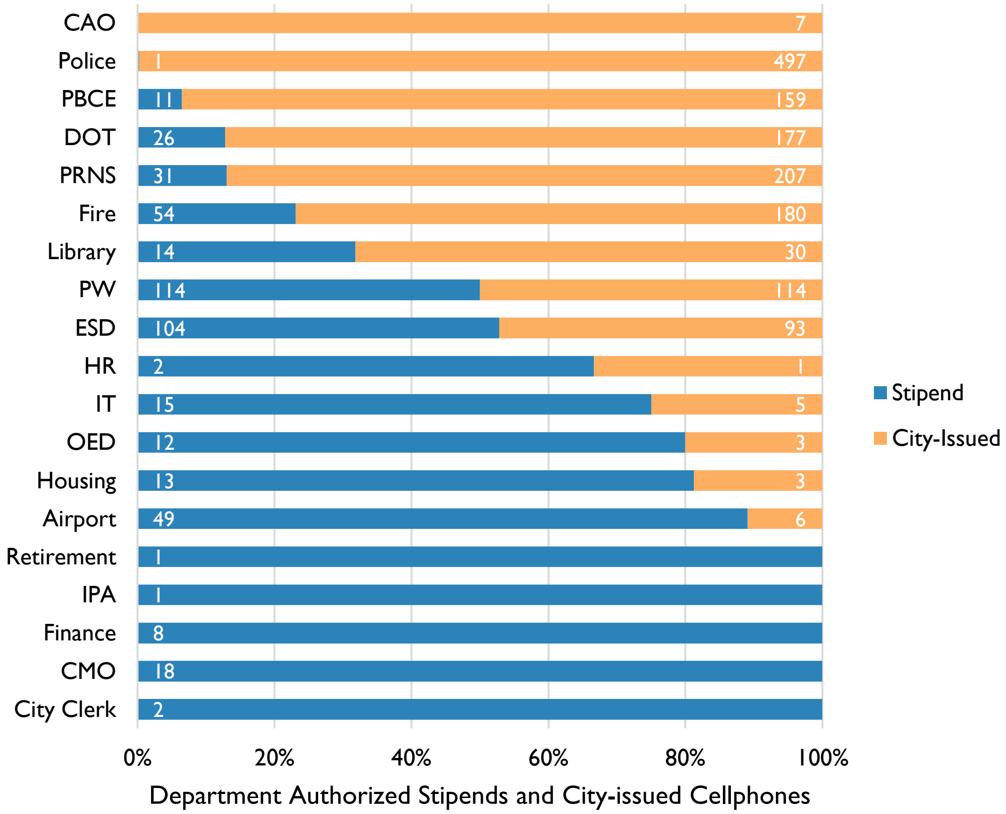
Individual decisions about whether a department should issue a cellphone or a stipend should be made on a case by case basis, based on projected usage and job duties as well as any associated administrative costs. In some cases, it may be more cost-effective to issue a City-owned cellphone; and in some cases it would not.

In reality, departments do not appear to assess the cost-effectiveness of offering a stipend, as required by the policy. Decisions generally tend to be based on employee preference, including concerns about handling two phones (one for work and one personal) and about privacy (whether personal devices would be subject to public records requests).[8] In some cases, it appeared departments preferred offering stipends because of the ease with which they could be managed compared to cellphones.

[7] This only includes the ongoing, monthly costs and does not include equipment costs or administrative costs to manage the cellphones or the stipends.

[8] The California Public Records Act defines "public record" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." A case pending in the California Supreme Court, *City of San José v. Superior Court of the State of California (Ted Smith)*, will consider whether records stored on privately owned devices that the City cannot access are subject to disclosure under the California Public Records Act.

Exhibit 8: Some Departments Tend to Prefer City-Issued Phones, While Others Prefer Stipends



Source: Auditor analysis of PeopleSoft data and department documents

Eligibility Criteria for Stipends Are Out of Date and Should Be Updated to Reflect Usage and Need

Current policies state that cellphone stipends can be offered to staff if it is determined that an employee has a business necessity for a cellphone; on the other hand, data stipends are only allowed for Division Managers or above unless approved by the City Manager's Office. The *Cellular Telephone Policy* (1.7.4) notes that data stipends are made available to allow employees to obtain data plans for smartphones that allow access to City email.

As described in more detail in Finding 2, the ownership of smartphones has grown considerably since 2011, when the most recent revision of the *Cellular Telephone Policy* occurred. Along with that growth has come an increased ability for individuals to access email away from work. Currently, multiple departments report that some employees use their smartphones to check their City email, regardless of whether they had data stipends or not.

Although the data stipend eligibility criteria may have reflected data usage and business necessity at the time of the last policy revision, in our opinion the criteria should be updated to reflect current technologies and the needs of departments and staff, rather than be based specifically on job classification.

The City Should Review and Update the Dollar Value of the Stipends Provided to Employees

According to the *Cellular Telephone Policy*, the monthly stipend amount is to be reviewed and/or adjusted annually to ensure its cost-effectiveness. However, it does not appear this review is regularly done. The current $35 cellphone and $40 data stipend amounts have been in effect for many years. The amount of the cellphone stipend has not been changed since the stipend program began in 2005, while that of the data stipend has not changed since at least 2007.

The stipend amounts should be reviewed and adjusted as necessary to reflect the current costs of price plans, as well as estimated usage of personal cellphones for business purposes by employees. The City's current standard voice price plan available to the City is $0.06/minute. The current monthly cost for an unlimited data plan ranges from $37.50 to $39.99/month (see Appendix A for more details on select price plans).

In addition, the City should review whether the separate stipends, as they are currently structured, continue to meet the business needs of City employees or current technologies. Other jurisdictions typically offer a single stipend amount to cover both phone and data, or distinguish stipend amounts by the capabilities of the device (e.g., smartphone vs. non-smartphone). For example, San Diego provides a $35 per month stipend for a standard cellphone or a $50 per month stipend for a smart device (i.e., smartphone or tablet).

Recommendation #2: To ensure that cellphone stipends are cost-effective and reflect current technologies and the usage and needs of City employees, the Information Technology Department should work with the Finance Department to:

a) Provide guidance for departments on how to assess the cost-effectiveness of offering a stipend as opposed to issuing a City-owned device;

b) Update the eligibility criteria for stipends to reflect business need (i.e., the same criteria for City-owned devices) and delegate approval to the department level; and

c) Review and adjust the amount and structure of the City's cellphone and data stipends.

The Information Technology and Finance Departments should update City policy accordingly.

Departments Do Not Regularly Review Employee Stipends to Verify Business Need

Per the *Cellular Telephone Policy*, departments are responsible for reviewing approved stipends on an annual basis to identify employees who may no longer qualify for stipends, and ensure that such stipends are terminated. Departments are also responsible for terminating stipends for employees when they transfer to other City departments.

However, most departments were unaware of these responsibilities. As a result, few departments conducted annual reviews of stipend holders and many did not terminate stipends when employees transferred to other departments. During our review, we found three individuals who had been receiving stipends while using City-issued cellphones.[9] In addition, because departments do not generally review stipend recipients, staff who have changed positions or departments may continue to receive stipends even if they may no longer qualify. Based on a review of a sample of authorization forms, at least one individual receiving a stipend had been authorized by a previous department; no authorization from the individual's current supervisor was on file.

We recommend that the Finance Department provide oversight of the stipend process by annually generating a list of stipend holders from PeopleSoft to send to departments to verify that these employees still qualify for stipends. In addition, departments should check the stipend list against current inventories of City-issued phones to determine whether any individuals on the list have also been issued cellphones. Finally, Finance should work with the Human Resources Department to update the citywide *Employee Exit Checklist* to add a requirement that any cellphone and data stipends be terminated upon an employee's transfer to another department.

Recommendation #3: To ensure cellphone stipends are terminated for employees who no longer qualify for them, the Finance Department should annually generate a list of stipend holders and send it to departments for verification that employees on the list still qualify for stipends and that they do not also have City-issued cellphones.

Recommendation #4: The Finance Department should work with the Human Resources Department to revise the Employee Exit Checklist to include a requirement that department staff notify the Finance Department's Payroll Division to terminate a stipend when an employee transfers from the department or otherwise becomes ineligible for the stipend.

[9] The cost of these stipends totaled $1,260 annually. We notified the respective departments about these three individuals. Two of the individuals had their cellphone stipend terminated. The third returned their City-issued cellphone.

The City Should Clarify the Difference Between Taxable and Non-Taxable Stipends

Currently, cellphone or data stipends can be either taxable or non-taxable. The large majority of stipends issued are taxable; just 37 individuals (or 8 percent of total stipend holders) receive non-taxable stipends.

The *Cellular Telephone Policy* (1.7.4) states that "[t]he stipend shall not be considered additional compensation to the employee." However, it does not provide clear guidance on what is required for the stipend to be non-taxable. According to the *Cellular Authorization Form*, which departments submit to Finance to initiate a stipend, employees are required to submit documentation that justifies that work-related cellphone charges are at least equal to the amount of the stipend. The *Cellular Authorization Form* specifically states:

> *My signature below indicates that I have incurred or will be incurring business cell phone expenses on my personal cell phone that equal the stipend amount being reimbursed through the City payroll system. If I am receiving the stipend as NON-TAXABLE, I have attached a copy of my contract or monthly bill, and I also authorize the City to recover any cell phone stipend amount I have received for which I do not have cell phone expense at least equal to the stipend amount or justification that qualifies as an IRS business expense reportable on IRS form 2106.*

In our review of a sample of stipend authorization forms, such required documentation was not always present. In at least one instance, the attached documentation showed monthly charges less than the stipend amount.

As described earlier, staff in departments were often not aware of or did not understand their specific responsibilities surrounding stipends. This extended to the difference between taxable or non-taxable stipends and the documentation required for stipends to be non-taxable.

Recommendation #5: The Finance Department should:

a) Work with the City Attorney's Office to clarify City policy on the taxability of stipends and either eliminate non-taxable stipends, or provide guidance to department staff on what documentation is required for a stipend to be non-taxable.

b) If non-taxable stipends are continued, the Finance Department should review the authorization forms for employees for non-taxable stipends for required documentation to justify the non-taxable status of the stipends. Finance should then work with departments to compile any missing documents or change the status to taxable.

This page was intentionally left blank

Finding 2 The City Should Develop a Mobile Device Policy to Reflect Current Technologies and Business Needs

Summary

City policies related to mobile devices are outdated and do not provide an efficient or effective framework to achieve the benefits or address the risks of such devices. Currently, up to 17 City Administrative Policies can apply to the use of mobile devices by City employees. It can be difficult for staff across the City to understand their roles in the day-to-day management or use of these tools. The City should consolidate policies related to mobile devices under a Mobile Device Policy that encompasses all mobile devices and clarifies responsibilities for staff to manage such devices at the department level. The policy should also address potential information security risks by including guidelines about the degrees of access allowable for various types of devices, required conditions for user access to the City's networks, and other areas. Finally, the policy should include user friendly guidelines for employees to understand their responsibilities as well as allow for limited, incidental personal use of mobile devices similar to the allowance provided for non-cellular City telephones.

Up to 17 Different City Policies Can Impact the Utilization of Mobile Devices

Currently, up to 17 different City Administrative Policies can apply to the use of mobile devices by City employees. Included among these are policies related to the use of City equipment, technology, human resources, purchasing, and public records. Many of these have been developed or revised in recent years; however, with each new policy or revision, it can become more difficult for staff across the City to understand their roles and responsibilities under the policies as they relate to the day-to-day management or use of mobile devices.

This is further complicated by rapid changes in mobile technologies and the increased use of mobile devices broadly. For example, the percentage of U.S. adults who own a smartphone has nearly doubled since 2011 (reaching 68 percent in 2015). Also, just 4 percent of U.S. adults owned a tablet in 2010 (the year the first iPad was released); by 2015, nearly half of U.S. adults owned one. These trends are particularly evident among younger adults, who make up the largest segment of the U.S. working population.[10]

[10] Richard Fry, *Millennials surpass Gen Xers as the largest generation in U.S. labor force*, Pew Research Center, May 11, 2015, http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/.

Exhibit 9 shows a timeline showing the rapid development of technologies since 2003 as well as implementation or revision dates of select City policies.

Exhibit 9: Timeline of Changes in Technology and Select City Policies

2003	**E-Government Policy implemented** Release of the first Blackberry smartphone
2004	**Telecommuting policy implemented** Release of the first Motorola Razr – 65% of adults in the U.S. own a cellphone
2005	**Personal Use of City Equipment Policy revised**
2006	**Remote Access Policy revised** Introduction of Twitter Facebook opens to all users
2007	Release of the first generation iPhone
2008	**Procurement of Information Technology Policy revised** **Information Security Policy implemented** Release of Dropbox
2009	
2010	Release of the first iPad – 4% of U.S. adults own a tablet
2011	**Cellular Telephone Policy revised** Release of Microsoft Office 365 – 35% of U.S. adults own a smartphone
2012	Release of Microsoft Surface
2013	Majority of U.S. adults (56%) own a smartphone, 35% own a tablet
2014	World Wide Web Consortium recommends finalized version of HTML 5, supporting mobile-friendly web design
2015	**Procurement of Laptops and Tablets Policy implemented** 68% of U.S. adults own a smartphone, 45% own a tablet Release of the Apple Watch
2016	**Flexible Workplace Policy revised** **Open Data Implementation Policy and Procedures implemented**

Source: Auditor analysis based on City Administrative Policy Manual, Pew Research Center data on device ownership, and various industry websites and publications

The City Needs a Mobile Device Policy to Address the Use of Current Mobile Resources

The City currently does not have a single policy that outlines staff responsibilities surrounding the use of all types of mobile devices across the City. Such a policy should address IT's broad responsibilities in maintaining the City's information assets and security; the role of individual departments in managing mobile devices required to deliver City services; and individual employees' responsibilities as users of mobile devices for City business.

The City's Cellular Telephone Policy Is Limited in Its Application

The City's *Cellular Telephone Policy (*1.7.4) provides guidelines and criteria regarding the purchase and use of City-issued cellphones, including smartphones. This policy was originally created in 1989 and has gone through various revisions over time. Because the most recent revision occurred in 2011, it does not reflect current usage of mobile technologies.

Although the policy recognizes the value of cellphones, it states that authorization to purchase such phones will be limited to certain circumstances, such as when other means of communication including pagers or mobile radios are determined to be infeasible or impractical or are less cost-effective. Since 2011, the uses of cellular phones have grown beyond the circumstances described in the policy, and now include email, use of apps, and other functions (nearly half of all City-owned cell phones are smartphones).

In addition, the current policy only applies to cellphones and does not apply to other mobile devices. As described in Finding 1, we estimate the City currently has more than 950 tablets in use across the City. The majority of these are either iPads or Microsoft Surfaces. The first iPad was introduced in 2010, and the first Surface was introduced just four years ago in 2012. For data-enabled tablets and mobile hotspots (that allow for wireless access to laptops, tablets, or other devices), wireless services are billed through the same wireless service vendors as the City's cellphones.[11] As described in Finding 4, data charges related to these devices as well as smartphones account for the large majority of the monthly billings from the wireless service vendors.

Clarification of Roles and Responsibilities Can Ensure Effective Management of Mobile Devices Across the City

The City's *Cellular Telephone Policy* states that departments are responsible for tracking and controlling cellphone costs. It also provides that a department should have a Cell Phone Liaison and lists specific responsibilities such as coordinating the purchase of a cellphone and initiating service, the reassignment of existing phones, and administering random audits of cellphone bills to ensure they are only used for City business. The Cell Phone Liaison also has responsibilities relating to cellphone and data stipends. With the exception of a few small departments, City departments have identified staff to manage their cellphones.

[11] This does not include non-data enabled tablets, or devices that solely use traditional WiFi available through a wireless access point in a building, for example, and not through a cellular provider.

Although there are no similar guidelines for other mobile devices, departments generally have assigned staff to similarly manage tablets, hotspots, and laptops. However, this may not be the same staff assigned to be the Cell Phone Liaison. Responsibilities surrounding purchase (of both devices and lines with the wireless service vendors), bill review and payment, and others may be divided among staff across devices or across divisions.

Staff across the City assigned to manage mobile devices report that they had generally learned their roles and responsibilities on the job and had not received specific training on the City's *Cellular Telephone Policy* or related policies. As a result, general understanding of responsibilities and management of mobile devices varies across departments. Examples include, but are not limited to, the following:

- Some staff assigned to manage mobile devices were not aware of the various wireless service providers and plans available to the City.
- As described in Finding 1, inventory management is one area where there is great variation across the City. The *Cellular Telephone Policy* does not provide clear guidance for department liaisons to maintain inventories of cellphones or smartphones, and the maintenance of such inventories was not consistent across the City.
- Staff across departments were not clear on what to do with surplus devices. Although City policy generally requires that departments send surplus property to Public Works, some departments sent their surplus mobile devices to IT. In one instance staff passed old cellphones to Happy Hollow Park and Zoo as part of a recycling donation fundraiser. Others kept their surplus items within their departments for later reassignment; however, these were often kept at an individual's desk and it is not clear how securely they were maintained.
- While some departments used specialized software to install applications to City-issued devices, one department issued instructions to staff on how to install applications for City business, requiring the individual creation of a Google Play account and associated Gmail. As an alternative, the instructions allowed staff to use personal Gmail accounts for the creation of the account, potentially in violation of the City's policy on the *Use of E-Mail, Internet Services, and Other Electronic Media* (1.7.1) and the *Cellular Telephone Policy*.

Other jurisdictions, including Denver and Sacramento, have developed or begun to update their administrative policies to reflect technologies beyond cellphones, including tablets and other devices. The City should similarly update its policies to clarify the responsibilities and expectations of departments for managing mobile devices.

Recommendation #6: The Information Technology Department should develop a *Mobile Device Policy* to supersede the current *Cellular Telephone Policy* (1.7.4) to:

a) Reflect the use of all mobile devices by employees across the City, including both personal and City-owned cellphones, smartphones, tablets, hotspots, and laptops.

b) Clarify the specific duties and responsibilities of mobile device liaisons within departments who are tasked with managing such devices.

The new policy should cross-reference with the City's *Information Security Policy*, the *Remote Access Policy*, and any other relevant policies that relate to mobile devices.

Recommendation #7: To ensure consistent application of the *Mobile Device Policy*, the Information Technology Department should develop and provide periodic training for department liaisons on their specified administrative duties and responsibilities outlined in the policy for both City-issued and personal devices used for City business.

The Growth of Mobile Devices Has Increased the City's Information Security Threats

Mobile devices can pose additional information security threats to the City as they are physically less secure and may require frequent software updates to remain secure. According to the U.S. Government Accountability Office, common vulnerabilities that allow for threats on mobile devices include failure to enable password protection, the limited capability to intercept malware, and operating systems that are not kept up to date with the latest security software.[12]

According to Check Point Software Technologies Ltd.'s 2016 Security Report, there are five major categories of attacks and vulnerabilities that mobile devices face today:

[12] U.S. Government Accountability Office - Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged, September 2012.

System Vulnerabilities Operating system variations increase attack vectors. Android devices are especially vulnerable to attack.

Configuration Changes Bypassing authorized settings and configurations to create subtle changes, potentially without users ever knowing. Rooting or jailbreaking a phone are common examples of this.[13]

Repackaged or Fake Apps Like phishing, fake apps look real but have unexpected features.[14]

Trojans and Malware Embedding malicious code in attachments and applications remains a large area of concern for mobile devices. Many do not have any kind of antivirus or threat prevention.

Man-in-the-Middle Attacks Free and public WiFi hotspots are very easy to fake, making them more prevalent. Spoofing encryption security certificate credentials makes it easier to intercept, alter data in transit, or install Trojans.[15]

The City's mobile devices can be subject to any of the vulnerabilities listed above.

Information Security on Mobile Devices Is Not Explicitly Addressed in City Policies

Although a number of policies refer to information security of devices in general such as the *Remote Access Policy* (1.7.3); *Use of E-mail, Internet Services, and Other Electronic Media Policy* (1.7.1); *Flexible Workplace Policy* (4.2.14); *Telecommuting Policy* (1.7.2), and the *Information Security Policy* (1.7.6), none of them explicitly address mobile devices. The policies are especially outdated as they do not directly refer to the security of personally owned devices used for City business, either with or without cellphone stipends.

Information security standards such as the National Institute of Standards and Technology (NIST) policy on mobile devices,[16] ISACA,[17] and the Criminal Justice Information Services security policy[18] recommend that organizations have

[13] Rooting (Android operating systems) and jailbreaking (iOS operating systems) refer to the process of allowing users of devices to attain control over the customization of the operating system.

[14] Phishing refers to the attempt at obtaining sensitive information by posing as a trustworthy entity in an electronic communication, most often this is attempted when a user clicks on a web link.

[15] Spoofing is a term that refers to disguising the identity of the entity in an attempt to obtain sensitive information through electronic means.

[16] *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards and Technology (June 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[17] *Securing Mobile Devices*, Information Systems Audit and Control Association (ISACA) (August 2010), http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx.

[18] *Criminal Justice Information Services (CJIS) Security Policy*, U.S. Department of Justice (June 2016), https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf.

policies that include certain elements regarding the security of mobile devices. For example, policies should:

- Define which organizational resources may be accessed via mobile devices;
- Define which types of devices are permitted to access the organization's resources;
- Define the degree of access that various classes of mobile devices may have;
- Define the way provisioning should be handled;[19]
- Be consistent with the security policy for non-mobile systems;
- Include a Bring-Your-Own-Device[20] component if applicable; and
- Develop incident handling procedures for applicable scenarios, such as loss of device control, total loss of device, and/or potential device compromise.

Other jurisdictions have information security policies specific to mobile devices. For example, Denver's Mobile Device Policy defines which devices can access organizational resources and assigns responsibility to its information technology department to set-up the device and establish connectivity.

San Diego has a specific Mobile Device Security Policy that sets minimum security standards for mobile devices to protect the confidentiality of data and the integrity of data and applications. It applies to both city-issued and personally owned devices and defines specific responsibilities for users and central support departments (including the Information Technology and Communications Departments).

IT is currently in the process of updating the City's information security policies.[21] Although they present significant improvements over the current policies, IT can further clarify how they apply to mobile devices. For example, IT should define which organizational resources may be accessed via mobile devices and the degree of access that various classes of mobile devices may have. For instance, a City-issued smartphone may be allowed to access City email, whereas a Virtual Private Network (VPN) secured laptop may access various City software and databases.

[19] Provisioning refers to providing users with access to information systems and devices.

[20] Bring-Your-Own-Device refers to policies that permit employees to utilize their personally owned laptops, tablets, or smartphones for business purposes.

[21] Also see the City Auditor's *Audit of Information Technology Controls* issued in January 2012. Specific recommendations from this audit related to password protection and other user controls, guidelines on handling of personally identifiable information, and other issues are addressed in the draft policies.

Furthermore, although exempt employees are no longer required to file the *Remote Access Authorization Form* to gain access to the cloud-based Office 365 on their mobile phones, the form is mandated to be filed for non-exempt employees. Neither the policy nor the *Remote Access Authorization Form* have been updated; as a result, some departments were unaware of the change.

IT should clearly define access privileges based on employee classification for connecting to the City's network and/or the cloud-based Office 365 software on mobile devices, and update the appropriate policies and forms accordingly.

IT Should Develop Guidelines for Personally Owned Devices Used for City Business

The current and draft information security policies do not explicitly address personally owned devices used for City business, such as the use of a personal smartphone to access City email, yet best practices[22] recommend that the mobile device policy address the use of personally owned devices for accessing City resources.

According to benchmarking review, several elements should be included in the mobile policy and cross-reference any other information security policy related to mobile devices. For instance:

- Any applicable support expectations by IT for the personally owned devices should be defined. For instance, the policy can cross-reference the *Remote Access Policy* (1.7.3), showing that IT can authorize and configure personal devices by establishing secure access to the City's network (VPN access).
- Any applicable user conditions should be addressed—for example, that the user is liable for any damage or loss to their personal phone used for City business, that it is the user's responsibility to ensure that the device functions as intended, etc.

Furthermore, the policy should be consistent with the information security policy for non-mobile systems.

Other jurisdictions include guidelines for personally owned devices used for city business in their security policies. The Denver Mobile Device Policy addresses both personally owned devices with or without stipends and security guidelines

[22] *Criminal Justice Information Services (CJIS) Security Policy*, U.S. Department of Justice, June 2016, https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf.

Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Securing Mobile Devices, Information Systems Audit and Control Association (ISACA), August 2010, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx.

for employees to follow depending on which option they choose. Phoenix has a separate information security policy on personally owned mobile devices. It includes security best practices, user consent for IT controls over the device (e.g., enlisting a personal device on a mobile device management software) and other measures.

IT Should Develop Procedures to Protect Information on Lost or Stolen Mobile Devices

In cases of theft or loss, best practices[23] recommend that mobile devices be disconnected from the City's network, remotely wiped, and/or locked. The mobile device policy should address any IT control over mobile devices to allow for such actions, especially personally owned devices, to ensure a user's full consent. This process should be described in the Mobile Device Policy, including the assignment of responsibility to the employee to report such incidents to IT immediately.

Recommendation #8: To address information security risks associated with mobile devices, the Information Technology Department (IT) should develop, and include in the *Mobile Device Policy*, guidelines and procedures for both City-issued and personally owned devices that identify:

a) The degree of access for various types of mobile devices and employee classifications in connecting to either cloud-based City services or to the City's network;

b) Any applicable support expectations by IT for personally owned mobile devices used for City business;

c) Any applicable user conditions, especially if personally owned devices may be enlisted on a mobile device management software; and

d) Any applicable IT controls over mobile devices, such as remote locking or wiping of device in case of theft or loss.

Any authorization forms, such as the *Remote Access Authorization Form*, should be updated accordingly.

[23] *Criminal Justice Information Services (CJIS) Security Policy*, U.S. Department of Justice, June 2016, https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf.

Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

The Information Technology Department Should Develop Mobile Device User Guidelines for Employees

Beyond providing guidelines for managing mobile devices by administrative staff, various City policies also define specific employee responsibilities. However, these are not consolidated in one area, nor are they always cross referenced in a way that allows employees to easily understand all of the policies they are expected to follow. For example:

- The *Use of E-Mail, Internet Services, and Other Electronic Media* (1.7.1) policy provides guidelines about maintaining password protection, using proper etiquette in email messages, and refraining from using personal e-mail for City business.
- The *Remote Access Policy* (1.7.3) requires that employees ensure anti-virus software is kept up to date.
- The *Personal Use of City Equipment* (1.6.2) policy requires that employees exercise due care in securing and maintaining City equipment in their possession.

User Friendly Guidelines and Training on Information Security Can Better Protect City Data and Network Access

Aside from broad information security policies that should address mobile devices as stated above, IT should also ensure information security is practically enforced at the user level by providing users with general, non-technical guidelines on security best practices. These user guidelines should be included in the recommended Mobile Device Policy.

Such guidelines may include protecting the device with a strong password, re-entering the password after the device has been idle for 15 minutes (or fewer), using up-to-date malware software, and updating the devices with the latest security patches. They should also define guidelines for personally owned devices used for City business as well as user responsibilities and duties in case of theft or loss of device.

Currently, the dissemination of the City's information security policies and best practices is decentralized to departments, with no central training provided by the City's IT. The Information Systems Audit and Control Association (ISACA) recommends that the workforce be educated on basic security practices when using devices to access City resources and that trainings be provided to spread awareness.

Recommendation #9: The Information Technology Department should:

a) Develop user friendly guidelines on mobile device information security and include it as part of the *Mobile Device Policy*.

b) Establish periodic information security awareness trainings for all personnel who access the City's network on City-issued and personal devices.

The City Does Not Allow for Incidental Personal Use of City Cellphones

Both the City's *Cellular Telephone Policy* (1.7.4) and the *Personal Use of City Equipment* (1.6.2) policy state that City-issued cellphones and other mobile devices are to be used for City business only. The *Cellular Telephone Policy* does allow for personal use in cases of emergency, but notes that this may require reimbursement to the City for any associated costs.

Specifically, the policy requires Cell Phone Liaisons to distribute cellphone bills and reimbursement forms to employees at least once per year. The employee is expected to review and identify any personal calls and reimburse the City for calls at a rate of $0.06/minute. The employee is to reimburse the City for the personal calls if the total amount owing is $1.00 or more. [24] This process can be burdensome for departments, in particular those with large inventories of cellphones. In at least one instance, a department no longer reviewed for personal use because it was deemed a big workload and not a good use of resources.

The City Does Allow for Incidental Use of City Desk Phones

The *Personal Use of City Equipment* policy does allow a personal use exception for non-cellular telephones, stating:

> *It is recognized that from time to time employees need to make/receive personal calls. … It is appropriate to use City landline phones for such calls <u>within the following guidelines</u>:*
>
> *A. Personal calls may be a distraction from the employee's assigned duties. Accordingly, such calls should be of short duration and infrequent. Supervisors are responsible for ensuring that*

[24] Based on interviews with departments, those that do distribute cellphone bills and reimbursement forms for employee review report not having received any reimbursements for some time. See Finding 4 for more information about how the City can more effectively identify cases of abuse.

> *personal calls do not negatively impact services to the public or departmental operations.*
>
> *B. Calls of a personal business nature (e.g. selling goods or services) shall not be made or accepted on City phones.*
>
> *C. City telephone numbers should not be listed in want ads, sales offers, bulletin boards, newspapers or any electronic media form in conjunction with personal use and/or personal business.*
>
> *D. City telephones should not be used for personal long distance calls.*

Many City workers regularly work in the field and may not have ready access to City landline phones. Current City policy would require these workers to carry second cellphones in addition to any City-owned cellphones to make any necessary personal calls. We believe this is unfair for such workers given the allowable personal use exception for other telephone usage.

Other jurisdictions, including Denver and Portland, allow for reasonable, limited, or incidental use of mobile devices. The City should similarly provide guidelines on incidental or limited personal use in the proposed Mobile Device Policy similar to the personal use exception for landline phones.

Recommendation #10: The Administration should consider allowing short, infrequent personal calls by employees using City-owned cellphones, similar to the exception for such calls using City landline phones in the *Personal Use of City Equipment* policy. This exception should be included in the *Mobile Device Policy*.

Finding 3 The Process for Ordering Mobile Devices Can Be Streamlined

Summary

City policies currently require multiple levels of approval and/or review to order tablets, laptops, and smartphones. While departments may order cellphones directly, without additional review, tablets and laptops must be ordered through IT, and smartphone purchases must be approved by the City Manager's Office. This may unnecessarily slow the process, however, as both IT and the City Manager's Office tend to defer to department directors' assessments of business need. Also, despite centralized approval and ordering processes, the City has no central record of approved or ordered devices by department.

Additionally, the Procurement of Laptops and Tablets Policy directs departments to order the most cost-effective device based on business need, but the laptop and tablet price list (which informs decision-making) is inaccurate and difficult to find. In some instances, it appears the City has paid more than retail for some laptops and tablets, at least in part because the responsibility for checking the City's discount is not clearly assigned.

Finally, though hotspots and accessories are ordered and billed through the same wireless service purchase orders as cellphones and smartphones, they are not addressed within the City's policies on mobile device procurement.

The Purchase of Laptops, Tablets, and Smartphones Requires Multiple Levels of Review and/or Approval

The *Procurement of Laptops and Tablets Policy* (1.7.8) requires that IT order all laptops and tablets across the City.[25] While this policy has largely been understood and followed by departments, this additional step is not an effective control on costs or inventory and may unnecessarily slow the cycle time between order request and receipt.

According to the *Procurement of Laptops and Tablets Policy*, prior to approving a tablet or laptop purchase, a department director, assistant director, or deputy director should determine that there is valid business need to justify the purchase. Because IT has no other means of knowing the exact business needs of a particular individual or department, IT tends to rely on departmental approval and does not provide any additional oversight over the purchasing

[25] The Police Department has a separate departmental purchase order for Mobile Data Computers (MDCs), including the rugged laptops for patrol cars. The Fire Department and Department of Transportation have also ordered through this purchase order. For tablets and non-MDC laptops, the Police Department orders through the IT help desk systems and follows the same approval process.

process.[26] IT also does not generally provide guidance to departments on which mobile devices would best suit their needs; IT solely reviews the request to check that the department has submitted an approval letter and business need.

The Ordering Process for Tablets and Laptops Takes Weeks

For standard tablet and laptop requests, IT then orders the item through an online vendor portal, which lists only City-approved configurations. Deliveries typically go to IT, where the receipt and invoice are filed. IT then sends the device on to departments. For a standard item, the time from request to delivery to IT is usually three weeks for a laptop, or one to two weeks for a tablet. For non-standard items, the process is longer. For example, a department may request a ruggedized laptop with more memory or a more advanced processor than the standard configuration, which takes additional time to process on the vendor side, but may also undergo a more thorough approval process within the City.

For Many Devices, Internal Processing Through IT Can Be Eliminated

Unless requested by a department, IT does not additionally configure devices, but delivers them to departments as-is. Developing a process by which IT or department staff configure devices to meet the City's information security requirements and allowing departments to directly order standard, City-approved devices through citywide purchase orders would save staff time and facilitate inventorying. Based on business need, staff could obtain the same level of approval (i.e., from their department director, assistant director, or deputy director) and order devices through the current online vendor portal, showing only City-approved configurations, and have the devices shipped directly. For departments with the ability to secure their own devices, this would eliminate the time associated with internal processing through IT.

Smartphone Purchases Require the Approval of the City Manager

The City's *Cellular Telephone Policy* (1.7.4) similarly requires a departmental cellphone liaison obtain approval for a new cellphone or smartphone from the department director. For a smartphone, the policy requires the liaison to then forward the approved *Cellular Authorization Form* to the City Manager's Office for final approval. Currently, this approval is done by a Deputy City Manager. The Policy clearly states:

> ***Smartphone/PDA cellular telephones purchases must be approved by the City Manager prior to purchase****…Once approved, the requesting Department's Cell Phone Liaison will coordinate… the purchase of a City*

[26] Until recently, IT had authority to approve or deny laptop and tablet requests. Over the course of the audit, this procedure was updated to delegate approval authority to the departments. However, the policy requiring IT order devices has not been changed.

> *cell phone and service initiation with the City's cellular telephone service provider…*

In practice, approval of smartphones entails wet signatures of multiple parties—potentially including the user, a department cellphone liaison, a user's supervisor, a department director or deputy director, and a deputy city manager.

Currently, there are at least 701 City-issued smartphones across all departments—all of which should have been approved by the City Manager under current policy. Almost all departments reported going through the City Manager's Office for smartphone requests. According to the City Manager's Office, these approvals generally defer to department directors regarding business need.

This additional level of approval slows ordering turn-around without providing additional control, representing an inefficient use of staff time and a restriction on the purchase of a common business tool. While some department liaisons reported receiving approval within a few days, several departments reported never receiving any confirmation or reply for forms submitted. After receiving no confirmation, one department purchased the smartphones anyway.

Given that smartphones are a common business tool and that the City Manager's Office defers to departmental approval, City Policy should be updated to delegate authority to approve smartphone purchases to departments.

City Policy Does Not Address Ordering for Hotspots or Cellular Accessories

Currently, there are at least 434 hotspots in the City, used by departments to provide access to the internet in the field (where secure WiFi is not available) or in the event of an outage. Department liaisons are able to order hotspots through the same open purchase orders as cellphones and smartphones, and they receive monthly bills for hotspots that are the same as those for cellphones and smartphones.

Neither the *Cellular Telephone Policy* nor the *Procurement of Laptop and Tablet Policy* mentions hotspots or similar technology. As such, there are no specified levels of approval to order hotspots. Since hotspot ordering and use are very similar to the ordering and use of cellphones and smartphones, departments tend to apply the same internal processes for hotspots as for cellphones and smartphones. Furthermore, department staff expressed confusion about the purchase of cellular accessories. This included whether they could use a p-card for purchases and what level of authorization was required. The Administration should clarify that policies relating to cellphone and smartphone approvals also apply to hotspots. It should also clarify departments' authority to approve and order mobile accessories.

Recommendation #11: To reduce ordering turn-around and demands on staff time, we recommend the Administration:

a) Allow departments to order mobile devices (cellphones, smartphones, hotspots, tablets, and laptops) and accessories directly, through appropriate citywide purchase orders;

b) Develop a process for IT or department staff to configure devices to meet information security standards in the *Mobile Device Policy*.

c) Update City policy accordingly.

Paper-Based Approval Process Is Slow and Unreliable

The approval process could further be streamlined if the need for wet signatures were eliminated. Currently, paper or PDF approval forms are routed or emailed within or across departments, which can lead to delays. In addition to automating a common business process, a citywide online approval form available through the intranet could also create a record of all technology approvals (and denials) by department and item. This could further improve transparency and provide an audit trail. Currently, Cellular Authorization Forms for City-issued devices are not centrally stored and there is no central record of City-issued mobile devices, so the current number and location of all devices is uncertain.

Recommendation #12: To reduce ordering turn-around and demands on staff time, and to provide greater transparency and citywide inventory control, we recommend the Administration:

a) Explore tools to develop online approval form(s) for the approval of City-issued cellphones, smartphones, hotspots, tablets, and laptops, including whether the device will require remote network access, to be authorized electronically and saved in a centralized, searchable database; and

b) Revise the *Procurement of Laptops and Tablets Policy* (1.7.8) and reference the *Remote Access Policy* (1.7.3) accordingly.

The City's Posted Equipment and Price List for Tablets and Laptops on the IT Intranet Site Is Outdated and Difficult to Find

The City's purchase order for tablets and laptops is updated about annually. IT determines minimum technical specifications to meet the City's needs, and the Finance Department puts out a bid based on those City-approved configurations.

The vendors then determine which devices meet the City-approved configurations. The City price list, posted on IT's Tech Procurement intranet page, is updated to reflect the negotiated price for mobile devices meeting minimum configuration standards established in the purchase order bid. The price list for laptops was last revised in July 2016, and, for tablets and laptops, had been updated in January 2016 before then. Appendix B shows the two most recent price lists, as of September 29, 2016.

The Posted List of Devices Does Not Always Reflect What Is Actually Offered

When a manufacturer releases an upgraded tablet between bids, the vendor may replace the initial tablet with the newer version, under the same purchase order. As a result, the price list may not always reflect the technical specifications of the available devices, which may exceed the City-approved configuration. In some cases, the devices on the price list are no longer sold retail. At least two departments received devices different than they had ordered and several departments expressed frustration with limited or outdated options.

Prices, too, are sometimes inaccurate. For example, though IT listed the price for a Microsoft Surface Pro as $971 per unit, vendor invoices show the City paid $825 per unit for the Surface Pro 3 and has paid $875 per unit since the vendor switched to the upgraded Surface Pro 4.

Furthermore, the City's posted discount does not always keep pace with drops in retail prices. In March 2016, Apple reduced retail prices for the iPad Air (Wi-Fi only) from $499 to $399 and the iPad Air (WiFi + Cellular) from $629 to $529. Through May, the City continued to pay $473.50 and $597.42, respectively.[27]

According to Finance, the City should receive the same negotiated discount relative to reduced retail prices, but departments are responsible for checking prices before buying items through the laptop and tablet purchase order. This responsibility is not reflected in the *Laptop and Tablet Procurement Policy* (1.7.8).

It Is Unclear Whether Departments May Order Based on Lowest Price

Moreover, it is not clear whether departments can order tablets and laptops through alternative vendors, since the *Laptop and Tablet Procurement Policy* requires departments order through the IT ticket system. Other City vendors offer select mobile devices at prices that compare favorably with the City's negotiated discount for tablets and laptops. At least one of the City's wireless service providers advertises data-enabled tablets for less. Office Max, the City's

[27] We notified Purchasing of this lapse in discount. According to Finance, the City can receive credit for the difference after the reduction in retail price. They are currently working with the vendor to resolve the issue.

office supplies vendor, appears to offer ruggedized laptops meeting the City's configuration requirements at a lower price as well.

Finally, tablet pricing on the IT intranet site is difficult to find. The link to the price list references only laptops, not tablets, though the document lists prices and configurations for both. The City *Laptop and Tablet Procurement Policy* asks departments to consider:

- *The type of usage and application for the mobile device (for example, heavy data entry may be better suited for a device with a full sized keyboard rather than a virtual keyboard)*
- *Whether the equipment will be used by a group of shared users for a specialized purpose (e.g. laptops for presentations)*
- *Whether the required applications are compatible with the operating system of the device and whether support is provided by the application administrator or owner.*

Having access to accurate, up-to-date information on available devices, technical specifications, and prices helps departments to make informed decisions about which device will best meet their business needs at the lowest expense.

Recommendation #13: To facilitate departmental budgeting and business need determinations, and ensure the prudent expenditure of public funds, we recommend the Information Technology Department establish and implement procedures to regularly update the City price list to accurately reflect the current discounted prices and technical specifications of available devices, and put an explicit link to tablet pricing on its intranet site.

Finding 4 IT Should Provide Greater Oversight of Mobile Devices to Address Information Security Risks and Control Costs

Summary

IT is responsible for the City's data and voice communications, including telecommunications. However, individual departments currently manage their mobile devices with little oversight by IT. This management structure may not be practical today given the changing technical environment of mobile devices. For example, the administration of mobile device security controls is currently decentralized to departments. Given the utility of mobile device management (MDM) software in securing sensitive data stored in mobile devices, IT should implement such software citywide for devices that pose the greatest information security risks for the City.

The review of mobile device costs and usage is also decentralized. While most departments review bills to some extent, current processes are inconsistent and ineffective in identifying significant cost savings. IT should provide oversight and clarify the management structure for controlling mobile device costs and appropriate use, and revise policy accordingly. As a result, the City could save at least $189,000 per year in costs and minimize risks associated with inappropriate personal use.

IT Should Take a More Active Role in Overseeing Departmental Management of the City's Mobile Devices

IT's mission is to "[e]nable the service delivery of [its] customers through the integration of city-wide technology resources." According to the City's Operating Budget, IT is responsible for enabling the availability and relevancy of data and voice communications—including telecommunications—as part of one of its core services (Information Technology Infrastructure).

Prior to FY 2003-04, IT administered the City's cellphone program, coordinating equipment purchases, phone activations, billings, and reimbursements. In FY 2003-04, the program was decentralized; departments became responsible for ordering phones, tracking personal usage, and requesting reimbursements for personal use as needed. Although this decentralized approach to mobile device management may have been practical in FY 2003-04, it may not be in today's mobile device environment.

The types, capabilities, and variety of uses and features of cellular phones and mobile devices have changed dramatically since FY 2003-04 (as described in Finding 2). In 2003, Blackberry had just released its first smartphone; the first iPhone was still four years away, and the first iPad was seven years away. Today, City-issued smartphones and data-enabled tablets and laptops allow employees to remotely access their work email, the Internet, and, in some cases, the City's network. Such mobile devices are billed through the City's three wireless service vendors, each with its own selection of phone, text, and data plans and features from which departments must choose.

These rapid advancements in mobile technologies and much larger selection of options have bolstered the potential of mobile devices to improve service delivery in the City. But they have also contributed to the complexity, risks, and potential costs of managing mobile devices. In light of its mission and technological capacity, IT should play a key role in addressing information security risks and controlling costs within the City's mobile device management structure. In this way, mobile devices can be effectively and strategically deployed to meet the City's evolving technological needs.

Mobile Device Management Software Can Address Potential Information Security Risks of Mobile Devices

Currently, the enforcement of mobile device information security is primarily managed at the departmental level and varies widely across the City. While IT grants remote access to mobile devices and in some cases configures newly purchased tablets and laptops, departments enforce basic security measures such as passwords and antivirus software.

The information security enforcement procedures are not uniform citywide. For instance, while some departments require passwords and screen locks on mobile devices, others do not. Departments that typically handle sensitive data may utilize specific software for data encryption; for example, the Police Department utilizes NetMotion, a mobile performance management software, to encrypt data from laptops used in patrol cars to comply with Department of Justice regulations.

A few departments, including Transportation, Environmental Services, Fire, and Public Works, have started to use mobile device management (MDM) software to track and manage their mobile devices. For instance, Environmental Services and Fire currently use an MDM software called AirWatch, to begin providing remote support to devices and help alleviate support questions for tablets; they plan on enlisting smartphones on the software in the future. Transportation and Public Works have also begun using AirWatch to install applications and monitor the status of enlisted devices.

Currently, only a small portion—about 150—of the City's total mobile device inventory is enlisted on the software, as current usage is limited to the above listed departments and implementation is in its early stages. Exhibit 10 shows common features of MDM software.

Exhibit 10: Common Features of a Mobile Device Management Software

Supported Devices	Smartphones, tablets, laptops and rugged[28] devices.
Single Management Dashboard	Both City-owned, employee-owned and pooled mobile devices can be enrolled into a single management dashboard.
Operating Systems	Support for every major operating system including Android, Apple iOS, BlackBerry, Mac OS X and Windows.
Device Enrollment	When users enroll and are authenticated, the appropriate restrictions, apps and content are pushed automatically.
Policy Enforcement and Compliance	Software continuously monitors for unauthorized users, compromised devices and other risks.
Commands	Typically, commands can be executed such as device query, lock device, find device, or wipe device.
Real-Time Inventory	Typically, administrators can see a high-level and real-time view of device inventory and drill down into device and user information details.

Source: Software brochures of various MDM software including MobileIron and AirWatch

MDM Software as a Best Practice and Its Use in Other Jurisdictions

According to the National Institute of Standards and Technology (NIST), centralized mobile device management is a best practice for controlling the use of both City-issued and personally owned mobile devices by enterprise users. Similarly, the Criminal Justice Information Services Security Policy recommends MDM that "facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery."

Although MDM software use is a recommended practice, many cities have only recently started to use it. Almost all the cities that we benchmarked were either in the early stages of evaluating its benefits and costs or were just starting to implement it organization-wide.[29] For instance:

[28] A rugged or ruggedized computing device is specifically designed to operate reliably in harsh usage environments and conditions. These are typically used in the fields of public safety or public works at the City level.

[29] Staffing for mobile device management varied in other jurisdictions. Jurisdictions that employed more staff usually tended to have broad, central management of mobile devices with little departmental support.

- In Denver, central IT administers MDM software for about 3,500 devices (both city-issued and personally owned) organization-wide without any departmental controls. Currently, one staff member maintains the MDM software, although the initial implementation had been staffed with four employees.
- Phoenix had MDM at the departmental level, but is transferring sole control over its administration to central IT following an audit recommendation, which found that departments lacked a consistent approach in complying with IT security standards.
- Sacramento began implementation of MDM in early 2016. IT centrally administers the city's MDM software and has so far enlisted 1,200 devices. Currently, IT employs one FTE to administer the MDM software citywide.

Mobile Device Management Software in the City

As described earlier, some departments have already implemented AirWatch based upon an assessment of their technical and programmatic needs for mobile devices. The security controls already in place at the departmental level have set the stage for establishing central administrative oversight with IT, which is primarily responsible for maintaining the City's information security infrastructure.

According to the City's *Information Security Policy* (1.7.6),

> *The Chief Information Officer (CIO) has the duty to administer the City's central computer systems and functions, manage the City's communication services and provide advice and recommendations regarding current and proposed computer system maintenance and planning.*

Furthermore,

> *It is the policy of the City of San Jose to ensure the ongoing critical City operations by establishing and maintaining proper Security of its Information Technology Systems and the data contained therein against terrorist, criminal or unauthorized attack or disclosure.*

IT should work with departments to implement an MDM solution to secure mobile devices citywide.[30] Information security is generally better managed centrally because a global perspective helps to identify trends in threats and

[30] It should be noted that the Police department has its own information security measures and safeguards and could be excluded from this effort.

vulnerabilities more effectively. Further, not all City departments have a technical arm to address their security needs. IT should develop basic minimum security standards that apply to mobile devices within the MDM software to protect City data, for instance, applicable connectivity settings, application use, etc. These basic settings should be applied uniformly to all devices enlisted on the MDM software.

According to best practices[31] and benchmarking review, organizations should perform risk assessments to determine which devices, depending on the sensitivity of the data they carry, should be enlisted on MDM. Most organizations can bear a certain degree of risk; this should be considered in procuring and deploying MDM to ensure practicality and flexibility of device use without unnecessary IT control. Thus, IT should prioritize enlisting devices on MDM according to their levels of information security risk (e.g., those that carry personally identifiable information have greater risk).

Recommendation #14: To address the information security risks of mobile devices, the Information Technology Department (IT) should work with departments citywide to implement Mobile Device Management (MDM) software citywide for the devices that pose the greatest information security risks for the City. Specifically, IT should:

a) Prioritize devices that pose the greatest information security risks for the City to be enlisted on an MDM software, and work with departments to implement MDM software citywide for those devices;

b) Establish basic minimum standards or settings within the MDM software to protect City data within the software; and

c) Either directly manage mobile devices for departments or provide administrative access for departments to manage their own devices if they have the internal capacity to manage those devices.

[31] *Criminal Justice Information Services (CJIS) Security Policy*, U.S. Department of Justice, June 2016, https://www.fbi.gov/file-repository/cjis-security-policy-v5_5_20160601-2-1.pdf.

Guidelines for Managing the Security of Mobile Devices in the Enterprise, National Institute of Standards and Technology (June 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

Current Policies and Procedures Provide Minimal Guidance for Departments to Control Mobile Device Costs

The *Cellular Telephone Policy* (1.7.4) delineates some departmental duties that can help control associated costs. In particular, it states that:

- Department Directors or their designees are responsible for reviewing cellular telephone usage on an annual basis to identify and terminate phones that may be unnecessary or underutilized.
- Cellphone liaisons are to distribute phone bills to employees at least once annually for review and request reimbursement for personal calls.
- An employee is to be offered a stipend based on a comparison with the cost of providing a City-issued device (see Finding 1 for more information on stipends).

In accordance with this policy, most departments review bills to some extent. For example:

- Several departments send bills to users for them to report personal use and submit reimbursements as applicable based on an "honor system." One department does not check for personal use whatsoever.
- A couple of departments examine monthly bills in total and investigate further when there are spikes in total costs.
- Two departments noted that they review bills for overages.

However, in the current account management structure, it is unclear who within departments should review bills to control costs and how they should do this. As a result, departments' current bill review procedures do not allow them to consistently and effectively identify the most significant cost-saving measures, such as deactivating unused or underutilized devices (discussed further in this section).

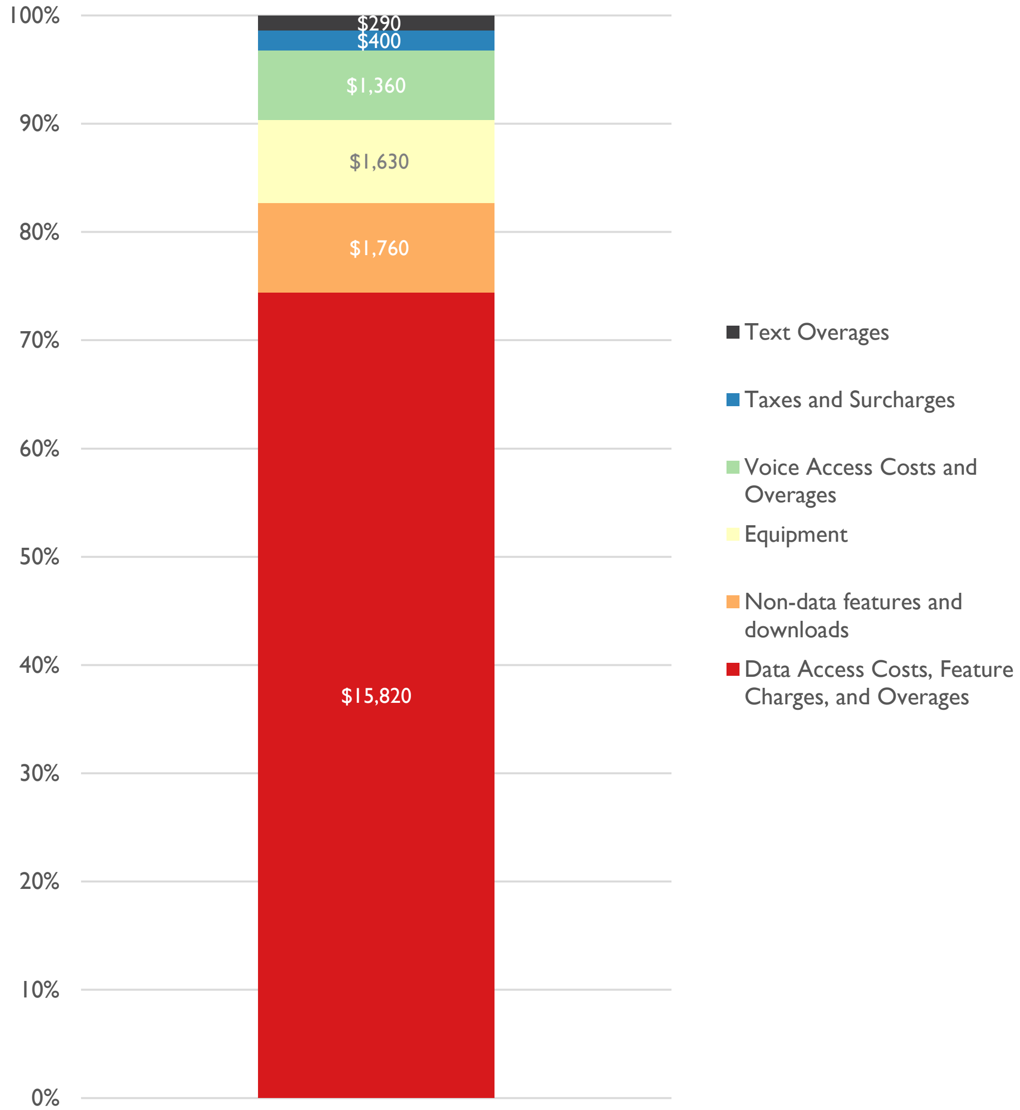
Reviewing Text and Data Costs and Usage, and Informing Users What Their Plans Cover Can Help Control Costs

The *Cellular Telephone Policy* is unclear as to what types of usage departments should review. The policy refers only to cellphones, excluding data-only devices like tablets and mobile hotspots. Even for cellphones, despite the growing importance of text and data in today's technological environment, the policy does not specifically require that departments review text and data usage in addition to phone calls. Neither does the policy require that wireless service users are made aware of their plans' features and limitations.

Some departments do not review text usage as a means to control costs. For example, five high users in one department accrued nearly $170 in text overage charges in June 2016, though Verizon's unlimited text feature for $12 could have been added to their lines. The department liaisons had not been reviewing text usage and did not know of the unlimited text feature. According to the liaisons, these high users may have assumed that they had unlimited text since most of them had unlimited data. Such costs could be avoided if the liaisons and users knew of the applicable plan features and limitations, and/or if the plans were adjusted based on need and average usage.

At the time of the audit, it appears only two departments had been reviewing data usage for the purpose of controlling costs. Due to the significant proportion of vendor charges for data-related plans, features, and overages, bill reviews should include an examination of data usage and costs. As seen in Exhibit 11, data-related charges represented a significant majority of the City's payments to Verizon.

Exhibit 11: Verizon Wireless Service Charges by Category (Monthly)

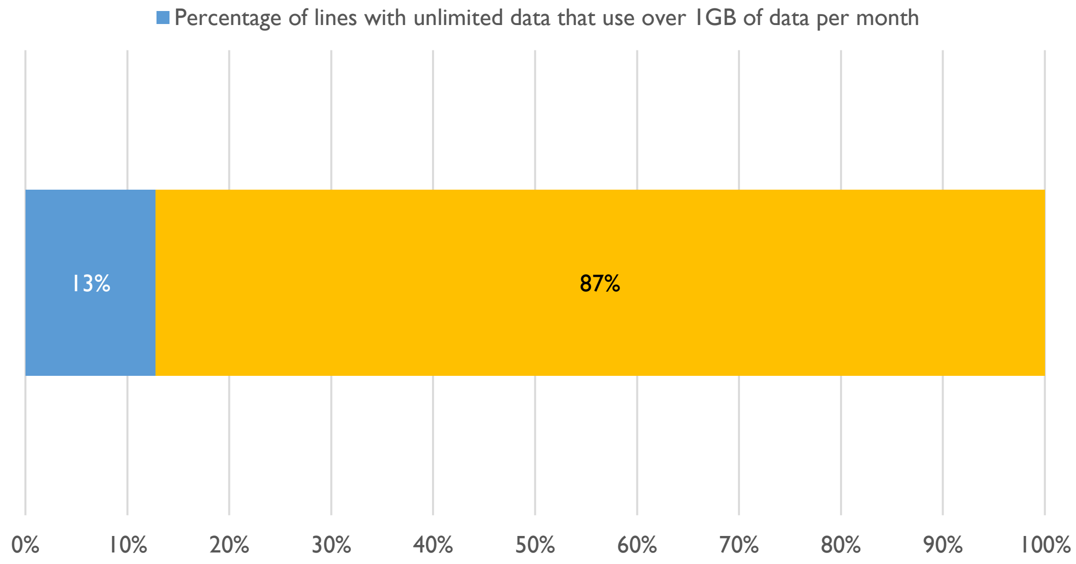


Source: Auditor analysis based on cost and usage data from Verizon Wireless.

Note: Monthly charges estimated by averaging monthly costs from April to June 2016. These are best estimates based on available data. We were not able to access cost and usage data for all lines with Verizon, nor could we accurately parse charges by category for the other wireless service vendors using available data.

It seems departments are generally unaware of the range of wireless service plans available from each vendor. As a result, they often choose unlimited data plans, which may not be necessary according to projected and actual usage of data by individual users. As can be seen in Exhibit 12, only **13%** of lines with unlimited data used more than 1GB per month.

Exhibit 12: Data Usage by Lines with Unlimited Data Plans/Features



Source: Auditor analysis based on cost/usage data and billing invoices from Sprint, AT&T, and Verizon.

Note: Percentages based on a total of 567 lines determined to have unlimited data. Monthly charges estimated by averaging monthly costs from April to June 2016. These are best estimates based on available data; we were unable to access cost and usage data for all lines from the wireless service vendors. There are likely other lines with unlimited data for which we did not have information, or for which we could not clearly determine the applicable data plan/feature.

The median data usage for lines with unlimited data plans was only **0.1GB**, and the average data usage was only **0.9GB**,[32] suggesting that much of the City's significant data-related charges are unnecessary. Based on programmatic needs and data usage over time, departments could save costs by either pooling data among these lines or downgrading their data plans.[33]

Greater Familiarity with Various Wireless Service Plans and Use of Vendor Tools Can Help Minimize Unnecessary Costs

City policy and procedures do not delineate how the City should maintain contact with mobile device vendors to control costs. In the current account management structure, in which departments open accounts and lines with vendors directly, some departments restrict themselves to flat-rate plans or other plans popular within their departments because they are not aware of the detailed plans available from each vendor—especially data and text plans. A working knowledge of various plans through regular communication with the vendors would allow them to make informed decisions about the most

[32] For context, according to AT&T, with 1GB users can send roughly 11,600 emails (25% with standard attachments) or stream about 4 hours of standard video. Several City lines with unlimited data plans used an average of over 25GB per month from April-June 2016.

[33] For example, according to the City's Sprint representative, a line could add 1GB to a pooled data plan for $19.99. Switching lines with low data use from unlimited plans to this plan could save $18 per line per month.

appropriate plans for departmental users based on projected usage and plan pricing.

Additionally, few departments utilize tools provided by vendors to analyze usage. Most departments either do not have access to or do not use vendors' online portals, where they can run vendor reports to conduct such analysis. Similarly, most department liaisons do not receive optimization reports, in which the vendors recommend plan changes based on usage in order to save costs; at least two departments with large accounts were not even aware of such reports. For one vendor, point persons who receive these optimization reports are often in different departments and, in such cases, do not appear to forward the reports to applicable department liaisons. Another vendor does not regularly send the City optimization reports, and the report accessible on its website was inaccurate at the time of the audit.

The City should work with vendors to make informed decisions about plans, including cost as a factor, and use vendor-provided tools to analyze usage and change plans to save costs. City policy and procedures should be updated accordingly.

A Clearer Oversight Structure and Guidance for Staff Can Help Departments Control Costs

Cell Phone Liaisons—typically Account Clerks or Analysts—are generally removed from the duties of line staff who have City-issued cellphones. As a result, they may be unfamiliar with usage patterns of certain positions or work groups, particularly in large departments, making it difficult for them to determine appropriate levels of usage and review costs for reasonableness. They may be reluctant to review bills and request personal use reimbursements from supervisors or other work groups because the authority to do so is unclear.

Furthermore, department liaisons are generally not trained on how to identify cost savings, work directly with vendors, and choose from available plans based partly on cost. Many liaisons are sent paper billing invoices up to hundreds of pages without being trained to access and analyze corresponding electronic datasets, making it unreasonably burdensome to manually identify patterns of underutilization, personal use, etc.

Minimal Oversight of Mobile Device Costs Based on Usage Results in Additional Costs to the City and May Enable Inappropriate Personal Use

By promoting active management of mobile devices—including suspending and deactivating unused or underutilized lines, and switching rate plans based on usage, we estimate the City can save at least **$189,000** per year (over 25 percent of the estimated total annual cost of wireless services), as seen in Exhibit 13 below.

Exhibit 13: Potential Cost Savings on Wireless Services

Cost-Saving Measure	Potential Cost Savings*	Notes
Deactivate or suspend zero- and low-use lines	At least $117,000 per year	Citywide, about 32% of lines had no voice, text, or data use over three months ("zero-use"). About 1% have average voice, text, and data usage at or below the 25th percentile over three months ("low-use").
Actively manage lines and adjust plans based on usage	At least $17,000 per year	Because departments receive minimal guidance on how to control costs related to mobile devices and most do not work closely with vendors, they do not actively manage lines to save costs based on analysis of individual and departmental usage. Select examples of the lack of active management include: • Many departments do not receive optimization reports due to lack of communication with vendors and the inappropriate assignment of City contacts to receive the reports. Thus, departments do not adjust rate plans based on vendor recommendations in such reports. • NASPO's nationally negotiated rate for unlimited data plans is $39.99, but the rate negotiated specifically in the State of California is lower, at $37.99. Some departments are paying $39.99 because they are not aware of the lower rate for the same plan. • A few departments have suspended lines that still accrue costs either because they were suspended *with billing* or because they were reactivated after reaching the limit for the number of days a line can be suspended. It should be noted that the City can fully deactivate and reactivate lines rather than suspending them, since governments do not accrue early termination fees on wireless service contracts.
Pool data based on data usage within departments and/or divisions	At least $55,000 per year	Pooling allows the sharing of data among many lines with various levels of usage. The total amount of data to be shared by the lines can be assessed by analyzing their average consolidated data usage. At least two departments have saved costs (about $39,000 per year in total) by pooling data among groups of lines.

Source: Auditor analysis based on cost and usage reports from Sprint, AT&T, and Verizon, as well as information gathered from interviews with the wireless service vendors and departments.

* Annual cost savings were estimated by averaging monthly costs and usage from April to June 2016, then multiplying this three-month average by 12 months. We were unable to access cost and usage data for all lines with each wireless service vendor; we would have likely estimated greater cost savings had we been able to access more complete reports. Savings from pooling data may overlap with cost savings from suspending or deactivating zero- and low-use lines. Departments would be best equip to determine whether lines with low data usage should be suspended/deactivated or pooled.

Active management and monitoring of costs and usage can also help insulate the City from employee abuse and negative publicity should such abuse take place. Aside from resulting in unnecessary overage costs, potential personal use among City employees could result in increased risk to the City. In reviewing high-use lines, we identified at least one individual who appeared to have been engaging in significant personal use of a City-issued cell phone.[34] The total bill for this individual's line averaged to about $130 per month from April to June 2016.

IT Oversight of Billing Management Could Facilitate More Effective Cost Control and Communication with Mobile Device Vendors

The City maintains foundation accounts[35] with Sprint, AT&T, and Verizon. It pays for around 70 distinct billing accounts.[36] These accounts are managed by about 30 individuals in various departments throughout the City. This sprawling structure for managing mobile device accounts has led to confusion in correspondences and transactions between the City and its wireless service vendors. IT oversight and coordination could assist in not only communicating with the vendors, but also saving costs citywide.

Limited Oversight of the City's Many Wireless Service Accounts Has Contributed to Billing Issues and Ineffective Communication with Wireless Service Vendors

The Sprint, AT&T, and Verizon account managers who oversee the City's accounts are each available to speak with liaisons in any City department. However, they primarily correspond with a few City employees who become the points of contact for other, unrelated departments. Several of these contacts have stated that they do not know why they have been designated as primary City contacts and/or that they do not believe it is appropriate for them to take up the role.

As noted earlier in this Finding, departments that may not be in regular contact with the wireless service vendors face difficulty in accessing bills and data, and understanding the full range of available plans. For instance, Verizon sends its monthly audits[37] to three individuals in the City who oversee Verizon accounts for all departments. It appears these individuals do not forward the reports to the applicable departments, perhaps because they may not know the appropriate contacts within those departments. As a result, the departments that do not

[34] We referred this case to the Office of Employee Relations for further investigation.

[35] A *foundation account* consists of multiple *billing accounts* paid for by various departments.

[36] We identified several City accounts not under Sprint's primary foundation account; the City's Sprint representative did not know these accounts existed. We also identified at least two accounts opened with procurement cards (discussed further below) and administered separately from the City's foundation accounts. In conjunction with (incomplete) account information provided by the wireless service vendors, we identified some accounts paid through the City's financial management software; however, not all transactions included account numbers. In light of such circumstances, it is possible there are additional wireless service accounts. Also note that roughly 5-10 of these accounts were canceled before or during the audit but are still maintained in the vendors' account databases.

[37] Verizon uses this term to refer to what we previously noted as *optimization reports.* These monthly audits consolidate Verizon's recommendations for all accounts in the City.

receive the monthly audits cannot benefit from the vendor's cost-saving recommendations.

The large number of City accounts also seems to have contributed to billing issues. Departments and vendors reported several instances in which a payment to one account was credited to another account, leading to over- and underpayments. Departments have noted that the process to correct such errors requires much time—one error took four months to resolve—and extensive correspondence with the vendors' billing units.

Additionally, the lack of centralized account management makes it burdensome, if not impossible, to determine the appropriateness of current and newly opened mobile device accounts. For example, Dolce Hayes Mansion maintains lines under the City's foundation account with Verizon and benefits from the City's government-discounted rates, although it appears Hayes Mansion staff receives and pays the bill for the relevant account. Both Hayes Mansion staff and the City's designated point of contact for this account do not know why it was included under the City's foundation account.

Further, two departments opened wireless service accounts with procurement cards. It was not clear to all departments that, according to Finance, City policy prohibits such purchases.[38] These departments, as well as others, were unaware that they could open accounts with AT&T and Verizon in addition to Sprint through the City's purchase order for wireless services.

Using Centralized Telecommunications Expense Management Software, IT Can Coordinate Citywide Changes to Control Costs

In light of the challenges associated with the City's current account management structure, we recommend IT correspond with both wireless service vendors and departments to ensure the cost-effective utilization of mobile devices throughout the City. Access to telecommunications expense management software would greatly assist IT in consolidating data on costs and usage for the City's many individual billing accounts.

Other jurisdictions utilize telecommunications expense management software through their Information Technology Departments to manage wireless service billings. For instance:

- Sacramento's software allows users to upload paper and electronic bills into the system to facilitate billing and usage analysis; to create cost allocation or other reports; and to create a database of all vendor-

[38] Our office alerted the two departments that City policy prohibits opening wireless service accounts with procurement cards.

offered plans, features, devices, and accessories.[39] Using the software, Sacramento's Office of the City Auditor identified $284,000 in estimated annual cost savings in an August 2014 report.

- Portland has used similar software to identify over $200,000 in estimated annual cost savings since November 2015 by pooling voice and data usage across departments.
- Aside from allowing billing and cost analysis, Denver's software also includes a central portal for ordering devices. Departments can access this portal directly to order devices, pending Denver's Information Technology Department's final approval.

Sacramento and Portland each have one central mobile device coordinator who performs cost and usage analysis of mobile devices throughout the city; the coordinator in Sacramento also oversees the use of MDM software in addition to other duties not related to mobile devices. For Sacramento, the Information Technology Department conducts high-level review of usage and costs; it defers to the relevant departments, which have more knowledge about specific programmatic needs, to make final determinations on suspending zero-usage lines and implementing other potential cost-saving opportunities.

A central point of contact for both departments and wireless service vendors could:

- Consolidate electronic cost and usage data from each wireless service provider and identify citywide trends, such as underuse and overuse of lines relative to their plans.
- Ensure that responsible individuals receive guidance to determine the most appropriate plans and vendors based on pricing and programmatic needs; to inform users what their plans include; and to identify cost savings, including utilizing vendor tools such as optimization reports.
- Ensure that the City communicates with its vendors on an ongoing basis about updated pricing, deals and discounts, and billing issues.
- Explore and coordinate potential large-scale, systemic changes to mobile devices, such as pooling minutes and/or data across departments, or transitioning employees' personal devices to City accounts at the government rate.[40]

[39] Sacramento currently pays $3,375 per month for the software. This includes software implementation and ongoing training from the vendor.

[40] Verizon Wireless has confirmed that it would be possible to terminate employees' personal lines and open new lines with the City using the same device.

Recommendation #15: In order to ensure that the City and/or departments control costs related to mobile device, the Information Technology Department (IT), in consultation with the Finance Department where applicable, should:

a) Administer citywide review of mobile device bills for usage and potential cost savings (e.g. zero- and low-use, plan optimization, minute and data pooling, etc.), potentially through the acquisition and utilization of telecommunications expense management software.

b) Clarify the management structure between IT and other departments in its updated *Mobile Device Policy* (see Recommendation #6)—including some level of departmental bill review—and provide procedures and annual trainings to responsible individuals.

c) Ensure that appropriate individuals within departments receive vendor reports and communications.

d) Ensure that all wireless service users in the City are informed of their plans' features and limitations.

This page was intentionally left blank

Finding 5 Cross-Departmental Coordination Is Needed to Foster Mobile Strategies Citywide

Summary

Mobile devices are a necessary tool for City staff and are utilized in a variety of ways across the City. Currently, several departments in the City are working independently to develop mobile applications to improve City services. According to best practices, organizations should plan and develop a mobility strategy comprehensively, rather than relying on individual initiatives. The City should create an interdepartmental working group to serve as a forum to share mobile solutions and applications and facilitate mobile strategies across the City.

Mobile Devices Have Become Necessary Tools for Business

It is clear that the mobile device has become a necessary tool—rather than a privilege—in today's economy. According to the Pew Research Center, in 2015 68 percent of U.S. adults owned a smartphone, 92 percent owned a cellphone generally, and 45 percent owned a tablet.[41] The International Data Corporation (IDC) forecasts that by 2020, mobile workers will account for over 72 percent of the total workforce in the United States.[42]

Both private and public sectors are working towards creating mobile workforces with seamless access to enterprise data and resources, enabling employees to work where they are most efficient. According to a 2015 survey by VMware on the *State of Business Mobility*,[43] most respondents "have already enabled basic individual productivity applications such as email, calendar, and secure browsing via mobile devices […] nearly two-thirds of companies surveyed report they are actively reengineering or have plans to reengineer a core business process…" Similarly, The Center for Technology in Government[44] found "[…] mobile is a top priority across the board and that agencies see its many impacts affecting three major areas: citizen services and participation, workplace skills and processes and interoperable collaborations."

[41] Monica Anderson, "Technology Device Ownership: 2015," Pew Research Center, October 29, 2015, http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

[42] "IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020," IDC, June 23, 2015, https://www.idc.com/getdoc.jsp?containerId=prUS25705415.

[43] VMware, *State of Business Mobility*, November 2015, http://www.air-watch.com/downloads/resources/VMware-State-of-Business-Mobility-Report-Nov-2015.pdf.

[44] James Costello, "Government in a Mobile World," Center for Technology in Government, State University of New York at Albany, 2011, https://www.ctg.albany.edu/publications/issuebriefs/mobile.

The City Should Coordinate Mobile Strategy Across Departments to Improve City Services

As discussed in the Background and Finding 1, mobile devices are a necessary tool for City staff and are utilized in a variety of ways across the City. Beyond communications, departments use mobile devices for group work, field work, and community outreach. Often, such uses of mobile devices requires re-imagining process workflows and may necessitate the development or procurement of applications and secure connections to backend systems, which are potentially resource intensive. In the future, the growth of mobile assets may cause the City to re-evaluate what the City assigns and pays for, such as whether to purchase desktop phones or full desktop computers for many employees.

Departments Are Working on Mobile Projects Independently Despite Facing Similar Obstacles

Currently, several departments in the City are working independently to develop mobile applications and business processes to improve City services. Staff in these departments have come across similar obstacles relating to data security, systems access, and limited budget and training—and have variously found solutions. While there is some interdepartmental consultation (e.g., Fire has consulted with ESD regarding the secure configuration of devices, and PRNS has consulted with Public Works regarding the use of asset management apps), it has generally been on an ad hoc basis. There is no central coordination of mobile strategies and initiatives within the City.

Departments have different levels of experience and expertise, but most agree there is a steep learning curve in managing mobile devices and implementing mobile projects. Some departments are stalled in implementation, and at least one department has expressed difficulty in moving beyond the pilot phase. Small departments, without internal IT, may be limited in their ability to fully utilize devices. Considering the similarities in applications of mobile devices across departments—field inspections, work order management, asset control—the City could benefit from coordinated development, pooling resources, and reducing duplicative efforts.

Interdepartmental Coordination Is a Best Practice in Mobile Strategy

According to best practices, organizations should plan and develop a comprehensive mobility strategy, rather than relying on individual initiatives. A 2012 White House report, *Digital Government: Building a 21st Century Platform to Better Serve the American People*, recommends the establishment of "a Digital Services Innovation Center and Advisory Group," explaining that:

> *Approaching [common] challenges as one government will enable agencies to focus their time and money on developing innovative, mission-facing solutions rather than re-inventing the wheel. Identifying opportunities for sharing existing solutions at agencies and building new solutions for government-wide use requires strong leadership, coordination, and support.*

The Administration, through the newly created Office of Civic Innovation, could help promote cross-departmental collaboration to realize mobility, efficiency, and service delivery improvements. An interdepartmental forum could provide a space for departments to identify common problems, share solutions, train staff, pool resources, vet ideas, coordinate interdepartmental projects, and set the pace for creating mobile-ready City systems. Support through the Office of Civic Innovation would be in keeping with its mission to "provide oversight, coordination and implementation support for City innovation projects."

Recommendation #16: To support staff training, pool resources, and foster departmental innovation, the Administration should create an interdepartmental working group to serve as a forum for departments to share mobile solutions and processes, and facilitate mobile strategies across the City.

This page was intentionally left blank

Conclusion

City employees use mobile devices (cell phones, smartphones, tablets, laptops, and hotspots) as necessary tools in their jobs, typically for work in remote offices or in the field. Mobile device benefits include enhancing workplace flexibility, improving communications, and connecting workers to City systems for field reporting or outreach. The City owns at least 4,000 mobile devices, with an estimated cost of roughly $3 million. In addition, wireless services cost at least $670,000 annually, and cellular and data stipends for nearly 500 employees who use their personal devices for City business cost roughly $250,000 annually. There are also an unknown number of employees who use their own personal devices for work without a stipend. The objective of this audit was to assess the cost, usage, and management of the growing number of mobile devices used by City employees in light of rapid advancements in mobile technologies and the City's changing technological needs.

To ensure that the City achieves the benefits from mobile devices while at the same time address any potential risks from these devices, the City should improve its inventory and stipend management practices; develop a mobile device policy to reflect current technologies and business needs; streamline the approval and ordering processes for mobile devices; provide that IT play a larger management and oversight role over mobile devices; and coordinate cross-departmental strategies to implement mobile solutions. This report has 16 recommendations.

RECOMMENDATIONS

Recommendation #1: To ensure appropriate controls over City-owned mobile devices (including cellphones, smartphones, hotspots, tablets, and laptops), the Administration should require departments to label City-owned mobile devices and maintain current inventories. The inventories should include the type of device, serial number, the name and ID of the employee to whom the device is assigned, the phone number (if applicable), the date of issuance, and the date returned (if applicable).

Recommendation #2: To ensure that cellphone stipends are cost-effective and reflect current technologies and the usage and needs of City employees, the Information Technology Department should work with the Finance Department to:

a) Provide guidance for departments on how to assess the cost-effectiveness of offering a stipend as opposed to issuing a City-owned device;

b) Update the eligibility criteria for stipends to reflect business need (i.e., the same criteria for City-owned devices) and delegate approval to the department level; and

c) Review and adjust the amount and structure of the City's cellphone and data stipends.

The Information Technology and Finance Departments should update City policy accordingly.

Recommendation #3: To ensure cellphone stipends are terminated for employees who no longer qualify for them, the Finance Department should annually generate a list of stipend holders and send it to departments for verification that employees on the list still qualify for stipends and that they do not also have City-issued cellphones.

Recommendation #4: The Finance Department should work with the Human Resources Department to revise the Employee Exit Checklist to include a requirement that department staff notify the Finance Department's Payroll Division to terminate a stipend when an employee transfers from the department or otherwise becomes ineligible for the stipend.

Recommendation #5: The Finance Department should:

a) Work with the City Attorney's Office to clarify City policy on the taxability of stipends and either eliminate non-taxable stipends, or provide guidance to department staff on what documentation is required for a stipend to be non-taxable.

b) If non-taxable stipends are continued, the Finance Department should review the authorization forms for employees for non-taxable stipends for required documentation to justify the non-taxable status of the stipends. Finance should then work with departments to compile any missing documents or change the status to taxable.

Recommendation #6: The Information Technology Department should develop a Mobile Device Policy to supersede the current Cellular Telephone Policy (1.7.4) to:

a) Reflect the use of all mobile devices by employees across the City, including both personal and City-owned cellphones, smartphones, tablets, hotspots, and laptops.

b) Clarify the specific duties and responsibilities of mobile device liaisons within departments who are tasked with managing such devices.

The new policy should cross-reference with the City's Information Security Policy, the Remote Access Policy, and any other relevant policies that relate to mobile devices.

Recommendation #7: To ensure consistent application of the Mobile Device Policy, the Information Technology Department should develop and provide periodic training for department liaisons on their specified administrative duties and responsibilities outlined in the policy for both City-issued and personal devices used for City business.

Recommendation #8: To address information security risks associated with mobile devices, the Information Technology Department (IT) should develop, and include in the Mobile Device Policy, guidelines and procedures for both City-issued and personally owned devices that identify:

a) The degree of access for various types of mobile devices and employee classifications in connecting to either cloud-based City services or to the City's network;

b) Any applicable support expectations by IT for personally owned mobile devices used for City business;

c) Any applicable user conditions, especially if personally owned devices may be enlisted on a mobile device management software; and

d) Any applicable IT controls over mobile devices, such as remote locking or wiping of device in case of theft or loss.

Any authorization forms, such as the Remote Access Authorization Form, should be updated accordingly.

Recommendation #9: The Information Technology Department should:

a) Develop user friendly guidelines on mobile device information security and include it as part of the *Mobile Device Policy*.

b) Establish periodic information security awareness trainings for all personnel who access the City's network on City-issued and personal devices.

Recommendation #10: The Administration should consider allowing short, infrequent personal calls by employees using City-owned cellphones, similar to the exception for such calls using City landline phones in the Personal Use of City Equipment policy. This exception should be included in the Mobile Device Policy.

Recommendation #11: To reduce ordering turn-around and demands on staff time, we recommend the Administration:

a) Allow departments to order mobile devices (cellphones, smartphones, hotspots, tablets, and laptops) and accessories directly, through appropriate citywide purchase orders;

b) Develop a process for IT or department staff to configure devices to meet information security standards in the *Mobile Device Policy*.

c) Update City policy accordingly.

Recommendation #12: To reduce ordering turn-around and demands on staff time, and to provide greater transparency and citywide inventory control, we recommend the Administration:

a) Explore tools to develop online approval form(s) for the approval of City-issued cellphones, smartphones, hotspots, tablets, and laptops, including whether the device will require remote network access, to be authorized electronically and saved in a centralized, searchable database; and

b) Revise the *Procurement of Laptops and Tablets Policy (*1.7.8) and reference the *Remote Access Policy* (1.7.3) accordingly.

Recommendation #13: To facilitate departmental budgeting and business need determinations, and ensure the prudent expenditure of public funds, we recommend the Information Technology Department establish and implement procedures to regularly update the City price list to accurately reflect the current discounted prices and technical specifications of available devices, and put an explicit link to tablet pricing on its intranet site.

Recommendation #14: To address the information security risks of mobile devices, the Information Technology Department (IT) should work with departments citywide to implement Mobile Device Management (MDM) software citywide for the devices that pose the greatest information security risks for the City. Specifically, IT should:

a) Prioritize devices that pose the greatest information security risks for the City to be enlisted on an MDM software, and work with departments to implement MDM software citywide for those devices;

b) Establish basic minimum standards or settings within the MDM software to protect City data within the software; and

c) Either directly manage mobile devices for departments or provide administrative access for departments to manage their own devices if they have the internal capacity to manage those devices.

Recommendation #15: In order to ensure that the City and/or departments control costs related to mobile device, the Information Technology Department (IT), in consultation with the Finance Department where applicable, should:

a) Administer citywide review of mobile device bills for usage and potential cost savings (e.g. zero- and low-use, plan optimization, minute and data pooling, etc.), potentially through the acquisition and utilization of telecommunications expense management software.

b) Clarify the management structure between IT and other departments in its updated *Mobile Device Policy* (see Recommendation #6)—including some level of departmental bill review—and provide procedures and annual trainings to responsible individuals.

c) Ensure that appropriate individuals within departments receive vendor reports and communications.

d) Ensure that all wireless service users in the City are informed of their plans' features and limitations.

Recommendation #16: To support staff training, pool resources, and foster departmental innovation, the Administration should create an interdepartmental working group to serve as a forum for departments to share mobile solutions and processes, and facilitate mobile strategies across the City.

APPENDIX A

Select Price Plans by Wireless Service Vendor as of October 2016

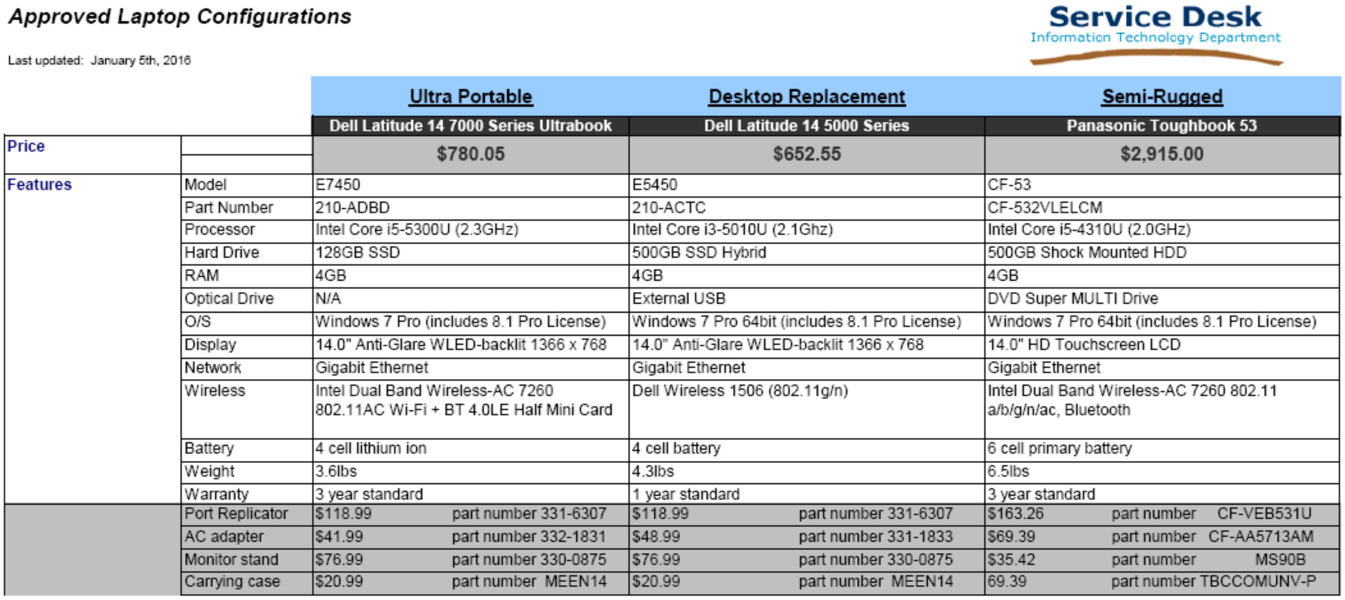
Plan Type	Price Plan	Sprint	AT&T	Verizon
Voice	Flat rate (consumption-based)	$0.06/minute	$0.06/minute	$0.06/minute
Voice	Unlimited	$19.99/month for basic cellphones Starting at $30.00/month for smartphones	$49.99/month	$54.99/month
Data	Mobile Broadband Unlimited	$37.99/month	$37.50/month for hotspots $39.99/month for tablets	$37.99/month
Data	Pooling	For $19.99 per line, each line adds 1GB to the pool Unlimited number of data-only lines	For 150GB pool, with maximum of 25 lines, $562.50 for first line $40 per additional smartphone; $20 per additional hotspot; $10 per additional tablet	For 150GB pool, $1025 Unlimited number of lines

Source: Auditor summary based on NASPO ValuePoint contract terms, vendor price plan lists, interviews with vendor account representatives, and interviews with City staff.

Note: Each vendor makes available a multitude of other rate plans with various specifications and prices.

APPENDIX B

IT Laptop and Tablet Price Lists

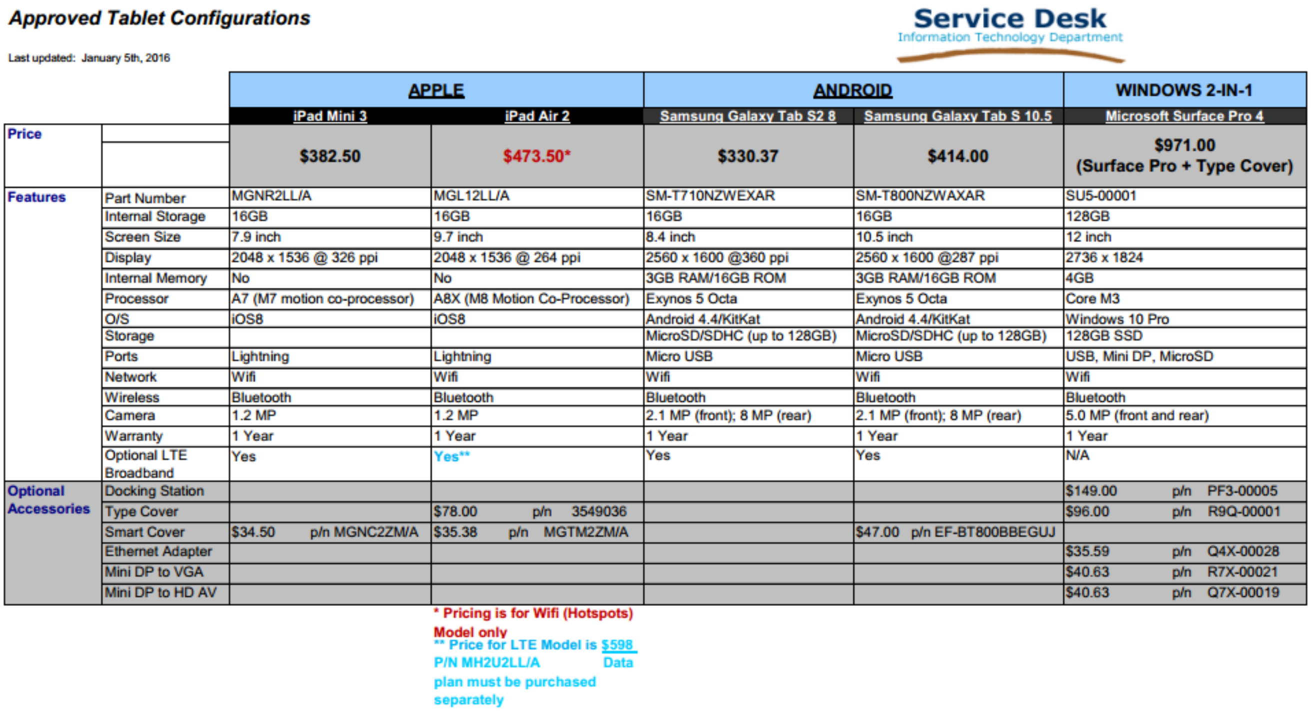


Approved Laptop Configurations

Service Desk
Information Technology Department

Last updated: January 5th, 2016

		Ultra Portable	Desktop Replacement	Semi-Rugged
		Dell Latitude 14 7000 Series Ultrabook	Dell Latitude 14 5000 Series	Panasonic Toughbook 53
Price		$780.05	$652.55	$2,915.00
Features	Model	E7450	E5450	CF-53
	Part Number	210-ADBD	210-ACTC	CF-532VLELCM
	Processor	Intel Core i5-5300U (2.3GHz)	Intel Core i3-5010U (2.1Ghz)	Intel Core i5-4310U (2.0GHz)
	Hard Drive	128GB SSD	500GB SSD Hybrid	500GB Shock Mounted HDD
	RAM	4GB	4GB	4GB
	Optical Drive	N/A	External USB	DVD Super MULTI Drive
	O/S	Windows 7 Pro (includes 8.1 Pro License)	Windows 7 Pro 64bit (includes 8.1 Pro License)	Windows 7 Pro 64bit (includes 8.1 Pro License)
	Display	14.0" Anti-Glare WLED-backlit 1366 x 768	14.0" Anti-Glare WLED-backlit 1366 x 768	14.0" HD Touchscreen LCD
	Network	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet
	Wireless	Intel Dual Band Wireless-AC 7260 802.11AC Wi-Fi + BT 4.0LE Half Mini Card	Dell Wireless 1506 (802.11g/n)	Intel Dual Band Wireless-AC 7260 802.11 a/b/g/n/ac, Bluetooth
	Battery	4 cell lithium ion	4 cell battery	6 cell primary battery
	Weight	3.6lbs	4.3lbs	6.5lbs
	Warranty	3 year standard	1 year standard	3 year standard
	Port Replicator	$118.99 part number 331-6307	$118.99 part number 331-6307	$163.26 part number CF-VEB531U
	AC adapter	$41.99 part number 332-1831	$48.99 part number 331-1833	$69.39 part number CF-AA5713AM
	Monitor stand	$76.99 part number 330-0875	$76.99 part number 330-0875	$35.42 part number MS90B
	Carrying case	$20.99 part number MEEN14	$20.99 part number MEEN14	69.39 part number TBCCOMUNV-P



Approved Tablet Configurations

Service Desk
Information Technology Department

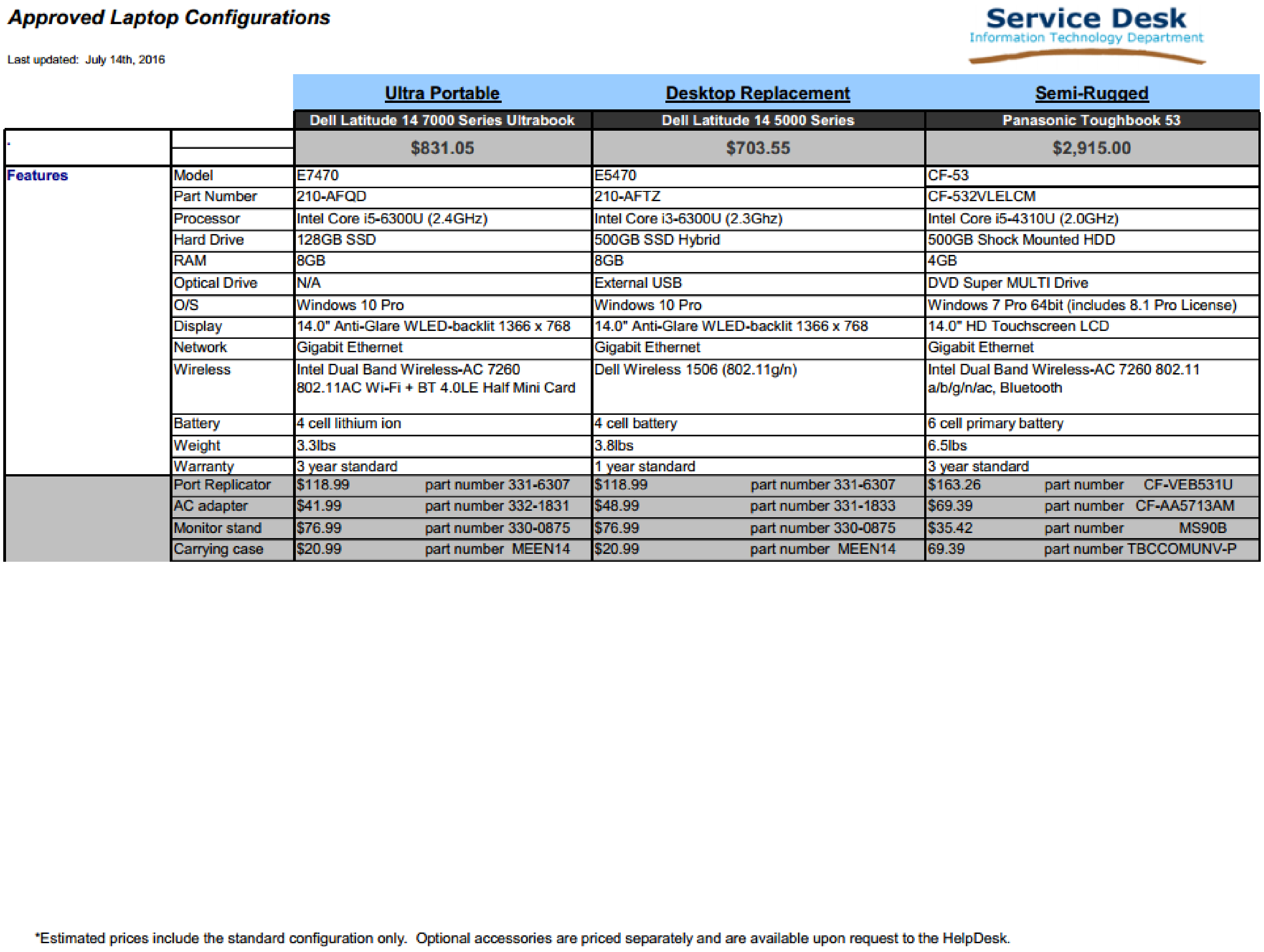
Last updated: January 5th, 2016

		APPLE		ANDROID		WINDOWS 2-IN-1
		iPad Mini 3	iPad Air 2	Samsung Galaxy Tab S2 8	Samsung Galaxy Tab S 10.5	Microsoft Surface Pro 4
Price		$382.50	$473.50*	$330.37	$414.00	$971.00 (Surface Pro + Type Cover)
Features	Part Number	MGNR2LL/A	MGL12LL/A	SM-T710NZWEXAR	SM-T800NZWAXAR	SU5-00001
	Internal Storage	16GB	16GB	16GB	16GB	128GB
	Screen Size	7.9 inch	9.7 inch	8.4 inch	10.5 inch	12 inch
	Display	2048 x 1536 @ 326 ppi	2048 x 1536 @ 264 ppi	2560 x 1600 @360 ppi	2560 x 1600 @287 ppi	2736 x 1824
	Internal Memory	No	No	3GB RAM/16GB ROM	3GB RAM/16GB ROM	4GB
	Processor	A7 (M7 motion co-processor)	A8X (M8 Motion Co-Processor)	Exynos 5 Octa	Exynos 5 Octa	Core M3
	O/S	iOS8	iOS8	Android 4.4/KitKat	Android 4.4/KitKat	Windows 10 Pro
	Storage			MicroSD/SDHC (up to 128GB)	MicroSD/SDHC (up to 128GB)	128GB SSD
	Ports	Lightning	Lightning	Micro USB	Micro USB	USB, Mini DP, MicroSD
	Network	Wifi	Wifi	Wifi	Wifi	Wifi
	Wireless	Bluetooth	Bluetooth	Bluetooth	Bluetooth	Bluetooth
	Camera	1.2 MP	1.2 MP	2.1 MP (front); 8 MP (rear)	2.1 MP (front); 8 MP (rear)	5.0 MP (front and rear)
	Warranty	1 Year	1 Year	1 Year	1 Year	1 Year
	Optional LTE Broadband	Yes	Yes**	Yes	Yes	N/A
Optional Accessories	Docking Station					$149.00 p/n PF3-00005
	Type Cover		$78.00 p/n 3549036			$96.00 p/n R9Q-00001
	Smart Cover	$34.50 p/n MGNC2ZM/A	$35.38 p/n MGTM2ZM/A		$47.00 p/n EF-BT800BBEGUJ	
	Ethernet Adapter					$35.59 p/n Q4X-00028
	Mini DP to VGA					$40.63 p/n R7X-00021
	Mini DP to HD AV					$40.63 p/n Q7X-00019

* Pricing is for Wifi (Hotspots) Model only

** Price for LTE Model is $598 P/N MH2U2LL/A Data plan must be purchased separately

Source: City of San José Intranet



Approved Laptop Configurations

Last updated: July 14th, 2016

Service Desk
Information Technology Department

		Ultra Portable	**Desktop Replacement**	**Semi-Rugged**
		Dell Latitude 14 7000 Series Ultrabook	**Dell Latitude 14 5000 Series**	**Panasonic Toughbook 53**
.		**$831.05**	**$703.55**	**$2,915.00**
Features	Model	E7470	E5470	CF-53
	Part Number	210-AFQD	210-AFTZ	CF-532VLELCM
	Processor	Intel Core i5-6300U (2.4GHz)	Intel Core i3-6300U (2.3Ghz)	Intel Core i5-4310U (2.0GHz)
	Hard Drive	128GB SSD	500GB SSD Hybrid	500GB Shock Mounted HDD
	RAM	8GB	8GB	4GB
	Optical Drive	N/A	External USB	DVD Super MULTI Drive
	O/S	Windows 10 Pro	Windows 10 Pro	Windows 7 Pro 64bit (includes 8.1 Pro License)
	Display	14.0" Anti-Glare WLED-backlit 1366 x 768	14.0" Anti-Glare WLED-backlit 1366 x 768	14.0" HD Touchscreen LCD
	Network	Gigabit Ethernet	Gigabit Ethernet	Gigabit Ethernet
	Wireless	Intel Dual Band Wireless-AC 7260 802.11AC Wi-Fi + BT 4.0LE Half Mini Card	Dell Wireless 1506 (802.11g/n)	Intel Dual Band Wireless-AC 7260 802.11 a/b/g/n/ac, Bluetooth
	Battery	4 cell lithium ion	4 cell battery	6 cell primary battery
	Weight	3.3lbs	3.8lbs	6.5lbs
	Warranty	3 year standard	1 year standard	3 year standard
	Port Replicator	$118.99 part number 331-6307	$118.99 part number 331-6307	$163.26 part number CF-VEB531U
	AC adapter	$41.99 part number 332-1831	$48.99 part number 331-1833	$69.39 part number CF-AA5713AM
	Monitor stand	$76.99 part number 330-0875	$76.99 part number 330-0875	$35.42 part number MS90B
	Carrying case	$20.99 part number MEEN14	$20.99 part number MEEN14	69.39 part number TBCCOMUNV-P

*Estimated prices include the standard configuration only. Optional accessories are priced separately and are available upon request to the HelpDesk.

Source: City of San José Intranet

CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: SHARON W. ERICKSON

FROM: Rob Lloyd

SUBJECT: SEE BELOW

DATE: December 8, 2016

Approved Date 12/8/16

SUBJECT: RESPONSE TO THE AUDIT REPORT – MOBILE DEVICES: IMPROVEMENTS NEEDED TO ENSURE EFFICIENT, SECURE, AND STRATEGIC DEPLOYMENT

BACKGROUND

Our residents and businesses expect us to be connected and accessible. City employees increasingly rely on mobile devices for everything from responding to sewer overflows with an in house mobile app on a tablet, to answering emails while in the field from their phone. Given the transition of today's workforce to mobile access and communications, the City's processes and tools must be improved to support those expanding needs in an easy, efficient, and cost effective manner. This includes reliable controls to secure the City's information assets as field-based work trends continue to grow.

The Administration thanks the City Auditor's Office for the insights and recommendations included in the Audit Report entitled, *Mobile Devices: Improvements Needed to Ensure Efficient, Secure, and Strategic Deployment.*

The Audit Report identified neither major mobile device losses nor major misuse of mobile devices. It is positive that despite more than a decade of budget deficits and under investments in technology, technical and functional staff reductions, and decentralization of mobile device management, the City's inventory shows areas of improvement but not critical issues.

The Administration agrees with almost all of the audit points and recommendations to consider new approaches. Drafts of a new *Mobile Device Policy* and a *Security Policy* are in progress and are part of the Information Technology Department (ITD) workplan to complete this fiscal year. These new policies, along with updates to existing policies related to technology, will provide the guidance necessary to ensure efficient, secure, and strategic management of the mobile devices as new technologies emerge and mobile usage increases.

Implementing Audit Report recommendations can require operational change or additional financing and staffing. Each audit recommendation was analyzed in terms of resources and changes required to implement and is designated as Green, Yellow, or Red.

Green items are either in the departments existing workplan or work already underway.

Yellow items will take more than 40 hours of additional work including research and policy/ordinance development. In addition, yellow items are reviewed to determine alignment with department workplans, magnitude of effort, departmental capacity, and other relevant prioritized issues.

Red indicates the item is not recommended or feasible (e.g., the item violates existing federal or state law, contradicts established Council policy or does not lie within the City's jurisdictional authority).

The Administration's response to each of the Audit Report's recommendations is presented below.

RECOMMENDATIONS AND RESPONSE

Recommendation #1: To ensure appropriate controls over City-owned mobile devices (including cellphones, smartphones, hotspots, tablets, and laptops), the Administration should require departments to label City-owned mobile devices and maintain current inventories. The inventories should include the type of device, serial number, the name and ID of the employee to whom the device is assigned, the phone number (if applicable), the date of issuance, and the date returned (if applicable).

Administration Response to Recommendation #1

The Administration agrees with this recommendation that going forward, new City-owned devices should be identifiable with pertinent information on City-owned mobile devices with limited exceptions.

ITD and other departments must have a means of maintaining an accurate inventory of current devices, type of device, serial number, the employee to whom the device is assigned, contact information (if applicable), the date of issuance, warranty dates, and the date returned (if applicable). Administration will examine options and the cost-benefit of an inventory software to be used City-wide, as well as explore with phone carriers the possibility of obtaining assignments and inventory reports for departments to use in managing their mobile device inventories.

Green – Labeling all new city-owned devices can be implemented within six months with limited exceptions.

Yellow – An inventory management solution may require the reallocation or addition of resources. This will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities. Should an inventory software be purchased, the inventory list would take longer to implement and firm-up processes —estimated to be 12 to 18 months, including budget timing. If software is not purchased to track over 4,000 mobile devices, departments will need approximately nine months to manually create or update their own inventory list to ensure all the information is complete and accurate. However, manual methods systemically fail over time as they consistently fall out of date.

Recommendation #2: To ensure that cellphone stipends are cost-effective and reflect current technologies and the usage and needs of City employees, the Information Technology Department should work with the Finance Department to:

a) Provide guidance for departments on how to assess the cost-effectiveness of offering a stipend as opposed to issuing a City-owned device;

b) Update the eligibility criteria for stipends to reflect business need (i.e., the same criteria for City-owned devices) and delegate approval to the department level; and

c) Review and adjust the amount and structure of the City's cellphone and data stipends.

The Information Technology and Finance Departments should update City policy accordingly.

Administration Response to Recommendation #2

The Administration agrees with recommendation 2a and will develop guidelines to prompt managers to assess the cost-effectiveness of offering a cellphone stipend versus issuing a City-owned cellphone or a wireless data service.

The Administration agrees with the recommendation to update eligibility for stipends to align with work on Recommendation # 2a. However, the Administration disagrees with fully decentralizing approvals to the department level. Continuing centralized approvals is important to ensuring continued adherence with policies, controlling costs, limiting liability related to use by non-exempt employees, and for consistency across departments. Centralized approvals allow for justifiable exceptions where there are critical business requirements at the department level. Administration will assess if centralization in a different staff area may be more effective.

The amount and structure of the City's cellphone and data stipends will be reviewed with the work on Recommendation # 2a. The City's new *Mobile Device Policy*, recommended by Administration to replace the *Cellular Telephone Policy*, will address employee use of personal devices for City business, as well as the evolving role of communications/technology stipends.

Green – Recommendation 2a and updating the eligibility criteria for stipends as detailed in 2b will be implemented within six months.

Yellow – For Recommendation 2c, updating the amount and structure of stipends may require the reallocation or addition of resources. This will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities. Any changes as a result of this evaluation may be subject to meet and confer.

Red – Delegating approval of stipends to departments as described in 2b is not recommended. The Administration would recommend that stipend approvals remain centralized.

Recommendation #3: To ensure cellphone stipends are terminated for employees who no longer qualify for them, the Finance Department should annually generate a list of stipend holders and send it to departments for verification that employees on the list still qualify for stipends and that they do not also have City-issued cellphones.

Administration Response to Recommendation #3

The Administration agrees with this recommendation, Finance and ITD will work together on processes to generate stipend reports at least annually and then work with departments to verify that employees receiving stipends still qualify for the benefit.

Departments will conduct a separate analysis to ensure that employees receive a stipend or a City-issued cellphone, but not both items.

Green – Recommendation 3 should be implemented within six months.

Recommendation #4: The Finance Department should work with the Human Resources Department to revise the *Employee Exit Checklist* to include a requirement that department staff notify the Finance Department's Payroll Division to terminate a stipend when an employee transfers from the department or otherwise becomes ineligible for the stipend.

Administration Response to Recommendation #4

The Administration agrees with this recommendation and will revise the *Employee Exit Checklist* to include a requirement that department staff notify the Finance Department's Payroll Division to review stipends when employees transfer departments and are no longer eligible for the benefit. Where continuation is merited, the process will allow staff to reassign benefit costs to the new department.

Green – Recommendation 4 should be implemented within three months.

Recommendation #5: The Finance Department should:

a) Work with the City Attorney's Office to clarify City policy on the taxability of stipends and either eliminate non-taxable stipends, or provide guidance to department staff on what documentation is required for a stipend to be non-taxable.

b) If non-taxable stipends are continued, the Finance Department should review the authorization forms for employees for non-taxable stipends for required documentation to justify the non-taxable status of the stipends. Finance should then work with departments to compile any missing documents or change the status to taxable.

Administration Response to Recommendation #5

The Administration agrees with this recommendation and will clarify City policy on the taxability of stipends and either eliminate the non-taxable stipends or provide guidance to departmental staff on the required documentations for a stipend to be non-taxable. Should non-taxable stipends be continued, the Finance Department will review the authorization forms and supporting documentation to ensure compliance with the City policy and ensure that all necessary documentation is submitted with the authorization form to avoid risk for the City.

Green – Recommendation 5 should be implemented within six months.

Recommendation #6: The Information Technology Department should develop a *Mobile Device Policy* to supersede the current *Cellular Telephone Policy* (1.7.4) to:

a) Reflect the use of all mobile devices by employees across the City, including both personal and City-owned cellphones, smartphones, tablets, hotspots, and laptops.

b) Clarify the specific duties and responsibilities of mobile device liaisons within departments who are tasked with managing such devices.

The new policy should cross-reference with the City's *Information Security Policy*, the *Remote Access Policy*, and any other relevant policies that relate to mobile devices.

Administration Response to Recommendation #6

The Administration agrees with the intent of this recommendation. The *Mobile Device Policy* will replace the current *Cellular Telephone Policy*. The new policy would reflect current uses of mobile devices by employees that are City-issued or personal devices and clarify specific duties and responsibilities of mobile device liaisons within departments. All authorization forms related to the use of mobile devices will be user-friendly and will be revised based on the new policy and cross-referenced with all relevant policies related to security, information and communication and these other policies will be updated accordingly.

Green – Recommendation 6 should be implemented within six months.

Recommendation #7: To ensure consistent application of the *Mobile Device Policy*, the Information Technology Department should develop and provide periodic training for department liaisons on their specified administrative duties and responsibilities outlined in the policy for both City-issued and personal devices used for City business.

Administration Response to Recommendation #7

The Administration agrees with this recommendation and should provide trainings annually or as requested to departmental staff on coordinating the purchase of a cellphone and initiating service, the reassignment of existing cellular phones, and phone carrier tools to track and control cellular phone costs. Employees assigned to manage mobile devices should be educated about the various policies related to the use of mobile devices and the numerous wireless service providers and available plans; the importance of maintaining a departmental inventory list of mobile devices; and receive instructions on how to surplus mobile devices. In addition, Administration will work with phone carriers to identify departmental contacts to access and/or send optimization reports periodically, allowing departments to cancel lines or change plan types to maximize cost savings.

Yellow – This recommendation can be implemented within 12 to 18 months if additional resources are allocated to develop and provide the city-wide trainings. This will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other city-wide and departmental funding priorities.

Recommendation #8: To address information security risks associated with mobile devices, the Information Technology Department (IT) should develop, and include in the *Mobile Device Policy*, guidelines and procedures for both City-issued and personally owned devices that identify:

a) The degree of access for various types of mobile devices and employee classifications in connecting to either cloud-based City services or to the City's network;
b) Any applicable support expectations by IT for personally owned mobile devices used for City business;
c) Any applicable user conditions, especially if personally owned devices may be enlisted on a mobile device management software; and
d) Any applicable IT controls over mobile devices, such as remote locking or wiping of device in case of theft or loss.

Any authorization forms, such as the *Remote Access Authorization Form*, should be updated accordingly.

Administration Response to Recommendation #8

The Administration agrees with this recommendation and the *Mobile Device Policy* will include guidelines and procedures for both City-issued and personally-owned devices regarding the degree of access, applicable support expectations and controls by the City, and applicable user conditions. All authorization forms related to the use of mobile devices would be user-friendly, revised based on the new *Mobile Device Policy*, and cross-referenced with all relevant policies related to security, information, and communication.

Green – All parts of the recommendation, with the exception of 8d, should be implemented within six months.

Yellow – For Recommendation 8d, mobile device management software options would need to be evaluated along with policy controls to determine the best solution to implement City-wide.

Implementation of mobile device management software by ITD or departments would be based on risk and cost, as not all mobile devices would need the software. This would require the reallocation or addition of resources and will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities. Recommendation 8d could take up to 12 to 18 months to implement.

Recommendation #9: The Information Technology Department should:

a) Develop user friendly guidelines on mobile device information security and include it as part of the *Mobile Device Policy*.

b) Establish periodic information security awareness trainings for all personnel who access the City's network on City-issued and personal devices.

Administration Response to Recommendation #9

The Administration agrees with this recommendation and the *Mobile Device Policy* will include user friendly guidelines on mobile device information security. ITD should develop and provide trainings with a focus on security awareness for all personnel who access the City's network on City-issued and personal devices.

Green – Recommendation 9a is expected to be implemented within six months.

Yellow – For Recommendation 9b, developing and providing appropriate security awareness training would require the reallocation or addition of resources and will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities.

Recommendation #10: The Administration should consider allowing short, infrequent personal calls by employees using City-owned cellphones, similar to the exception for such calls using City landline phones in the *Personal Use of City Equipment* policy. This exception should be included in the *Mobile Device Policy*.

Administration Response to Recommendation #10

The Administration disagrees with the recommendation to consider allowing personal use of City-issued cellular telephones. With very limited exceptions, City-owned equipment is to be used solely for official City business pursuant to several City Administrative Policy Manual sections, including but not limited to the Code of Ethics.

Red – Recommendation 10 is not recommended to be implemented.

Recommendation #11: To reduce ordering turn-around and demands on staff time, we recommend the Administration:

a) Allow departments to order mobile devices (cellphones, smartphones, hotspots, tablets, and laptops) and accessories directly, through appropriate citywide purchase orders;

b) Develop a process for IT or department staff to configure devices to meet information security standards in the *Mobile Device Policy*.

c) Update City policy accordingly.

Administration Response to Recommendation #11

The Administration agrees with this recommendation to allow departments to order mobile devices and accessories directly, through the appropriate city-wide purchase orders and with configurations appropriate to the risks. Departments will be responsible for labeling and maintaining an inventory of the City-issued mobile devices. A process will be developed for ITD or departmental IT staff to configure the devices to meet the security standards set by the *Mobile Device Policy* through the implementation of a mobile device management software should funding be available. The Mobile Device and the Procurement of Laptop and Tablet policies will include the approval process for the purchase of hotspots and other mobile accessories.

Green – Recommendation 11 is expected to be implemented within nine months.

Recommendation #12: To reduce ordering turn-around and demands on staff time, and to provide greater transparency and citywide inventory control, we recommend the Administration:

a) Explore tools to develop online approval form(s) for the approval of City-issued cellphones, smartphones, hotspots, tablets, and laptops, including whether the device will require remote network access, to be authorized electronically and saved in a centralized, searchable database; and

b) Revise the *Procurement of Laptops and Tablets Policy (*1.7.8) and reference the *Remote Access Policy* (1.7.3) accordingly.

Administration Response to Recommendation #12

The Administration agrees with this recommendation and will explore options for a city-wide business automation solution for the online approval form(s) that will be authorized electronically and saved in a centralized, searchable database. The *Procurement of Laptop and Tablet Policy* will be revised to reference the *Remote Access Policy*.

Yellow – Recommendation 12a may require the reallocation or addition of resources and will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities. Assuming that funding is identified, this recommendation would be implemented within 18 months.
Green – Recommendation 12b is expected to be implemented within nine months.

Recommendation #13: To facilitate departmental budgeting and business need determinations, and ensure the prudent expenditure of public funds, we recommend the Information Technology Department establish and implement procedures to regularly update the City price list to accurately reflect the current discounted prices and technical specifications of available devices, and put an explicit link to tablet pricing on its intranet site.

Administration Response to Recommendation #13

The Administration agrees with this recommendation and ITD will establish and implement procedures to regularly update the City's list detailing the list of approved manufacturers and models and reflecting the amount of discount off the manufacturer's list price.

An explicit link to the pricing for tablets has been added to Technology Procurement Details on the City's intranet site and can be found at http://www.sjcity.net/index.aspx?NID=364#laptops.

Green – Recommendation 13 is expected to be implemented within nine months.

Recommendation #14: To address the information security risks of mobile devices, the Information Technology Department (IT) should work with departments citywide to implement Mobile Device Management (MDM) software citywide for the devices that pose the greatest information security risks for the City. Specifically, IT should:

a) Prioritize devices that pose the greatest information security risks for the City to be enlisted on an MDM software, and work with departments to implement MDM software citywide for those devices;

b) Establish basic minimum standards or settings within the MDM software to protect City data within the software; and

c) Either directly manage mobile devices for departments or provide administrative access for departments to manage their own devices if they have the internal capacity to manage those devices.

Administration Response to Recommendation #14

The Administration agrees with this recommendation and mobile device management software should be used city-wide if funding becomes available. The software would be implemented on the mobile devices based on cost and risk as not all mobile devices would need the software. ITD would establish basic minimum standards for security within the mobile device management software or policy functions, providing a baseline of administrative oversight. Administrative access may be given by ITD to departments should departments have the resources necessary to manage their own mobile devices.

Yellow – For Recommendation 14, mobile device management software would need to be evaluated along with policy controls to determine the best software available to implement city-wide. Implementation of mobile device management software by ITD or departments would be evaluated based on risk and cost. This would require the reallocation or addition of resources and will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other City-wide and departmental funding priorities. Should funding become available, this recommendation could take up to 12 to 18 months to implement.

Recommendation #15: In order to ensure that the City and/or departments control costs related to mobile device, the Information Technology Department (IT), in consultation with the Finance Department where applicable, should:

a) **Administer citywide review of mobile device bills for usage and potential cost savings (e.g. zero- and low-use, plan optimization, minute and data pooling, etc.), potentially through the acquisition and utilization of telecommunications expense management software.**
b) **Clarify the management structure between IT and other departments in its updated *Mobile Device Policy* (see Recommendation #6)—including some level of departmental bill review—and provide procedures and annual trainings to responsible individuals.**
c) **Ensure that appropriate individuals within departments receive vendor reports and communications.**
d) **Ensure that all wireless service users in the City are informed of their plans' features and limitations.**

Administration Response to Recommendation #15

The Administration agrees with this recommendation and ITD, in consultation with the Finance Department, administer a City-wide review of the mobile device bills to manage costs. Staff will explore the use of telecommunications expense management software to assist with the review of the bills and will determine if the savings from using the software will be greater than the cost of the software. In addition, the Administration will work with phone carriers to identify departmental contacts to access and/or send any available optimization reports, as well as request carriers provide communications and/or trainings periodically on the wireless plan features and limitations. The *Mobile Device Policy* will detail the management structure between ITD and other departments and the roles and responsibilities.

Yellow – This recommendation can be implemented within 12 to 18 months if additional resources are added for staff to administer the city-wide review of the mobile device bills and provide trainings and communications related to the mobile devices. A cost-savings analysis will be performed to determine if a telecommunications expense management software should be purchased. The need for the additional resources will be evaluated by the Administration as part of the annual budget process in light of the City's budget outlook and other city-wide and departmental funding priorities.

Recommendation #16: To support staff training, pool resources, and foster departmental innovation, the Administration should create an interdepartmental working group to serve as a forum for departments to share mobile solutions and processes, and facilitate mobile strategies across the City.

Administration Response to Recommendation #16

The Administration agrees with this recommendation and an interdepartmental working group will be created to serve as a forum to share solutions and processes and facilitate mobile strategies.

Green – The recommendation is expected to be implemented within nine months.

CONCLUSION

We would like to thank the City Auditor for surfacing concerns and providing recommendations in this Audit Report. We value these recommendations and in the upcoming months, the Administration will identify changes in our city policies and procedures to improve the management of mobile devices. The benefits and potential costs to implement the audit recommendations will be evaluated by the Administration as part of the annual budget process.

COORDINATION

This response was coordinated with the Finance, Human Resources, and Environmental Services departments, Department of Transportation, City Attorney Office, Department of Public Works, City Manager's Budget Office, and the Office of Employee Relations.

Rob Lloyd
Chief Information Officer

For questions, please contact Rob Lloyd, Chief Information Officer at 408 535-3566