Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT
Report Number: 2015-005

FINAL REPORT - Review of Cobb County Mobile/Wireless Telecommunication Costs

January 28, 2015

Latona Thomas, CPA, Director
Andrea Clayton, Staff Auditor I
Steven Harper, Staff Auditor I
Barry Huff, Staff Auditor I (retired)

Table of Contents

COBB COUNTY INTERNAL AUDIT

Latona Thomas, CPA
Director

100 Cherokee Street, Suite 250
Marietta, Georgia 30090
phone: (770) 528-2559 • fax: (770) 528-2642
TDD/TTY: (678) 581-5429
latona.thomas@cobbcounty.org

January 28, 2015

MEMORANDUM

TO: David Hankerson, County Manager

FROM: Latona Thomas, CPA, Director

SUBJECT: **FINAL REPORT** - Review of Cobb County Mobile/Wireless Telecommunication Costs

Attached for your review is the subject final report. The objective of our audit was to determine if the County has the processes and procedures in place to manage the acquisition, accountability, and security of mobile/wireless devices (cellular and smartphones, AirCards[1], wireless-enabled tablets).

Impact on the Governance of the County

The use of mobile/wireless devices has become more pervasive in the workplace. The recommendations in this report will ensure that the County is using the devices as an effective and efficient tool used to increase the productivity of County employees, costs are minimized, and devices are accounted for and secured to protect the integrity of the County's network.

Executive Summary

The County does not have adequate controls to mitigate inherent risks in the use of mobile/wireless devices. Although there are policies in place to address the use of mobile/wireless devices, there is no enterprise-wide mobile device management strategy to regulate the use of mobile/wireless devices or any Bring Your Own Device (BYOD) policy to regulate and secure the use of personal devices used by employees while conducting County business. There is no centralized solution in place to provide an enterprise-wide method for managing mobile/wireless devices.

[1] AirCard® is a registered trademark name for a broadband mobile/wireless device that connects devices via a cellular network to the internet. We used this generic name to represent mobile/wireless cards used as Automatic Vehicle Locator (AVL) cards, mobile/wireless-enabled tablets, mobile/wireless modems, and mobile/wireless cards used in laptops. We also included devices that create mobile "hot spots" (MiFi) where several devices can connect mobile/wirelessly to access the internet.

We also determined that current policies and procedures did not ensure mobile/wireless devices were properly acquired, accounted for, or secured. Our review showed that:

- The County has not implemented an enterprise-wide approach to the acquisition of mobile/wireless devices. As a result, the County utilizes over 27 different phone plans and does not always use the contracted AirCard vendor.
- Documentation to support the business need for a device is not always maintained.
- Documentation was not always maintained to show that users were aware of the policies that govern the use of mobile/wireless devices.
- Unmanaged and untrustworthy[2] County-owned and personal phones are connected to the mail server and network.
- There is no Countywide approved employee reimbursement process for employees who use their personal phones for business purposes. The County has not determined whether the reimbursement process would be more efficient than owning phones.
- Department's inventory listings of mobile/wireless devices were inaccurate, incomplete, and/or did not follow the County's accountable equipment guidelines.
- Over 10% of the phones (68 of 642) and AirCards (84 of 805) showed no usage over a three-month period. Management decided that most phones are needed for backup purposes, alternate communication or emergency use; however, no written documentation was maintained to substantiate their decision. Service for 14 phones and 28 AirCards was discontinued, saving the County $1,252 a month. In addition, plan changes to another three phones resulted in $111 savings in monthly service charges.
- Controls need to be strengthened to ensure only authorized users have access to the County's mail service and network.

Recommendations

We recommended the creation of a Mobile Device Management/Security (MDM) policy to address the management and security of all types of mobile devices including cell phones. The policy should be consistent with and complement the County's security policy for non-mobile systems. The development of a BYOD policy should be incorporated within the MDM or as a standalone policy to address the use of personal mobile/wireless devices in the workplace. We also recommended:

- Centralizing management of mobile/wireless devices in one function that controls, manages and secures the devices and takes advantage of enterprise-wide cost savings that may be available.
- Using existing software capability to eliminate unauthorized devices from access to the network and implement a security profile for all mobile/wireless devices.

[2] Organizations should assume that all mobile devices are untrusted unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data. *Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124, Revision.*

- Implementing an enterprise-wide mobile device management software solution to help ensure all mobile/wireless devices are properly secured and monitored to protect the integrity of the County network.
- Evaluating whether the reimbursement of employees for the business use of their personal phone is a more effective and/or efficient alternative than using County-owned phones.

Response

We received a combined response to our draft report from the County Manager through the Support Services Agency, Information Services, and Finance Department Directors. They concurred with six of the eight recommendations, and proposed acceptable alternative solutions to the remaining two recommendations. All corrective actions are to be implemented by November 2015. The complete responses to the draft report are included in Appendices VI and VII. We will perform a follow-up in six months on the implementation of corrective actions.

A copy of this report will be distributed to managers affected by the report recommendations. Please contact me at (770) 528-2559 if you have questions.

Background

The County uses mobile/wireless devices to enhance communication between employees, stakeholders, the County networks, systems and the internet. In this report, when we refer to mobile/wireless devices, we are not only referring to regular cell phones whose capability is primarily the placing and receiving of calls, but also to smartphones[3], tablets[4], wireless-enabled devices that can connect to the County network to retrieve mail, contacts, calendar information and access data in the users' authorized workspace on the network.

In June 2013, the County spent $41,698 on mobile/wireless resources including feature[5] and smartphones, AirCards, pagers and reimbursement to employees for the business use of their personal mobile/wireless devices. In order to ensure we identified all the mobile/wireless related expenditures, we categorized and totaled all the payments to mobile/wireless communication vendors. Annualizing the monthly expenditures resulted in mobile/wireless telecommunication cost for FY2013 of approximately $500,000.

According to accounting records, in Fiscal Year (FY) 2013, the County spent approximately **$303,040**[6] for *Wireless & Portable Telephone Service (Expenditure Object Code 6385)*; however, we identified approximately $200,000 in other mobile/wireless expenditures charged to different expense codes other than *Wireless & Portable Telephone Service*. See report section ***Misclassification of Mobile/Wireless Device Expenditures*** on page 25 for a more detailed explanation. The result of our initial analysis is below.

Monthly Expenditures by Device

Device Type	Description	Monthly Cost	Number of Devices
Phones	Mobile phones, some with data plans and text messaging.	$14,291	625
AirCards	Broadband modems that allow devices to connect to the internet using a cellular connection.	$24,578	805
Pagers	Wireless telecommunication devices that receive and display numeric or text messages, or receive and announce voice messages.	$279	155
Reimbursed Devices	Some departments reimburse their employees for the business use of their personal phones.	$2,550	54
Total		**$41,698**	

Table 1 - Source: June 2013 invoices from Accounts Payable records, County Financial System.

[3] A mobile phone with more advanced computing capability and connectivity than basic feature phones including a media player, a digital camera, GPS navigation unit, touch screen computer, including web browsing, Wi-Fi, and 3rd-party apps.
[4] A tablet is a computer contained in a single panel that is operated through a touch screen.
[5] Feature phones do not have the computing capability of smartphones, only voice, messaging and text.
[6] Total of expenditures in expense object code 6385, Mobile/Wireless & Portable Telephone Services for FY2013.

The following is a more detailed breakdown of the telecommunications costs. To provide more up-to-date information, we updated the phone data using April and May 2014 invoices (see Table 2) anticipating it was more subject to change than the AirCards, pagers, and employee reimbursement data. The remaining information is based on the June 2013 invoices (Tables 3-5).

Cellular Phones

AT&T provides service for 80% of the phones used in the County. Eighty-four percent (435) are established within three types of legacy pool plans. The pool plans are contracts where numerous cell phones are assigned and share the minutes included within the plan. These pool plans usually have several thousand minutes of purchased voice minutes. A per phone fee is paid each month whether the phone is used or not. Extra charges are assessed for smartphone data plans and messaging.

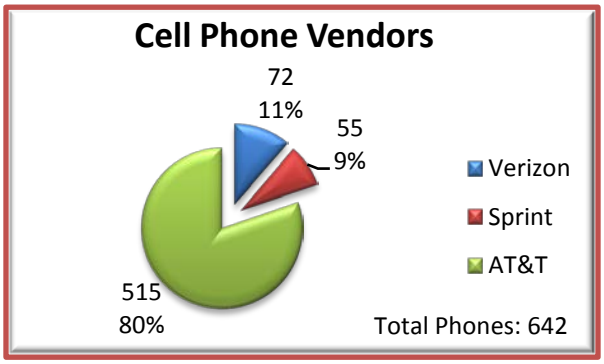

Chart 1 - Source: April and May 2014 invoices from accounts payable records, County Financial System

Nine additional AT&T plans, seven Verizon plans and eight Sprint plans provide service for the remaining 207 phones. These pool plans have much lower voice minutes to share with fewer (as low as one) phone user(s). Some have data and messaging options and often involve the use of a smartphone (i.e. iPhones).

Based on our revised analysis, we determined that there were 642 County-owned feature and smartphones costing $14,568 monthly using three different vendors—Verizon, Cingular (AT&T), and Nextel (Sprint). See Table 1 on next page.

Number and Monthly Cost of Phones

Dept/Office	Total Phones	TYPE		Amount
		Smart	Feature	
Community Development	27	3	24	$931.91
County Manager	2	2		$114.91
Dept. of Transportation	30	6	24	$1,243.14
Dept. of Public Safety[7]	86	26	60	$2,939.63
Administration[8]	***3***		**3**	***$59.52***
Animal Control	***8***	***1***	***7***	***$197.69***
E911	***21***	***6***	***15***	***$718.55***
Police	***52***	***19***	***33***	***$1,924.21***
Training Center	***2***		**2**	***$39.66***
Economic Development	1	1		$57.46
Elections	217[9]	3	214	$640.08
Extension Service	2	2		$114.91
Fire	55	21	34	$2,321.24
Human Resources	1	1		$57.46
Information Services	35	2	33	$726.32
Juvenile Court	42		42	$736.71
Library	5	1	4	$151.28
Parks	7	4	3	$249.19
Public Services	1	1		$57.46
Purchasing	1	1		$57.46
Senior Services	2	2		$114.91
Sheriff	6	6		$255.03
Superior Court	2	2		$131.61
Support Services	74	34	40	$2,410.44
Administration	***1***	***1***		***$57.46***
Fleet	***7***	***2***	***5***	***$246.54***
Property Management	***66***	***31***	***35***	***$2,106.44***
Tax Assessor	3	2	1	$134.12
Water	43	2	41	$1,123.16
Grand Total	**642**	**122**	**520**	**$14,568.43**

Table 2 - Source: April and May 2014 invoices from accounts payable records, County Financial System

[7] Includes three AT&T invoices (DPS, Police, E911) managed in the office of Public Safety.
[8] Items in bold italic are a subset of the previous non-italic line item and not included in totals.
[9] 201 of these feature phones are in suspense costing $.01 each per month while not in service during elections.

AirCards[10]

AirCards are primarily used in Water, Police, Transit (Bus) and Fire Department vehicles to track their location and usage and provide connectivity to the internet, the County network and other systems. Employees use other AirCards to receive and transmit data from tablets or laptops. The County usually pays a monthly access fee of $38.01 for each card; although Transit pays as little as $7 per month for cards used in their buses. Each card typically has a data usage limit and the County is charged for any use over this limit. The monthly per card fee is paid regardless of whether the card is used. The following chart shows the number of AirCards by vendor.

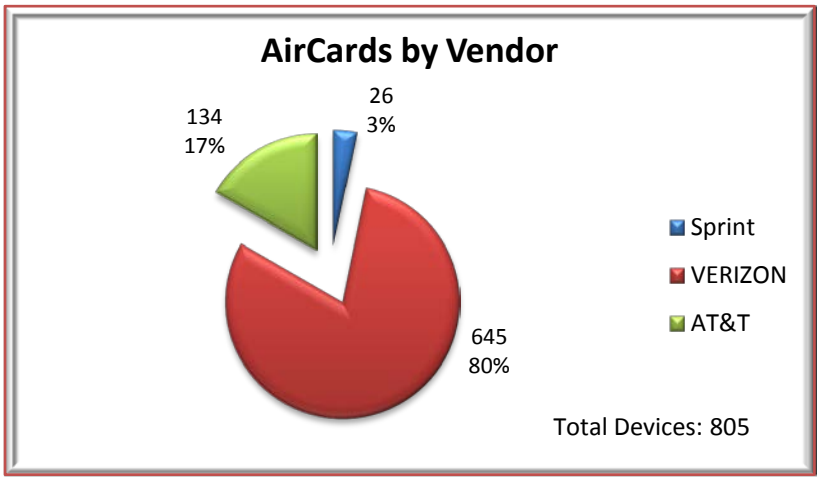

Chart 2 – Source: June 2013 invoices from accounts payable records, County Financial System

The table on the next page shows the number of AirCards per department/office.

[10] An AirCard® (aka broadband AirCard, cellular AirCard, AirCard modem, internet AirCard, mobile/wireless AirCard) is a high-speed mobile/wireless broadband card that gives users mobile Internet access using their cellular data service. Although the name AirCard is a registered trademark for Verizon's version of the card (Verizon AirCard 555), many people also use the word to signify other types of mobile broadband cards. ***Source:*** ***http://mobileoffice.about.com/od/glossary/g/aircard.htm***

Departments/Offices with AirCards

Departments/Offices	*AirCards*	*Monthly Cost*
800 MHz	3	$128.97
Animal Control	2	$76.02
Business License	4	$152.85
Clerk of Superior Court	1	$65.00
Code Enforcement	10	$380.10
Community Development	2	$90.77
Department of Transportation	4	$174.04
E911	7	$276.03
Emergency Management Agency	5	$190.05
Erosion Control	5	$190.05
Fire Department	71	$2,701.99
Fleet Management	5	$125.77
Information Services	5	$190.05
Community Development, Inspections	22	$836.22
Community Development, Planning	1	$38.01
Police Department	245	$9,312.53
Property Management	2	$76.02
Risk Management	7	$176.46
Sheriff	86	$3,269.42
Solicitor - Victim Witness 5%	1	$37.98
CobbWorks	16	$647.84
Tax Commissioner	1	$38.01
Traffic Mgt.-Signal Timing & Planning	14	$532.14
Transit	151	$1,118.10
Water	135	$3,753.21
Grand Total	**805**	**$24,577.63**

Table 3 - Source: June 2013 invoices from accounts payable records, County Financial System.

Pagers

Our review showed that the County paid $279 a month for 155 pagers used in various departments/offices. The pagers are useful for employees on 24-hour call, who interact with the public and do not want to give out their personal cell number or do not have a cell phone. In addition, DOT uses a pager circuit to send instructions to their school flasher system[11]. The table on the next page shows the departments/offices using pagers.

[11] Signs used in school zones to notify drivers of slower speed requirements.

Departments/Offices with Pagers

Departments/Offices	Pagers	Per Pager	Monthly Cost	Other Fees	Total
Water	107	$1.65	$176.55	$9.32	$185.87
Parks	35	$1.65	$57.75	$3.38	$61.13
	1	$3.95	$3.95		$3.95
Senior Services	1	$1.65	$1.65	$0.10	$1.75
DOT	3	$3.95	$11.85	$0.46	$12.31
Sheriff	3	$1.00	$3.00	$0.65	$3.65
	4	$1.65	$6.60		$6.60
	1	$3.95	$3.95		$3.95
Total	**155**				**$279.21**

Table 4 - Source: June 2013 invoices from accounts payable records, County Financial System.

Employee Reimbursement for Personal Use of Phones

In addition to County-owned cell phones, the County reimburses various employees for the business use of their personal phones. We identified 54 employees in eight departments or offices that received reimbursement for personal use of their phones totaling **$2,550** (as of June 2013). There is no official Countywide policy for the reimbursement of employees and there was no consistency between the departments and offices for what they reimbursed. Some used a standard amount (i.e. $30), while others were reimbursed for the full amount of their bill. Review of a sample of requests for reimbursement showed employees provided a copy of their phone bill as support for the requested amount. The table below shows the departments or offices that reimburse their employees, along with the estimated monthly total amount. Note: The DOT and BOC reimburse employees for data charges only.

Employees Receiving Reimbursement for Phone Use

Departments/Offices	Monthly Amount	Number of Employees
Circuit Defender	$160.48	1
Communications	$320.00	6
District Attorney	$600.00	20
Department of Transportation	$230.21	7
Board of Commissioners (BOC) – data only	$40.00	1
Juvenile Court	$377.96	5
Magistrate Court	$75.00	1
Sheriff	$745.96	13
Grand Total	**$2,549.61**	**54**

Table 5 - Source: June 2013 invoices from accounts payable records, County Financial System.

The scope of our audit covered all departments under the County Manager's direction. Elected officials' data is shown for informational purposes only. Costs are based on invoices paid in June 2013, except where noted otherwise. Detailed information on our audit objective(s), scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix III.

Results of Review

In October 2005, the County issued the Information Technology Security Standards (ITSS) and the Electronic Communications and Security Policy (ECSP) to provide an understanding of the expectations and procedures to protect Cobb County Government's computer information systems, networks and data stored on any County computing device. In January 2007, the Cellular Phone Policy (CPP) statement was issued to provide guidelines for the issuance, use, administration, and control of cellular telephones for the County. Several departments augmented these policies with their own departmental policies, procedural manuals and instructions governing cell phones and other mobile/wireless devices. These documents provide the overall Countywide framework for controls over the administration of cell phones and computing devices. Our review determined that these documents are not adequate to provide the processes and procedures to manage the acquisition, accountability, and security of all mobile/wireless devices.

The use of mobile/wireless devices in the workforce is increasing significantly. The County is providing more mobile/wireless technology to employees to improve productivity and efficiency. In addition, with the consumerization[12] of Information Technology (I.T.), many employees are utilizing their own mobile/wireless devices[13] rather County-owned devices that provide fewer features than they are accustomed. Some employees would rather avoid carrying more than one phone or want the convenience of accessing their work email account using their personal mobile/wireless device. With the proliferation of these devices and the risks they present to the integrity of our computer network, there is a need for a more effective and efficient process to manage and secure these devices.

Current Policies and Procedures Do Not Provide For an Effective and Efficient Enterprise-Wide Management of Mobile/Wireless Resources

We researched the best practices from other government entities, jurisdictions and professional organizations for policies and procedures that govern the use of mobile/wireless devices. We compared the information to the County's current policy statements.

We determined the current policies should be updated and enhanced to provide additional guidance on the acquisition, accountability and security of mobile/wireless devices. The ITSS needs updating to address the use of smartphones and tablets that require additional security consideration from the 'computing devices' referred to in the policy. Although smartphones and tablets can be considered computing devices by definition, the policy does not take into consideration the additional procedures and processes that are required to manage these devices over their predecessor, the Personal Digital Assistant[14] (PDA).

[12] See Glossary, Appendix II for explanation. Consumerization of IT - A Webopedia Small Business IT Definition

[13] How Enterprises Are Capitalizing On The Consumerization Of IT - Forbes

[14] See Glossary, Appendix II for explanation

In addition, the CCP should be replaced with an overall **Mobile Device Management/Security Policy (MDM)** that addresses the current trend in the use of mobile/wireless devices and the associated risks. Best practice and industry experts suggest an organization have a security policy that defines the rules, principles, and practices that govern the management of mobile devices, regardless if issued by the organization or owned by individuals. The policy should cover the full life cycle of a device from issuance to the user to retrieval after dismissal, transfer, or similar event.[15]

Bring Your Own Device (BYOD) provisions should be included in the policy or a standalone policy to provide guidelines for the use of personal devices in the workplace. The BYOD should have procedures for employee reimbursement and specify security guidelines.

Recommendation

The Information Services Director should:

Recommendation 1: Create a new Mobile Device Management/Security policy that addresses the acquisition, accountability and security of mobile devices including those that are personally owned. Consult the suggested recommendation of the National Institute of Standards and Technology or other subject matter experts in the development of the statement.

Items that should be included in the new MDM policy statement are described under the four sections that follow which addresses controls over acquisition, accountability and security as well as other issues concerning proper classification of mobile/wireless expenditures and procedures for paying mobile/wireless invoices.

Auditee Response: **Concur** with the recommendation to develop a County Mobile Device Management/Security policy that address the acquisition, accountability, and security of mobile devices including those personally owned and used by County staff in conducting County business. The IS Director will create a MDM policy that includes guidelines for employee owned devices (BYOD) being used for Cobb County business. The IS Director will coordinate with other agencies/departments currently managing their own devices to develop a standard enterprise policy (see Recommendation 6). **Target Date: 30 November 2015**

Current Processes and Procedures Over Acquisition of Mobile/ Wireless Devices are Not Adequate

Our audit testing showed a lack of consistency in the methodology of how phones are acquired. Documentation is not consistently maintained to verify users are aware of the cellular phone policy guidelines and whether managers determined the business need prior to granting the use of a mobile/wireless device. Employees are also using their personal phones to conduct County business without any enterprise-wide guidance.

[15] Guidelines on Cell Phone and PDA Security, National Institute of Standards and Technology, Special Publication 800-124

Inconsistent Methods Used to Acquire Phones

We surveyed offices (e.g. departments/agencies, County Manager, Emergency Management Agency (EMA), Clerk's Office) in the County to determine how they acquire their mobile/wireless devices. We determined that approximately half acquire them directly from the vendor while the other half (mostly offices with one or two devices) used Information Services to acquire their devices.

Because of the decentralization of device management, there was a lack of consistency in the plans used to acquire phones. Our review showed we currently have 27 different phone plans to accommodate the 642 phones and several different types of data and messaging plans for the 121 smartphones. Because there is no centralized source for acquisition that is apprised of the best plans from an enterprise-wide perspective, the County cannot streamline the type of plans used and take advantage of current plan packaging that could potentially result in financial savings for the County.

The legacy plans provide large blocks (i.e. 5,000; 12,000; 20,000; etc.) of voice minutes and were designed for old analog phones. Most departments have their own plan; however, some departments with few phones are combined on the same plan. We analyzed the voice usage for the plans over a three-month period and the average usage for the plans was under 45%. We discussed our current plans with the AT&T representative who believes the County can achieve some savings by utilizing new smartphone bundle plans and consolidating all the accounts into one.

We determined that designated department personnel have the capability to order mobile/wireless devices using the vendor's web portal. We did not identify any documents that explained how the employees were identified nor how their actions are monitored. Based on the results of our survey, the practice of departments/offices ordering their own phones through the portal or a representative continues without any oversight or monitoring outside of the respective department/office.

Our recommendation (Recommendation 7, Page 26) to centralize mobile/wireless device management will create a function that is aware of the current mobile/wireless environment and ensures the County takes advantage of the best service options presented by mobile/wireless vendors.

Cellular Phone Policy Statement Acknowledgment Forms are Not Maintained

The CPP requires all users to sign a form acknowledging they have reviewed and understand the policy. To determine if the forms were maintained, we judgmentally selected five departments/offices that have 282 (64%) of the 441 active phones and inquired whether they maintained copies of the acknowledgement forms. Three of the five departments/offices with 164 phone users (58%) did not maintain copies of the forms. Employees are also required to acknowledge they have reviewed the ITSS and ECSP policy statements. We determined that none of the offices maintained the acknowledgement forms for the ITSS and ECSP. Most believed the forms are maintained in the employee's personnel files located in Human Resources (HR) because the forms are signed during orientation. HR confirmed that the policies are discussed during orientation. Effective 2010, each new employee signs a form acknowledging receipt of the Employee Handbook that contains copies of the policies.

Acknowledgement forms for employees hired prior to the effective date referenced above should be maintained in the respective department files. It is important that employees be informed of their expectation in using cellular and other mobile/wireless devices, especially those that connect to our network. In addition, all employees should be periodically reminded to use mobile/wireless devices responsibly and in accordance with established policies. These actions are an integral part of an overall security process.

Business Need Was Not Documented and Maintained

It is the responsibility of the department head to determine the business need prior to approving a written request for a mobile/wireless device. Only one of the five offices sampled stated that they maintained approval documents for all phone users. The other four offices admitted they either did not maintain the approval documents or only had some of the required documents on file. Managerial approval of mobile/wireless devices helps ensure that only employees with a business need are issued devices and the employee gets the proper device to enhance their productivity at the lowest cost to the County.

The new MDM policy should require a new form where business need is documented and the type of device and services required enumerated. Users can acknowledge they are aware of all policies pertaining to the use of the device or the policies can be incorporated into the 'terms of use'[16] statement which must be accepted before the device is allowed to access the network through a mobile device solution (see discussion under 'Mobile Device Management Software', page 23 of report).

No Guidelines for Employee-Owned Phones in the Workplace

In addition to County-owned phones, our review identified instances where employees used their personal phones to conduct County business and/or access their County emails. Since there are no established Countywide guidelines, there are inconsistencies in how personal phones are utilized and additional security concerns are created. See page 19 for discussion on additional security risks.

In some instances, the County paid for the phone service or reimbursed the employee for the cost of their service. In other instances, the employee received no compensation for the business use of their personal phone. We also noted that some employees paid for upgrades to phones that offered more features than the County-issued phones, which brings into question ownership issues. The inconsistency of how personal phones are managed between departments/offices is discussed below. Guidelines for use of personal phones should be included in the new MDM policy as stated in Recommendation 1, Page 9.

Personal Phones Connected to the County Email

We determined that some employees request that I.S. set up their personal phones to access their County email while others configure their phones without I.S. assistance, knowledge, or approval. At the time of our tests, I.S. did not have a way to determine a complete list of employees with a direct connection to the mail server from a personal mobile/wireless device, but they did provide a file that contained 70 approved requests for email access on a personal phone.

[16] Rules which one must agree to abide by in order to use a service.

I.S. was in the process of installing the 2010 version of the mail client software, Microsoft Exchange[17], which will give them the capability to limit who has access to the mail server and establish a security profile for these mobile/wireless devices. We used one of our personal cell phones to test whether employees could set up their own phone to get direct mail access. After obtaining the County's web server name from a non-I.S. employee, we were able to establish a connection. The Microsoft Exchange software did require that we accept the security 'terms of use' during our setup, but we determined that I.S. has not developed a security profile or strategy for granting access to the mail server.

The County's network and data is vulnerable in this area because we do not have exclusive control over who connects to our mail server via mobile/wireless devices and we have not established a Countywide security profile to reduce the risk of exposure of our network to untrustworthy/unmanaged devices that connect to the web mail server. Organizations should assume that all mobile devices are untrusted unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data[18].

In addition, having unauthorized employees accessing their email accounts after normal business hours could be perceived as working without compensation leaving the County vulnerable to penalties for violating provisions of the Fair Labor Standards Act[19] which requires the payment of overtime for all nonexempt employees who work more than 40 hours in a week. Also the County's Compensatory Leave Policy allows a covered employee to accumulate compensatory leave at the rate of 1.5 hours credit for each hour worked over his or her regularly schedule hours each pay period. Management cannot ensure that this practice is not occurring unless they have the ability to limit who has access to the email server. Recommendation 4 on Page 21 provides a suggestion on how to ensure only authorized users have access to the mail server.

Personal Phones, Service Paid Directly By the County

Some employees are using their personal phones and the County pays the service. We do not have a policy or procedure in place to guide the use and security over these phones. Controversy may arise when the County tries to specify the scope of use and subject these phones to any security provisions. The new MDM policy should provide guidelines on how to handle this situation if permitted in the future.

In addition, some employees use their personal phones to answer calls transferred from their assigned County-owned phone. This allows them to answer calls to their County phone number without carrying two phones. Although this practice does not incur any additional cost to the County, departments should ensure the user has the appropriate plan to minimize the cost. For example, we identified two users in one department that transferred their calls but had smartphone plans costing a total of $82.75 per month. The department subsequently changed the plans of three users ($82.75 + $44.26 = $127.01) to the basic feature phone plan (3 x $5.26 = $15.78) saving the County $111.23 in monthly service charges.

[17] See Appendix II, Abbreviations and Glossary for further explanation.
[18] Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124, Revision 1
[19] United States Department of Labor - http://webapps.dol.gov/dolfaq/go-dol-faq.asp?faqid=320

Recommendation

Department Managers should:

***Recommendation 2*:** Identify all users who only use their County phone number to transfer calls to their personal phone and ensure they are assigned to the least costly phone plan.

Auditee Response: **Concur** with the recommendation for Department Managers to identify all users who only use their County phones to transfer calls to their personal phones and ensure they are assigned the least costly phone plan. The County Manager's Office will communicate with all Agency and Department Heads to request they identify their staff with County issued phones who use those phones solely for forwarding the calls to their personal phones and ensure those staff members are on the least costly phone plan. This is an interim measure to avoid wasted charges until the MDM plan with guidelines for use of personal phones is developed. **Target Date: 28 February 2015**

Personal Phones, Service Reimbursed By the County

The County does not have a Countywide policy in place to address the reimbursement to employees who use their personal phones for County business. In addition, our test revealed inconsistencies between the departments/offices reimbursement methodology. The Water System, Communications Department and DOT developed their own guidelines for the reimbursement of service costs for personal phones. Water System's guidelines specify a flat rate reimbursement amount of $10 for 20 minutes of business use and $.35 per minute over the 20 minutes. We did not identify any Water employees who were receiving reimbursement. The Communications Department uses a tiered flat rate approach[20] ($30, $60, $90) based on the projected use of the personal phone. The Director is reimbursed at $90 a month and decides at what level each individual will be reimbursed. Three employees are reimbursed at $30 and two at $60.

DOT reimburses employees, upon Director's approval, for the cost of data on their individual plans up to a maximum of $45. The amount of reimbursement varies according to the individual's plan. If the invoice submitted for reimbursement does not list the data cost separately, the data cost is estimated from prior bills or other similar plans. DOT has seven employees who received reimbursement monthly. The BOC Chairman receives $40 a month reimbursement for data charges on his personal phone. The remaining offices that reimburse employees are elected officials (See Table 5 on Page 6).

The County should evaluate whether the reimbursement of employees is a viable alternative to County-owned phones. There could be cost savings realized from eliminating the cost of the phones, reducing the cost of administration (i.e. inventory, monitoring usage, adding and cancelling phones) and limiting the reimbursement amount to the prevailing cost of a County-owned phone. The County's BYOD policy (Recommendation 1, Page 9) should provide a consistent Countywide reimbursement process that will be advantageous to the County and the employee. Consideration should be given to an annual certification of the business need, frequency of monitoring, and the established reimbursement amount(s). The payment could also be included as a payroll item.

[20] The level of reimbursement is determined and reviewed on an annual basis.

Personal Phones, Service Not Reimbursed By County

There are employees in the County who use their personal phone to conduct County-related business and the County does not provide any reimbursement. For instance, the County Attorney and many of her staff use their personal phones for County-related business but do not request reimbursement.

In addition, employees who use their phone should be made aware that any County-related information stored on the phone (emails or other data) is subject to Open Records Requests or subpoena, regardless of ownership. This policy, guidance and/or clarification should be included in the new MDM policy. (See Recommendation 1 on Page 9)

Employees Purchased Smartphone Upgrades

Vendors offer an array of phones where the cost ranges from free to several hundred dollars. The County usually makes free or low-cost phones available even though these may not be the latest model or best featured. One of the offices in our review allows employees to pay the cost of upgrades from the standard phone offered by the County. We did not solicit whether this was a practice in the other offices in our review. There is no Countywide established policy or procedure to address the ownership of these devices.

The department head should approve the type of phone acquired for an employee based on business need. The new MDM policy should provide guidance on whether an employee is allowed to pay for an upgraded phone and resolve the ownership issue. (See Recommendation 1 on Page 9)

Current Processes and Procedures are Not Adequate to Manage the Accountability of Mobile/Wireless Devices

Inventory Listings Were not Maintained in Accordance with Accountable Equipment Standards and Were Generally Inaccurate or Incomplete

We reviewed the listing provided to us by each department/office with mobile/wireless devices. We determined that the methodology for maintaining inventory of mobile/wireless devices varied between department/offices. The listings generally showed the assigned call number for the device and the person or unit the device is assigned. Some were downloads of inventory reports from the vendor websites and contained more information, such as the serial number of the device, but none of the listings were maintained in accordance with the minimum standard requirements of the Accountable Equipment Policy (AEP).

The AEP requires accountable equipment lists to include the date of purchase, purchasing document information and number, object code, description of the item, unit cost, quantity, manufacturer's serial number, County tag number, if applicable, and location of item.

In order to test the accuracy and completeness of inventory listings, we judgmentally selected four County agencies (Public Safety[21], Community Development, Transportation, and Water) to include in the test. The selected agencies account for 240 (57%) of the ***active*** phones (642-201[22]=421) and 681 (85%) of the AirCards. Some of these AirCards were inventoried as Automatic Vehicle Location cards used by the Water System to track their vehicles or Machine to Machine[23] cards used by DOT-Transit to transmit data from their buses.

Phones

Three of the four inventory lists for phones matched their current billing invoices. However, the Water System had 12 phones on their invoice that were not listed in inventory. Management acknowledged the list was incomplete and subsequently updated.

AirCards

Listing of Aircards for two of the four agencies was inaccurate primarily because the listing of AirCards used in vehicles (i.e. police cars, maintenance vehicles) were incomplete or outdated. Inventory lists for Public Safety vehicles were incomplete and/or not readily available for review and Water System listings had not been updated to reflect the transition of AirCards to another vendor.

Pagers

We also reconciled the total pager count for all departments/offices identified with pagers to the current invoices and determined that the Senior Service's pager had been discontinued and the pager count for DOT and Parks, agreed with no exceptions. The Water System's inventory listing originally included seventy-four more pagers than our initial invoice count of 107 (see Table 4 on Page 6). Our subsequent analysis identified 99 pagers. Water System management acknowledged the accuracy of 99 pagers and indicated they would update their inventory listing. They were unable to explain the discrepancy, recent change in inventory count, or the disposition of previous equipment.

County offices should ensure they adhere to the AEP requirements and accurately inventory these type of accountable items, classified as 'small and attractive', with their listing of other accountable items. Inadequate inventory controls prevent the identification of lost, stolen or unused devices and affects the accounting of accountable equipment. Reference to the AEP should also be included in the MDM policy (see Recommendation 1 on Page 9).

Recommendation

The County Manager should:

Recommendation 3: Issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory.

Auditee Response: **Concur** with the recommendation. The County Manager will issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory. **Target Date: 28 February 2015**

---

[21] Excluding the Fire Department. Except for the chiefs, they manage their own phones.

[22] The Elections Office keeps 201 of their feature phones in suspense when not in use during an election.

[23].See Appendix II, Abbreviations and Glossary for explanation. http://whatis.techtarget.com/definition/machine-to-machine-M2M

Offices Followed Different Procedures For Lost, Stolen Or Damaged Phones

The CPP requires that lost, stolen or damaged devices be reported to a supervisor immediately. An employee can be held financially liable and/or receive disciplinary action for being negligent in the management of the device. The ITSS requires that stolen County-owned portable devices be reported immediately to Risk Management and the Technical Operations Division (TOD) of I.S. The loss or theft of a personal device that was synchronized with the email system must also be reported to TOD. The AEP provides specific requirements for the disposition of accountable equipment items.

Eight of the offices with mobile/wireless devices stated they follow the same procedures of notifying management and holding the employee liable for replacement costs if negligence is proven. DOT and Elections stated they also notify the vendor. No department/office indicated they would follow current best practices of remotely disabling or wiping[24] data from lost/stolen smartphones.

No department/office explained the disposition of damaged or replaced devices, but several departments/offices (i.e. Fire, Public Safety, Water) indicated they would either donate their phones to charities (i.e. Wounded Warriors) or throw them away. Only one office stated they would surplus the items as required.

The AEP requires that all disposed or surplus accountable equipment items be listed on the Cobb County Surplus Property Disposition form and include the approval of the department head prior to sending to the Purchasing Department for disposition. Computer-related items require I.S. approval before sending to surplus. The current policy also requires the erasure of County data from all computer equipment or storage devices. I.S. or an approved contractor should complete removal of restricted data.

The new MDM policy (see Recommendation 1 on Page 9) should provide enhanced procedures to include all mobile/wireless devices that are lost, stolen or damaged. Instructions should provide for the remote wiping of devices that are lost and follow proper disposition procedures for mobile/wireless devices that may contain County data.

Unnecessary Usage Costs Are Being Paid For Unused And Underutilized Aircards And Phones

Phones

We analyzed the Countywide phone usage over a three-month period (March, April and May 2014) to identify phones that had no usage. We identified 68 phones with no voice usage over the three-month period. Each department/office with no usage phones indicated that most phones were needed for backup purposes, alternate communication, or emergency use, but other phones were identified whose service could be discontinued. Based on our inquiry, five departments cancelled the service on 14 phones, saving the County $188 a month in fees. See Table 2 on Page 3 for additional details on monthly costs.

[24] Remote wipe is a security feature that allows a network administrator or device owner to send a command to a computing device and delete data or lock the phone. How to Remotely Disable Your Lost or Stolen Phone | PCMag.com

Table of Phones with No Usage

Department/Office	Number of Phones	Deactivated	Still Active
Public Safety (Police, Animal Control, DPS Admin)	32	5	27
Property Mgt	9	0	9
Fire	3	2	1
Elections	3	0	3
I.S.	5	3	2
Water	6	1	5
DOT	2	0	2
E911	6	3	3
Parks	2	0	2
Total	**68**	14	54

Table 6 - Source: Analysis of vendor usage reports and invoices. Departmental responses to phone inactivity.

AirCards

We performed the same three-month analysis on the AirCard usage. Of the 805 AirCards in service in the County, 10% (84) had not been utilized for the three-month period. Some of the devices had not been in use for several months because the department/office did not know they existed or were still active. Other departments/offices had not monitored their usage. Departments/Offices decided to suspend service on 28 cards, saving the County $1,064[25] a month in fees. See Table 3 on Page 5 for additional details on monthly costs.

Table of Air Cards with No Usage

Department/Office	Number of Cards	Deactivated	Still Active
Police	19	10	9
Emergency Management Agency	1	1	0
Fire	4	0	4
Community Development	6	0	6
I.S.	4	4	0
Water	12	11	1
DOT/Transit	33	0	33
E911	3	0	3
Fleet	2	2	0
Total	**84**	28	56

Table 7-Source:Analysis of vendor usage reports and invoices. Departmental responses to AirCard inactivity.

[25] Twenty-eight (28) AirCards at $38.01 per card rate.

Pagers

We did not perform a utilization test on the pagers, but the departments/offices with pagers informed us that the pagers are still useful for employees on 24-hour call, employees who interact with the public and do not want to give out their personal cell number, and/or employees who do not have cell phones. In addition, DOT uses a pager circuit to send instructions to their school flasher system.[26]

The continual need for phones and other mobile/wireless devices should be periodically analyzed and a determination made on whether to continue or change the service. This process is good to identify unused devices that could be suspended in lieu of using other methods of communication (i.e. landline). Had the offices with the no usage devices performed this check, the savings identified on the previous page could have been realized sooner.

Personal Use Of Phones

The CPP provides "*The personal use of a County cellular phone*[27] *is prohibited…*" The policy provides for minimal use in an emergency or business related circumstance (i.e. unexpected overtime).

To test for personal use of phones, we analyzed vendor records to identify users with voice and text overage charges, high volume users (over 500 voice minutes per month), and invoices with miscellaneous charges. Although our review did identify indications of personal use of phones, there was no additional cost to the County for use of voice minutes. There were some users that had data/text overage charges.

Voice/Data/Text Overages

We utilized a report to analyze the AT&T phone usage for a three-month period (March, April May 2014). We reviewed the report and identified 18 users with voice overage charges. Although the report listed overage charges, review of the related invoices showed that the overages are credited against the available pool minutes. Although the individual plan minutes may have been exceeded, the total minutes of all plans in the pool were not.

We reviewed the data/text usage for all the phones for the same three-month period (March, April, May 2014). We identified 32 users who had 'per pay use' overage charges[28] for text messaging, averaging a total of $103 a month in overcharges for the three-month period. The top six users average monthly charges ranged from $4.73 to $32.80. The remaining 26 users averaged under $3 a month in overage charges. For the two users with the highest charges, there were some indications that the texting may have been personal (i.e. non-Georgia area codes and after hours patterns of texting). We did not conduct additional testing to confirm the personal usage, but the CPP policy regarding personal usage needs to be evaluated for current applicability.

---

[26] Signs that flash in school zones to notify drivers of slower speed requirement.

[27] The CPP provides that eligible employees should be assigned to an equipment account at a minimum level that fulfils the business need. The account should provide a combination of services including number minutes and coverage.

[28] Some users have 'pay per use' (usually $.20) provisions in their plans; therefore, these are not overage charges but 'pay per use' charges.

High Volume Users

We identified 36 cell phone users who averaged 500 or more minutes over the stated three-month period (March, April, May 2014). Departments/Offices with high voice minute users determined the high usage was justified based on the employee position and their respective duties. We did not conduct further analysis because there was no monetary consequence since the minutes were included in the users' account pool minutes. However, the usage of high volume users should be checked periodically to ensure that high volume is business-related.

Miscellaneous Charges

We looked for miscellaneous charges added to phone bills that may indicate inappropriate access to services not business-related or add-on fees by third-party vendors. We reviewed usage reports and identified two instances of miscellaneous charges related to international phone service. These charges were added to the service plan of one employee at their request when they were out of the country. The plan administrator was notified in advance and the service added appropriately.

Our review indicated the policy against personal phone use was not always adhered to and managers should reemphasize to their employees the prohibition against personal use of phones. Any personal use should be kept to a minimum to ensure that plan allowances for voice minutes, texting and data are not exceeded. As noted above, texting can cost the County additional money, especially if the phone plan has a 'pay for use' texting provision. Although the indications of personal voice minutes did not result in higher charges for voice service, it could prevent the County from saving on the cost of voice service by lowering the plan pool minutes available.

The new MDM policy statement (see Recommendation 1 on Page 9) should include provisions for periodic analysis of device usage to identify those that are not fully utilized for business purposes. The policy should also address current billing emphasis (i.e. unlimited voice and text) in context with the personal use provisions and the administrative costs associated with monitoring and enforcement of this provision. All services currently available (i.e. data, texting, video) should be addressed specifically.

Current Processes and Procedures are Not Adequate to Manage the Security of Mobile/Wireless Devices

The County does not have adequate security controls to mitigate inherent risks in the use of mobile/wireless devices. Unmanaged and untrustworthy County and personal mobile/wireless devices may be connected to the County's network. Records were not available to determine the definitive number of County-owned or personal devices connected to the network. However, a review of 90 forms used to request approval for access to the network showed that 70 (78%) were requests from employees with personal devices. In addition, 122 County-owned smartphones have the capability to access the network (See Table 2 on Page 3).

Direct access to employee mail, contacts and calendar information is the most frequent use of these devices, but they pose a threat to the network because they have not been evaluated to determine if they are properly secured and configured to minimize risk to the integrity of the network environment.

Current mail client software has the capability to require the users to accept a stipulated security configuration before access to the mail client is granted, but I.S. has not activated this feature.

In addition, I.S. cannot currently prevent the unauthorized connection of mobile/wireless devices to the mail server. The ITSS prohibits the installation of any non-approved hardware onto the County network. If the mobile device user acquires the necessary setup information, they can connect their mobile device to the County mail service in the same manner as you connect to other mail services like Yahoo or Gmail. This gap in security allows any employee with a network login and password to access their mail via their mobile device without authorization from anyone. I.S. currently has no way of identifying these unauthorized users. Although the current version of the mail client software requires Android[29] users to agree to certain security provisions prior to connection (Apple™ devices accept the provisions automatically); none of these security provisions have been activated.

Virtual Private Network (VPN)[30]

In addition, several of the mobile devices access the network via a VPN connection that allows the user to access their network workspace and potentially sensitive data. The ITSS requires approval from the user's manager/supervisor, department head and the I.S. Director to grant VPN access to the network. Generally, VPN connections are granted by submitting an email to the I.S. Department. I.S. can generate a report that shows who has used VPN to access the network over the past 30 days, but there is no documentation maintained showing managerial approval for the VPN connections and no listing of all authorized VPN users.

Use of Personal Phones

Several employees are using their personal phones for County business. They fall in the category of untrustworthy/unmanaged phones and present additional security problems. Since the user owns the phone, these phones are more likely used for personal reasons increasing the likelihood that malware and untrusted applications are present. The condition on how personal mobile/devices are used in the workplace should be addressed in the BYOD portion of the MDM as recommended on page 9, Recommendation 1. As stated previously (page 8), the ITSS needs updating on the type of personal devices approved for access to the network.

Android Devices

Using vendor device inventory reports, we were able to determine the operating system for 94 (63 AT&T and 31 Property Management) smartphones and determined that 15 (16%) are Android devices. According to security studies, Android devices are more susceptible to malware[31] infection and 97% of all mobile malware affects devices with an Android operating system.

---

[29] Android is a type of mobile operating system.

[30] A **Virtual Private Network** (**VPN**) extends a private network across a public network, such as the Internet. See Appendix II for a more detailed explanation.

[31] **Malware** is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

However, a March 24, 2014 Forbes[32] article indicates that these figures may be misleading and Android devices can be used safely if you limit the source of the apps to Google's[33] (Android developer) app store or take additional security precautions[34].

I.S. has recognized the need for an assessment of the security risks of mobile/wireless devices and the development of a device management strategy, but has not taken the actions necessary to put the controls needed in place. They are interviewing potential vendors to assess the risk and recommend solutions. They are also considering the use of current mail client software to apply security configuration and provisions to mobile devices accessing the County's mail server.

Recommendation

The Information Services Director should implement:

Recommendation 4:

A **short-term solution** including, but not be limited to the following:

1. Develop an updated request form (preferably electronically) to grant employee access to the mail server or establish a VPN connection for each mobile device. The business need must be stipulated and the form approved by Department Director/Elected Official and Information Services Director.

   Auditee Response: **Concur** with the recommendation of an updated request form with the following modifications. Information Services currently has a form for requesting access to email and two forms for requesting VPN access (County employee and non-County contractor) in electronic formats but these forms are not linked to a database for information storage purposes. Information Services proposes modifying the forms to reflect the recommendations of identifying the business need and management approval and also creating a database in which to store all pertinent information to be available for reporting purposes. Department Director/Elected Official approval is authority for connection. IS Director will review and send the list to Department Directors/Elected Officials annually for validation. **Target Date: 15 April 2015**

2. Require employees with a business need to access the County's network through their mobile/wireless device to submit a new approved request form (preferably electronically).

   Auditee Response: **Concur** with the recommendation of requiring employees with a need to access the County's network through their mobile/wireless devices who have forms on file to resubmit using the new form. **Target Date: 15 May 2015**

[32] http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/

[33] Google is a multinational corporation specializing in Internet-related services and products.

[34] Examples: Use mobile antivirus software, set up a call or SMS barring service to block the device from sending unwanted calls or messages, set device settings to allow only downloads from Google Play Store, use web browsing protection.

3. Block access of unauthorized users. Use 'live auditing' to discover all the devices that are currently synchronizing with the Exchange server. Set up live auditing by setting the default organizational access setting to 'quarantine'. Create a list of 'allowed' users, a list of quarantined devices will be generated. Use that list to create your 'allow and block' lists. All users will be prevented from synchronizing with the Exchange server until the 'allow' and 'block' lists have been created. Add new users to the 'allow' list, as needed.

   Auditee Response: **Concur with the concept** of blocking unauthorized users, but cannot validate at this time that the methodology described above is feasible. This has the potential to shut down valid users in Agencies who use mobile devices, some of which may not have been ordered through IS. This recommendation will take investigation by IS to capture an initial list of all users on the Exchange server, then determine which devices are County owned, which devices are mobile devices, and then work with Department Directors to validate an authorized users list. IS will investigate capabilities of the environment and provide a proposed alternative methodology for identifying and blocking unauthorized users. **Target Date: 15 March 2015**

4. Maintain authorization list and electronic copies of approved request forms.

   Auditee Response: **Concur** with maintaining an authorization list and copies of approval signatures **with the following modifications**. The actual forms will not be copied. The contents of the form and copies of the digital signatures will be copied into a database. Information Services proposes the development and maintenance of a database of authorized employees including digital approvals and signatures with appropriate reporting capabilities. **Target Date: 15 May 2015**

5. Using current mail client software[35], develop and implement basic security configuration for all County-owned and personally owned devices.

   Auditee Response: **Concur** with the recommendation to develop and implement basic security configurations using the capabilities of current email system. These configurations would need to be in alignment with any requirements which will be included in the new Mobile Device Management/Security policy. **Target Date: 30 November 2015**

A **long-term solution** including, but not be limited to the following:

Pursue the acquisition of a qualified security expert or initiate an internal effort to develop a mobile device security strategy. As suggested by a National Institute of Standards and Technology (NIST) report[36], use a project management methodology or life cycle model to ensure that an enforceable mobile device security policy is developed and the proper Mobile Device Management solution is procured to provide for ongoing management and security of County and personally-owned mobile devices and the resources they access.

---

[35] The 2010 version of Exchange gives I.S. the ability to limit the type of phones that can access the mail server and the capability to exercise control over the phone including, disabling the camera, requiring encrypted data, requiring passwords, limiting apps etc. (See Active Sync)

[36] National Institute of Standards and Technology (NIST) Report, Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124, Revision 1, June 2013

Auditee Response: **Concur** with the recommendation of the acquisition of a qualified security expert to develop a mobile device security strategy and utilize a project management methodology to ensure the successful development of the policy. Information Services has been in contact with providers of digital/cyber security services, including mobile device management, for the purpose of providing a gap analysis of the County's overall digital security posture based on the IS preferred SANS 20 Critical Security Controls – Version 5 (Sysadmin, Audit, Networking, Security – ESCAL Institute of Advanced Technology). Funding is available in the IS budget to conduct a gap analysis and develop a security plan roadmap. Information Services has been in contact with the Department of Homeland Security and is in the process of requesting a Cyber Hygiene Audit offered by their Cyber Security Division. Information Services has investigated mobile device management technologies and has funding available to implement a plan for up to 1,000 devices once a technology has been selected. **Target Date: 30 November 2015**

Administration of Mobile/Wireless Devices Needs to be Centralized

Currently, the County's management and monitoring of County-owned devices is decentralized with every department/agency or elected official responsible for ensuring the County's cellular phone and related policies are followed.

There is no one entity that keeps up with the current trends in the mobile/wireless environment and the most economical way of providing services at the best price. The I.S. Administrative Division Manager coordinates the acquisition and monitoring of phone usage for several departments/offices as a courtesy, but she is not the official telecommunications manager for the County.

Best Practices

Best practices and cyber security experts recommend a centralized approach to mobile/wireless device management. They suggest the use of a software solution that provides for centralized management of mobile devices including inventory management, policy enforcement, security configuration to protect data, heighten authentication controls, and remote access to devices to monitor security configuration and adherence to security policies. The solution could also provide, on personally-owned devices, segregation of business data and private data giving the organization control only over data necessary to ensure adherence to security policies while not infringing on the privacy of the device owner.

The enterprise-wide solution can be accomplished internally by assigning mobile/wireless device management to a specific department or acquiring an outside contractor to perform the tasks required. If done internally, there are software solutions designed to assist with mobile device management.

Mobile Device Management Software

Part of the County's overall strategy should include the evaluation of mobile device management suites (software) that provides for enterprise-wide management of mobile devices. These packages can provide the County with the capability to secure, configure and manage mobile devices, both County and personally owned.

Mobile devices can be enrolled, assigned a profile based on user role and device type, and secured against use of malicious code and insecure apps.[37] In addition, the loss of device information can be mitigated by remotely deleting enterprise data that may be on the device. Some applications provide expense management features to help ensure optimal pricing for use of mobile devices. In addition, a central administrator can run reports to monitor use and accountability of devices.[38]

Without an enterprise-wide solution to device management, the County cannot be assured:

- The risks of mobile devices accessing the network are minimized.
- The cost of mobile/wireless devices is minimized.
- The reimbursement practice, if approved Countywide, is effective and consistently applied.

Recommendations

The County Manager should designate a committee to:

***Recommendation 5*:** Designate a specific department/individual/function with Countywide oversight responsibilities for monitoring mobile/wireless device usage and security.

Auditee Response: **Concur with the following as modifications** to the recommendation. The County Manager will designate the Support Services Agency Director with oversight responsibility for mobile/wireless device usage and security. The Support Services Agency Director will coordinate with other Agency Heads to develop and implement an enterprise wide policy for Mobile Device Management. This may include centralized responsibility to procure, negotiate, and contract for Countywide phone and data usage rates. **Action Complete: Support Services Agency Director has been assigned this responsibility.**

***Recommendation 6*:** Study the feasibility of implementing a mobile device management solution to manage and secure mobile devices.

Auditee Response: **Concur with the following modification to** this recommendation. Information Services has been researching various mobile device management technologies and also has some funding available to implement security in a Mobile Device Management Strategy. Support Services Agency Director will coordinate an enterprise wide strategy to be implemented with other Service Agencies**. Target Date: 30 November 2015**

[37] A self-contained program or piece of software designed to fulfill a particular purpose; an application, especially as downloaded by a user to a mobile device.

[38] Article - 10-BYOD-Mobile-Device-Management-Suites-You-Need-to-Know

Procedures for Processing Payments for the Mobile/Wireless Devices Needs to be Evaluated

During our review, we determined that departments/offices were not consistent in using the proper coding for wireless device expenditures. We identified additional expenditures by researching payments to select vendors. This miscoding caused the cumulative yearly wireless expenditures to be understated by over $200,000. The departments with wireless expenditures and the Finance Department need to collaborate to ensure coding is consistent.

We also identified an inconsistency in the way wireless invoices are processed and paid. Some are paid directly by Accounts Payable and others are reviewed and approved by the department/office before payment. The County needs a consistent and efficient process that ensures invoices are reviewed for accuracy prior to payment.

Misclassification of Mobile/Wireless Device Expenditures

During our survey phase, we downloaded the June 2013 telecommunication expenditures by searching the Advantage Financial database for telecommunication related object codes and vendor names. We compiled a listing of all expenditure object codes used and screened to identify instances where potentially incorrect object codes were used. For instance, we looked at all the cellular phone expenditures and looked for instances where an object code other than 6385 (Mobile/Wireless Telephone) was used.

We identified approximately $18,000 in monthly telecommunication costs between 15 departments that appeared to be misclassified. They included cellular phone charges, AirCards, pagers and language line (translation) services.

AirCards

We identified 14 invoices where AirCard expenditures totaling $14,879.52 were charged to 6348 (Computer Charges), 6384 (Landline), 6386 (Data Communications), 6491 (Annual Maintenance and Support Contracts) and 6532 (Rental Equipment) that should have been charged to 6385 (Wireless & Portable Telephone Service). After discussions for clarification, the Water System changed the object codes in its template to process their invoices for 13 AirCards from 6491 to 6385. No other departments/offices were included in discussions.

Cellular Phones

We identified costs on three invoices totaling $510.33 that were charged to 6348 (Computer Charges), 6326 (Professional Services), 6384 (Landline) that should have been charged to 6385 (Mobile/Wireless & Portable Telephone Service).

Pagers

The monthly invoice for pagers totaling $279.21 was charged to 6532 (Rental Equipment) rather than 6385 (Mobile/Wireless & Portable Telephone Service).

Language Line Service

There were two invoices for language line services (translation service) totaling $2,080.71 that were expensed to 6384 (Landline) and 6385 (Mobile/Wireless & Portable Telephone Service). The costs should be reviewed to determine if it is more appropriate to be charged to 6326 (Professional Services) or 6330 (Interpreter Fee).

Information Services, Accounts Payable and the appropriate departments should coordinate to determine the proper classification of these expenditures. Proper classification ensures that the expenditures will be tracked properly for budgeting, planning, and financial reporting purposes.

Recommendation

The Finance Director/Comptroller should:

***Recommendation 7*:** Have Finance Department staff analyze the object codes used to classify the identified expenditures and where applicable, recommend departments update their records to properly charge the expenditures to object code 6385 or other agreed upon object code.

Auditee Response: **Concur -** Finance Director concurs with this recommendation with a target implementation date of July 31, 2015.

Paying Mobile/Wireless Device Invoices

During our review, we determined that the invoices for mobile/wireless devices are processed for payment in three different ways. First, some invoices go directly to Accounts Payable (AP) and processed like a utility bill — AP pays them every month using an electronic financial document called a GAXRE[39] and the department never sees the invoice. Second, invoices are downloaded from the vendor's website by the department, reviewed and approved for payment. A copy is scanned and forwarded to AP for payment using a GAX[40] document. In the third method, some invoices are processed using the 'Confirmation Delivery Order' (DO) process to allocate expenditures between multiple departments or units. For example, the I.S. invoice has expenditures allocated to 11 different departments/offices. Using DOs shifts the task of allocating and coding the invoice expenditures from AP to the departments. After the DO is processed, the department inputs a receipt (RC)[41] to approve the invoice for payment.

During our review, we identified a department who was not aware they were being billed for mobile/wireless devices because their invoice was paid using the GAXRE process and they were not seeing and approving the monthly billing. As with other expenditures, each department is responsible for ensuring that invoices are accurate and appropriate for payment. A consistent method for paying mobile/wireless invoices needs to be developed which includes a departmental review.

Recommendation

The Finance Director/Comptroller should:

***Recommendation 8*:** Collaborate with the respective departments, Purchasing Department personnel, and decide on the most efficient and effective way to pay the mobile/wireless invoices and disseminate this information to all departments, accordingly.

Auditee Response: **Concur -** Finance Director concurs with this recommendation with a target implementation date of July 31, 2015.

---

[39] An electronic document used to process and pay recurring general accounting expenses, usually monthly utility payments.
[40] An electronic document used to process payment of general accounting expenses.
[41] RC-(Receiver) – a document that is entered by departments to verify that they have received specific commodities.

Appendix I

Detailed Objectives, Scope, and Methodology

We conducted this review as part of our annual audit plan. The audit period for our initial analysis of mobile/wireless expenditures was June 2013. Where necessary, some current year invoices (see report for details) were used to update inventory and usage data.

Our overall objective was to determine if the County had the processes and procedures in place to manage the acquisition, accountability, and security of mobile/wireless devices (i.e. cellular and Smartphones, AirCards, wireless-enabled tablets).

In order to accomplish this overall objective, we performed the following sub-objectives:

I. Determined if the County had the processes and procedures in place to manage the acquisition of mobile/wireless devices.

A. Analyzed the current process for acquiring mobile/wireless services.

1. Obtained additional clarification regarding the procedures for acquiring wireless services with personnel in Information Services.

2. Obtained Department Directors' understanding of the wireless service acquisition process (via questionnaire).

B. Determined if County was utilizing the best plans for its mobile/wireless devices.

1. Analyzed the cost effectiveness of the County's current phone plans.

2. Determined if AirCards were acquired from approved vendors at the best price.

3. Determined if pagers could be obtained at a better price.

4. Coordinated with Legal department on the impact of personal use and exposure to Open Records requests.

II. Determined if the County had the processes and procedures in place to manage the accountability of mobile/wireless devices.

A. Conducted reconciliation of all mobile/wireless devices to determine if they were accounted for and in use.

1. Contacted each department, obtained inventory records for their phones and other mobile/wireless devices (pagers, AirCards), and determined if they accurately accounted for all devices.

B. Determined if devices were being fully utilized.

1. Contacted the vendors and obtained usage reports for the phones and AirCards.

2. Assessed the current need and utilization of pagers.

3. Identified suspected personal use of phones.

III. Determined if the County had the processes and procedures in place to manage the security of mobile/wireless devices.

A. Determined if mobile/wireless devices allowed to access the network were properly secured:

1. Identified all mobile/wireless devices with the capability to access the network.

2. Contacted the user/Information Services to determine the level of access to the network.

3. Determined if software had been installed to delete sensitive data from lost, stolen, damaged, or replaced devices.

4. Determined whether security concerns over the use of Android devices had been considered.

5. Determined if all employees had been informed of security procedures and expectations as they pertain to the use of mobile/wireless devices connected to the network.

Appendix II

Abbreviations and Glossary

AirCard®	AirCard® is a registered trademark name for a broadband wireless device that connects via a cellular network to the internet. We used this generic name to represent wireless cards used as Automatic Vehicle Locator (AVL) cards, wireless-enabled tablets, wireless modems, MiFis and wireless cards used in laptops.
BOC	Board of Commissioners
BYOD	Bring Your Own Device
CPP	Cellular Phone Policy
CGI Advantage	County's Financial System
Consumerization of I.T.	Consumerization of IT ("consumerization") is a phrase used to describe the cycle of information technology (IT) emerging in the consumer market, then spreading to business and government organizations, largely because employees are using the popular "consumer market" technologies and devices at home and then introducing them in the workplace. It is driven by employees who buy their own devices, use their own personal online service accounts, install their own applications and then connect to the corporate network with the device, often without the organization's knowledge or approval. Consumerization of IT - A Webopedia Small Business IT Definition
DA	District Attorney
DOT	Department of Transportation
Machine to Machine (M2M)	Machine to machine (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans
MDM	Mobile Device Management

Microsoft Exchange	Exchange's primary role is as an electronic mail message store but it can also store calendars, task lists, contact details, and other data. The 2010 version of Exchange will give I.S. the ability to limit the type of phones that can access the mail server and give them the capability to exercise control over the phone including disabling the camera, requiring encrypted data, requiring passwords, limiting apps, etc.
MiFi	MiFi is a brand name used to describe a wireless router that acts as mobile Wi-Fi hotspot where several devices can connect wirelessly to access the internet.
Mobile/Wireless Device	We are not referring to only regular cell phones, whose capability is primarily the placing and receiving of calls. We are referring to smartphones, tablets, wireless-enabled devices that can connect to the County network to retrieve mail, contact and calendar information as well as access data on the network.
PDA	Personal digital assistants (PDAs) are small, hand-held computers. They are used frequently as personal information managers (PIMs) to record telephone numbers, addresses, appointments, and to-do lists. PDAs can synchronize with microcomputers to transfer e-mail, text documents, spreadsheets, files, or databases
Smartphone	A mobile phone with more advanced computing capability and connectivity than basic feature phones including a media player, a digital camera, GPS navigation unit, touch screen computer, including web browsing, Wi-Fi, and 3rd-party apps.
Unmanaged and untrustworthy mobile devices	Organizations should assume that all mobile devices are untrusted unless the organization has properly secured them and monitors their security continuously while in use with enterprise applications or data. *Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST Special Publication 800-124, Revision.*

Virtual Private Network (VPN)	A VPN extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Appendix III

Major Contributors to the Report

Latona Thomas, CPA, Internal Audit Director
Barry G. Huff, Auditor-in-Charge

Appendix IV

Final Report Distribution List

Willie Hopkins, Support Services Agency Director
Sharon Stanley, Information Services Director
Ed Biggs, Information Services Division Manager
Kimberly Lemley, Information Services Division Manager
Judy Sheppard, Information Services, Administrative Division Manager
Jim Pehrson, CPA, Finance Director/Comptroller
Joe Tommie, Purchasing Director

Appendix V

Outcome Measure(s)

This appendix presents detailed information on the measurable impact that our recommended corrective action(s) will have on County governance. These benefits will be incorporated into our annual report to the Board of Commissioners, Audit Committee, and County Manager.

Type and Value of Outcome Measure:

- Decreased Expenditures – Actual: $1,335 ($111.23 x 12) annual savings in reduced wireless phone costs. (See page 12).
- Decreased Expenditures – Actual: $2,256 ($188 x 12) annual savings in wireless phone costs. (See page 16).
- Decreased Expenditures – Actual: $12,768 ($1,064 x 12) in annual savings in AirCard costs. (See page 17).

Methodology Used to Measure the Reported Benefit:

The monthly cost savings times 12 months provided the projected annual actual cost savings of phones and AirCards service that was discontinued or modified from the current billings.

Appendix VI

Auditees' Combined Response

COBB COUNTY MANAGER'S OFFICE

David Hankerson
County Manager

100 Cherokee Street, Suite 300
Marietta, Georgia 30090-7000
(770) 528-2600 • fax: (770) 528-2606
dhankerson@cobbcounty.org

MEMORANDUM

DATE: January 9, 2015

TO: Latona Thomas, CPA, Director of Internal Audit

FROM: David Hankerson, County Manager
Willie A. Hopkins, Jr., Director of Support Services Agency
Sharon Stanley, Director of Information Services Department

SUBJECT: Response to the Internal Audit Department's Draft Report on Cobb County's Mobile/Wireless Telecommunication Costs

This memo is in response to the subject report dated December 17, 2014. There were eight recommendations in the report. Responses to the recommendations are given below:

Recommendation 1: The Information Services Director should create a new Mobile Device Management/Security policy that addresses the acquisition, accountability, and security of mobile devices including those that are personally owned. Consult the suggested recommendation of the National Institute of Standards and Technology or other subject matter experts in the development of the statement.

Items that should be included in the new MDM policy statement are described under the four sections that follow which address controls over acquisition, accountability and security as well as other issues concerning proper classification of mobile/wireless expenditures and procedures for paying mobile/wireless invoices.

Response: Concur with the recommendation to develop a county Mobile Device Management/Security policy that address the acquisition, accountability, and security of mobile devices including those personally owned and used by County staff in conducting County business. The IS Director will create a MDM policy that includes guidelines for employee owned devices (BYOD) being used for Cobb County business. The IS Director will coordinate with other agencies/departments currently managing their own devices to develop a standard enterprise policy (see Recommendation 6).

Recommendation 2: Department Managers should identify all users who only use their county phone numbers to transfer calls to their personal phones and ensure they are assigned the least costly phone plan.

Response: Concur with the recommendation for Department Managers to identify all users who only use their county phones to transfer calls to their personal phones and ensure they are assigned the least costly phone plan. The County Manager's Office will communicate with all Agency and Department Heads to request they identify their staff with County issued phones who use those phones solely for

forwarding the calls to their personal phones and ensure those staff members are on the least costly phone plan. This is an interim measure to avoid wasted charges until the MDM plan with guidelines for use of personal phones is developed.

Recommendation 3: The County Manager should issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory.

Response: Concur with the recommendation. The County Manager will issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory.

Recommendation 4: The Information Services Director should implement a short term solution and long term solution as follows:

Concur that Information Services Director should implement a short term policy to manage security of Mobile Devices including but not limited to items 1 through 4 below:

1) **Develop an updated request form** (preferably electronically) to grant employee access to the mail server or establish a VPN connection for each mobile device. The business need must be stipulated and the form approved by Department Director/Elected Official and the Information Services Director.

   Response: Concur with the recommendation of an updated request form with the following modifications. Information Services currently has a form for requesting access to email and two forms for requesting VPN access (County employee and non-County contractor) in electronic formats but these forms are not linked to a database for information storage purposes. Information Services proposes modifying the forms to reflect the recommendations of identifying the business need and management approval and also creating a database in which to store all pertinent information to be available for reporting purposes. Department Director/Elected Official approval is authority for connection. IS Director will review and send the list to Department Directors/Elected Officials annually for validation.

2) **Require employees with a business need** to access the access the County's network through their mobile/wireless devices to submit a new approved request form (preferably electronically).

   Response: Concur with the recommendation of requiring employees with a need to access the County's network through their mobile/wireless devices who have forms on file to resubmit using the new form.

3) **Block access of unauthorized users.** Use "live auditing" to discover all the devices that are currently synchronizing with the Exchange server. Set up live auditing by setting the default organizational access setting to 'quarantine'. Create a list of 'allowed' users, a list of quarantined devices will be generated. Use that list to create your 'allow and block' lists. All users will be prevented from synchronizing with the Exchange server until the 'allow' and 'block' lists have been created. Add new users to the 'allow' list as needed.

   Response: Concur with the concept of blocking unauthorized users, but cannot validate at this time that the methodology described above is feasible. This has the potential to shut down valid users in Agencies who use mobile devices, some of which may not have been ordered through

IS. This recommendation will take investigation by IS to capture an initial list of all users on the Exchange server, then determine which devices are County owned, which devices are personal devices, and then work with Department Directors to validate an authorized users list. IS will investigate capabilities of the environment and provide a proposed alternative methodology for identifying and blocking unauthorized users.

4) **Maintain authorization list** and electronic copies of approved request forms.

   Response: Concur with maintaining an authorization list and copies of approval signatures **with the following modifications**. The actual forms will not be copied. The contents of the form and copies of the digital signatures will be copied into a database. Information Services proposes the development and maintenance of a database of authorized employees including digital approvals and signatures with appropriate reporting capabilities.

5) **Using current mail client software**, develop and implement basic security configuration for all County-owned and personally owned devices.

   Response: Concur with the recommendation to develop and implement basic security configurations using the capabilities of current email system. These configurations would need to be in alignment with any requirements which will be included in the new Mobile Device Management/Security policy.

A **long-term solution** including, but not limited to the following:

Pursue the acquisition of a qualified security expert or initiate an internal effort to develop a mobile device security strategy. As suggested by a National Institute of Standards and Technology (NIST) report, use a project management methodology or life cycle model to ensure that an enforceable mobile device security policy is developed and the proper Mobile Device Management solution is procured to provide for ongoing management and security of County and personally-owned mobile devices and the resources they access.

Response: Concur with the recommendation of the acquisition of a qualified security expert to develop a mobile device security strategy and utilize a project management methodology to ensure the successful development of the policy. Information Services has been in contact with providers of digital/cyber security services, including mobile device management, for the purpose of providing a gap analysis of the County's overall digital security posture based on the IS preferred SANS 20 Critical Security Controls – Version 5 (Sysadmin, Audit, Networking, Security – ESCAL Institute of Advanced Technology). Funding is available in the IS budget to conduct a gap analysis and develop a security plan roadmap. Information Services has been in contact with the Department of Homeland Security and is in the process of requesting a Cyber Hygiene Audit offered by their Cyber Security Division. Information Services has investigated mobile device management technologies and has funding available to implement a plan for up to 1,000 devices once a technology has been selected.

Recommendation 5: The County Manager should designate a committee to designate a specific department/individual/function with countywide oversight responsibilities for monitoring mobile/wireless device usage and security.

Response: **Concur with the following as modifications** to the recommendation. The County Manager will designate the Support Services Agency Director with oversight responsibility for mobile/wireless device usage and security. The Support Services Agency Director will coordinate with other Agency

Heads to develop and implement an enterprise wide policy for Mobile Device Management. This may include centralized responsibility to procure, negotiate, and contract for countywide phone and data usage rates.

Recommendation 6: The County Manager should designate a committee to study the feasibility of implementing a mobile device management solution to manage and secure mobile devices.

Response: Concur with the following modification to this recommendation. Information Services has been researching various mobile device management technologies and also has some funding available to implement security in a Mobile Device Management Strategy. Support Services Agency Director will coordinate an enterprise wide strategy to be implemented with other Service Agencies.

Recommendation 7: The Finance Director/Comptroller should have Finance Department staff analyze the object codes used to classify the identified expenditures and where, applicable, recommend departments update their records to properly charge the expenditures to object code 6385 or other agreed upon object code.

Response: Finance Director **concurs** with this recommendation.

Recommendation 8: The Finance Director/Comptroller should collaborate with the respective departments, Purchasing Department personnel, and decide on the most efficient and effective way to pay the mobile/wireless invoices and disseminate this information to all departments, accordingly.

Response: Finance Director **concurs** with this recommendation.

If you need further information about any responses, please let us know.

cc: Judy Skeel, Executive Assistant/County Manager
Jim Pehrson, Finance Director/Comptroller
Joe Tommie, Purchasing Director
Ed Biggs, Division Manager, Technical Operations/GIS

Auditees' Response Addendum

COBB COUNTY
INFORMATION SERVICES DEPARTMENT

Sharon A. Stanley
Information Services Director

100 Cherokee Street, Suite 520
Marietta, GA 30090
(770) 528-8733 • fax: (770) 528-8706
Sharon.Stanley@cobbcounty.org

MEMORANDUM

DATE: January 9, 2015

TO: Latona Thomas, CPA, Director of Internal Audit

FROM: Willie A. Hopkins, Jr., Director of Support Services Agency
Sharon Stanley, Director of Information Services Department

SUBJECT: Addendum to Response to the Internal Audit Department's Draft Report on Cobb County's Mobile/Wireless Telecommunication Costs

This memo is in response to the subject report dated December 17, 2014. It adds target implementation dates for the previously provided recommendations. There were eight recommendations in the report.

Recommendation 1: The Information Services Director should create a new Mobile Device Management/Security policy that addresses the acquisition, accountability, and security of mobile devices including those that are personally owned. Consult the suggested recommendation of the National Institute of Standards and Technology or other subject matter experts in the development of the statement.

Items that should be included in the new MDM policy statement are described under the four sections that follow which address controls over acquisition, accountability and security as well as other issues concerning proper classification of mobile/wireless expenditures and procedures for paying mobile/wireless invoices.

Response: Concur with the recommendation to develop a county Mobile Device Management/Security policy that address the acquisition, accountability, and security of mobile devices including those personally owned and used by County staff in conducting County business. The IS Director will create a MDM policy that includes guidelines for employee owned devices (BYOD) being used for Cobb County business. The IS Director will coordinate with other agencies/departments currently managing their own devices to develop a standard enterprise policy (see Recommendation 6). **Target Date: 30 November 2015**

Recommendation 2: Department Managers should identify all users who only use their county phone numbers to transfer calls to their personal phones and ensure they are assigned the least costly phone plan.

Response: Concur with the recommendation for Department Managers to identify all users who only use their county phones to transfer calls to their personal phones and ensure they are assigned the least costly phone plan. The County Manager's Office will communicate with all Agency and Department

Heads to request they identify their staff with County issued phones who use those phones solely for forwarding the calls to their personal phones and ensure those staff members are on the least costly phone plan. This is an interim measure to avoid wasted charges until the MDM plan with guidelines for use of personal phones is developed. **Target Date: 28 February 2015**

Recommendation 3: The County Manager should issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory.

Response: Concur with the recommendation. The County Manager will issue a memorandum to all County departments/offices reminding them to include mobile/wireless devices in their Accountable Equipment Policy inventory. **Target Date: 28 February 2015**

Recommendation 4: The Information Services Director should implement a short term solution and long term solution as follows:

Concur that Information Services Director should implement a short term policy to manage security of Mobile Devices including but not limited to items 1 through 4 below:

1) **Develop an updated request form** (preferably electronically) to grant employee access to the mail server or establish a VPN connection for each mobile device. The business need must be stipulated and the form approved by Department Director/Elected Official and the Information Services Director.

   Response: Concur with the recommendation of an updated request form with the following modifications. Information Services currently has a form for requesting access to email and two forms for requesting VPN access (County employee and non-County contractor) in electronic formats but these forms are not linked to a database for information storage purposes. Information Services proposes modifying the forms to reflect the recommendations of identifying the business need and management approval and also creating a database in which to store all pertinent information to be available for reporting purposes. Department Director/Elected Official approval is authority for connection. IS Director will review and send the list to Department Directors/Elected Officials annually for validation. **Target Date: 15 April 2015**

2) **Require employees with a business need** to access the access the County's network through their mobile/wireless devices to submit a new approved request form (preferably electronically).

   Response: Concur with the recommendation of requiring employees with a need to access the County's network through their mobile/wireless devices who have forms on file to resubmit using the new form. **Target Date: 15 May 2015**

3) **Block access of unauthorized users.** Use "live auditing" to discover all the devices that are currently synchronizing with the Exchange server. Set up live auditing by setting the default organizational access setting to 'quarantine'. Create a list of 'allowed' users, a list of quarantined devices will be generated. Use that list to create your 'allow and block' lists. All users will be prevented from synchronizing with the Exchange server until the 'allow' and 'block' lists have been created. Add new users to the 'allow' list as needed.

   Response: Concur with the concept of blocking unauthorized users, but cannot validate at this time that the methodology described above is feasible. This has the potential to shut down valid

users in Agencies who use mobile devices, some of which may not have been ordered through IS. This recommendation will take investigation by IS to capture an initial list of all users on the Exchange server, then determine which devices are County owned, which devices are mobile devices, and then work with Department Directors to validate an authorized users list. IS will investigate capabilities of the environment and provide a proposed alternative methodology for identifying and blocking unauthorized users. **Target Date: 15 March 2015**

4) **Maintain authorization list** and electronic copies of approved request forms.

   Response: Concur with maintaining an authorization list and copies of approval signatures **with the following modifications**. The actual forms will not be copied. The contents of the form and copies of the digital signatures will be copied into a database. Information Services proposes the development and maintenance of a database of authorized employees including digital approvals and signatures with appropriate reporting capabilities. **Target Date: 15 May 2015**

5) **Using current mail client software**, develop and implement basic security configuration for all County-owned and personally owned devices.

   Response: Concur with the recommendation to develop and implement basic security configurations using the capabilities of current email system. These configurations would need to be in alignment with any requirements which will be included in the new Mobile Device Management/Security policy. **Target Date: 30 Nov 2015**

A **long-term solution** including, but not limited to the following:

Pursue the acquisition of a qualified security expert or initiate an internal effort to develop a mobile device security strategy. As suggested by a National Institute of Standards and Technology (NIST) report, use a project management methodology or life cycle model to ensure that an enforceable mobile device security policy is developed and the proper Mobile Device Management solution is procured to provide for ongoing management and security of County and personally-owned mobile devices and the resources they access.

Response: Concur with the recommendation of the acquisition of a qualified security expert to develop a mobile device security strategy and utilize a project management methodology to ensure the successful development of the policy. Information Services has been in contact with providers of digital/cyber security services, including mobile device management, for the purpose of providing a gap analysis of the County's overall digital security posture based on the IS preferred SANS 20 Critical Security Controls – Version 5 (Sysadmin, Audit, Networking, Security – ESCAL Institute of Advanced Technology). Funding is available in the IS budget to conduct a gap analysis and develop a security plan roadmap. Information Services has been in contact with the Department of Homeland Security and is in the process of requesting a Cyber Hygiene Audit offered by their Cyber Security Division. Information Services has investigated mobile device management technologies and has funding available to implement a plan for up to 1,000 devices once a technology has been selected. **Target Date: 30 November 2015**

Recommendation 5: The County Manager should designate a committee to designate a specific department/individual/function with countywide oversight responsibilities for monitoring mobile/wireless device usage and security.

Response: **Concur with the following as modifications** to the recommendation. The County Manager will designate the Support Services Agency Director with oversight responsibility for mobile/wireless

device usage and security. The Support Services Agency Director will coordinate with other Agency Heads to develop and implement an enterprise wide policy for Mobile Device Management. This may include centralized responsibility to procure, negotiate, and contract for countywide phone and data usage rates. **Action Complete: Support Services Agency Director has been assigned this responsibility**

Recommendation 6: The County Manager should designate a committee to study the feasibility of implementing a mobile device management solution to manage and secure mobile devices.

Response: Concur with the following modification to this recommendation. Information Services has been researching various mobile device management technologies and also has some funding available to implement security in a Mobile Device Management Strategy. Support Services Agency Director will coordinate an enterprise wide strategy to be implemented with other Service Agencies. **Target Date: 30 November 2015**

Recommendation 7: The Finance Director/Comptroller should have Finance Department staff analyze the object codes used to classify the identified expenditures and where, applicable, recommend departments update their records to properly charge the expenditures to object code 6385 or other agreed upon object code.

Response: Finance Director **concurs** with this recommendation. **Finance Director to provide target date.**

Recommendation 8: The Finance Director/Comptroller should collaborate with the respective departments, Purchasing Department personnel, and decide on the most efficient and effective way to pay the mobile/wireless invoices and disseminate this information to all departments, accordingly.

Response: Finance Director **concurs** with this recommendation. **Finance Director to provide target date.**

If you need further information about any responses, please let us know.

cc: Judy Skeel, Executive Assistant/County Manager
Jim Pehrson, Finance Director/Comptroller
Joe Tommie, Purchasing Director
Ed Biggs, Division Manager, Technical Operations/GIS