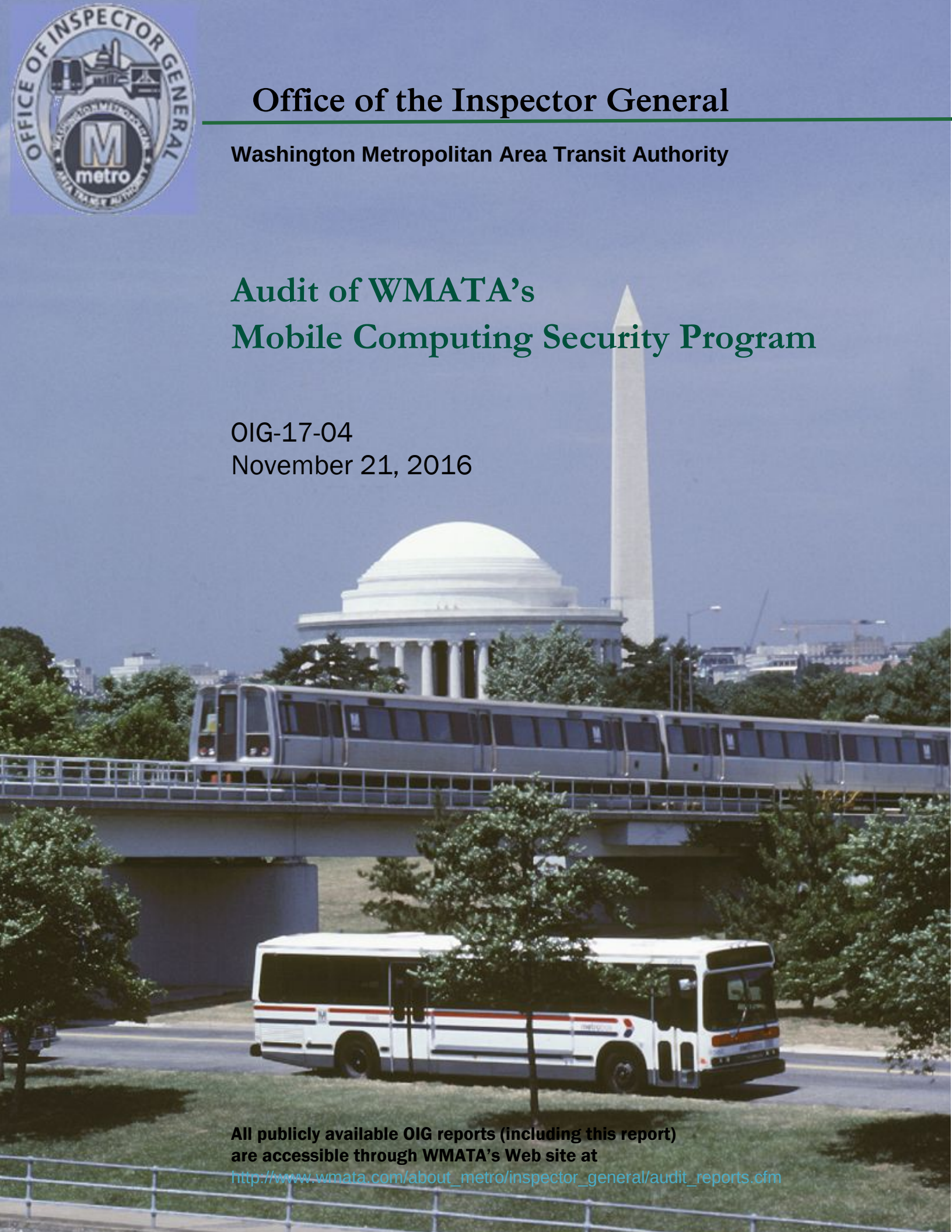
Office of the Inspector General

Washington Metropolitan Area Transit Authority

Audit of WMATA's Mobile Computing Security Program

OIG-17-04
November 21, 2016



All publicly available OIG reports (including this report) are accessible through WMATA's Web site at
http://www.wmata.com/about_metro/inspector_general/audit_reports.cfm

Washington Metropolitan Area Transit Authority
WASHINGTON, D.C. 20001

**OFFICE OF THE
INSPECTOR GENERAL**

MEMORANDUM

FROM: OIG - Helen Lew ***/s/*** DATE: November 21, 2016

TO: GMGR - Paul Wiedefeld

SUBJECT: AUDIT OF WMATA'S MOBILE COMPUTING SECURITY PROGRAM (OIG-17-04)

This Final Audit Report, entitled *Audit of WMATA's Mobile Computing Security Program,* presents the results of our audit. The audit objective was to determine whether WMATA had implemented adequate security controls over the management, administration and operation of mobile computing devices, (e.g., smartphones, notebooks, PDA's, thumb drives, and laptops). Following an Exit Conference on August 21, 2016 and the issuance of a Draft Report, WMATA staff provided written comments. WMATA staff agreed with the findings.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG follow-up.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me on (202) 962-[redacted] or Stephen D. Dingbaum, Assistant Inspector General for Audit, on (202) 962-[redacted].

cc: CFO - D. Anosike
IBOP - J. Kuo
COUN - P. Lee

Office of the Inspector General

Washington Metropolitan Area Transit Authority

Results in Brief

OIG-17-04
November 21, 2016

Audit of WMATA's Mobile Computing Security Program

Why We Did This Review

Mobile devices are key components of WMATA's information technology infrastructure. Mobile devices include smartphones, notebooks, portable digital assistants (PDA's), thumb drives, and laptops.

Mobile devices have been called the weakest link in a network. Mobile devices can contain a vast amount of sensitive and personal information and are connected to WMATA's networks. As such, mobile devices make attractive targets for criminals seeking to exploit the devices.

The audit objective was to determine whether WMATA had implemented adequate security controls over the management, administration and operation of mobile computing devices.

What We Found

WMATA does not have adequate controls over its mobile devices. Specifically:

- mobile device program guidance needs improvement,
- WMATA did not have an accurate inventory of mobile devices,
- mobile device management system security parameter settings did not fully comply with WMATA configuration standards,
- mobile phone plan selection and phone utilization were not optimized,
- controls over removable storage devices were inadequate, and
- mobile device security awareness training needs improvement.

These deficiencies increase the opportunity for theft, loss, and misuse of mobile devices and the data they contain. Further, these deficiencies may have resulted in approximately $1,054,900 in cost that could have been avoided or put to better use.

The report makes recommendations to improve the controls over WMATA's mobile device program. When implemented, these recommendations will strengthen WMATA's security over mobile devices and the information contained on the devices and network.

Management's Response

Management fully concurred with our findings and recommendations and agreed to implement controls over the custody of mobile devices and implement a comprehensive mobile device program that was responsive to our findings and recommendations.

TABLE OF CONTENTS

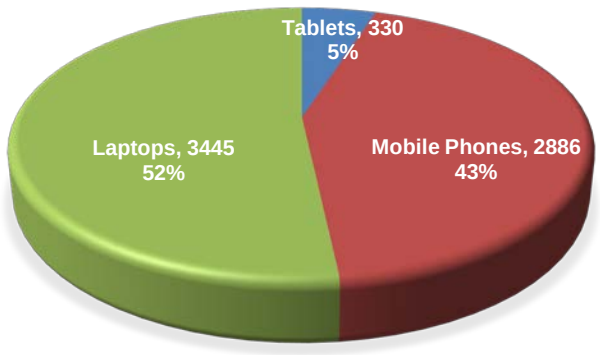
ABBREVIATIONS AND ACRONYMS

ABBREVIATION	DESCRIPTION
AMB	Asset Management Branch
BYOD	Bring Your Own Device
CFO	Chief Financial Officer
CIS	Center for Internet Security
DCI	Data Center Infrastructure
GAO	Government Accountability Office
ISACA	Information Systems Audit and Control Association
IT	Department of Information Technology
MD Strategy	WMATA Enterprise Mobile Devices Strategy
MDM	Mobile Device Management
MDM SOP	Mobile Device Management SOP
MITS	Metro Information Technology Security
NCS	Network Communication Services
NIST	National Institute of Standards and Technology
NIST SP 800-124	The National Institute of Standards and Technology Special Publication 800-124, Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
OS	Operating System
P/I	Policy Instruction
PACPPM	The Property Accounting/Control Policies and Procedures Manual
PC	Personal Computers
PDA	Personal Digital Assistant
SOIC	Standards for Internal Control in the Federal Government
PI	Policy Instruction
SOP	Standard Operating Procedures
U.S. CERT	United States Computer Emergency Readiness Team
VDCT	Voice and Data Communication Technology
WMATA	Washington Metropolitan Area Transit Authority

BACKGROUND

Mobile Device Overview - Mobile devices are key components of WMATA's Enterprise Mobile Device Strategy to provide WMATA employees more flexibility in accessing its networks. Mobile devices tend to be small, easily transported, and have connectivity to corporate networks. For purposes of this audit, mobile devices included: (1) cellphones; (2) laptops, (3) tablets, and (4) removable storage devices. According to the Department of Information Technology (IT), WMATA has 6,661 mobile devices as illustrated in Diagram 1.

Diagram 1 - Laptops, Tablets, and Mobile Phone Universe



WMATA Mobile Device Management - The following IT offices: Metro Information Technology Security, Network Communication Services, and Data Center Infrastructure are responsible for approving, procuring, managing, and controlling voice and data communications technology to include mobile devices. Additionally, these IT offices are responsible for corresponding with the service provider to place devices on the service provider's network, maintaining a mobile device inventory, providing technical support, and developing mobile device policy instructions.

The Chief Financial Officer (CFO), Office of Accounting, Asset Management Branch (AMB) is responsible for tracking WMATA assets, to include "sensitive items". *The Property Accounting/Control Policies and Procedures Manual* (PACPPM)[1] dated June 30, 1995, provides sensitive items are "… items costing $100 or more that are susceptible to theft or loss." Sensitive items should include mobile phones, tablets, laptops and removable storage devices.

Mobile Device Challenges and Risks - Mobile devices can possess computing capability and extend the workplace environment. However, mobile devices pose unique security threats because of their size, portability, network connectivity, and location services. These threats include the following: (1) loss or theft of data, (2) exposure to untrusted and unsecured networks/systems, (3) exposure to untrusted and malicious

[1] A January 2016 Asset Management Manual had been drafted, but it had not been finalized or disseminated.

applications (Apps), (4) reduced technical controls, and (5) exposure of private information. Further, when mobile devices are used, the diversity of available devices, operating systems, carrier provided services, and apps present additional security challenges.

Cybersecurity[2] **Risks** - Mobile devices and mobile applications have been called the weakest link in a network. Mobile devices can contain a vast amount of sensitive and personal information, as such, mobile devices make attractive targets for criminals seeking to exploit the devices. According to the Ponemon Institute, 6 out of 10 cybersecurity breaches were the result of a mobile device.[3] Consequently, the need for organizations to implement commensurate and continuous mitigating measures is critical to building a robust mobile device management program.

[2]According to Information Systems Audit and Control Association (ISACA) Glossary, Cybersecurity is "[t]he protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems."

[3]Ponemon Institute is considered a pre-eminent research center dedicated to privacy, data protection, and information security policy.

AUDIT OBJECTIVE AND AUDIT RESULTS

Audit Objective

The audit objective was to determine whether WMATA had implemented adequate security controls over the management, administration and operation of mobile computing devices.

Audit Results

WMATA does not have adequate controls over its mobile devices. Specifically:

- mobile device program guidance needs improvement,
- WMATA did not have an accurate inventory of mobile devices,
- mobile device management system security parameter settings did not fully comply with WMATA configuration standards,
- mobile phone plan selection and phone plan utilization were not optimized,
- controls over removable storage devices were inadequate, and
- mobile device awareness training needs improvement.

These deficiencies increase the opportunity for theft, loss, and misuse of mobile devices and the data they contain. Further, these deficiencies may have resulted in approximately $1,054,900 that could have been avoided or put to better use. For these reasons, WMATA needs to improve the controls over its mobile device program.

Findings are rated as High,[4] Medium,[5] or Low[6] risk, and require management corrective actions to strengthen internal processes and provide for more effective and efficient operations. The details of the above findings are discussed below.

[4] High - Exception is material to accomplishing organization objectives. Corrective action by appropriate Senior Management is required. Resolution would help avoid loss of material assets, reputation, critical financial information or ability to comply with critical laws, policies or procedures.

[5] Medium - Exception may be material to accomplishing organization objectives. Corrective action is required and the results are reported to management quarterly. Resolution would help avoid negative impact on the unit's assets, financial information, or ability to comply with important laws, policies, or procedures.

[6] Low - Exception has a minor impact on the accomplishment of organization objectives but may result in inefficient operations. Resolution would help improve controls and avoid inefficient operations within the unit.

FINDINGS AND RECOMMENDATIONS

FINDING 1 - MOBILE DEVICE PROGRAM GUIDANCE NEEDS IMPROVEMENT (Risk - Low)

The mobile device policy instructions and departmental standard operating procedures (SOP) did not align with WMATA's Mobile Device Strategies. This occurred because WMATA has not given sufficient attention to mobile device program policies and procedures. As a result, inconsistencies existed in the management and administration of the mobile devices program.

Policy and Procedure Requirements

Government Accountability Office (GAO), Standards for Internal Control in the Federal Government, dated September 2014, (SOIC) section OV2.03 provides "[a]n entity determines its mission, sets a strategic plan, establishes entity objectives, and formulates plans [policies and SOPs] to achieve its objectives." SOIC section OV2.19 provides "[o]perations [organizational business units] objectives relate to program operations that achieve an entity's mission. An entity's mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill those objectives. Effective operations produce the intended results from operational processes, while efficient operations do so in a manner that minimizes the waste of resources."

Diagram 2 illustrates the flow, as enumerated by GAO, from the initial development of strategic plans, through the intermediary development of corresponding policy instructions and SOPs, and to the eventual delivery of goods or services to constituents.

Diagram 2 - Strategy and Policy Instruction Alignment

T
.

Mobile Program Strategic Alignment

IT created a detailed and comprehensive mobile device strategy, entitled the *WMATA Enterprise Mobile Devices Strategy* (MD Strategy), dated July 1, 2014. WMATA's mobile device policies are found in Policy Instruction (P/I) 15.4/1; mobile device procedures are found in *Mobile Device Management* SOP (MDM SOP). However, many lapses and gaps exist between the MD Strategy, P/I 15.4.1, and the MDM SOP as outlined in Table 1.

Table 1 - Gap Analysis

NO.	MOBILE DEVICE POLICY AREA	WMATA MOBILE DEVICE STRATEGY[7]	WMATA POLICY INSTRUCTION (P/I 15.4/1)	MDM SOP
1.	Establishment of User Groups	X		
2.	Mobile Device Configuration Standards and Requirements for various groups	X		X
3.	Mobile Device Acceptable Use Policy	X		
4.	Enforcement	X		
5.	Bring Your Own Device (BYOD)	X	N/A	N/A
6.	Data Loss	X		
7.	Device damage, Loss, Theft or Compromise	X		X
8.	Commingling WMATA and Personal Data	X		
9.	Malware and Virus Protection	X		
10.	Bandwidth and Productivity Constraints	X		
11.	Independent Device Ecosystems	X		
12.	Security Requirements	X		
13.	Access Registration Requirements	X		
14.	WMATA's responsibility for Managing Mobile Devices	X		
15.	Wi-Fi Access to WMATA's Network	X		
16.	WMATA's Right to Monitor and Protect	X		
17.	Approved Technology	X		
18.	MDM Registration	X		X
19.	Provisioning	X	X	X
20.	Requisitioning and Distribution of Mobile Devices			
21.	Departmental Roles and Responsibilities			X
22.	Maintenance			X
23.	Mobile Application Review Board			X
24.	Mobile Device Inventory Control			X
25.	Risk Management, assessment/mitigation			

The MD Strategy includes 19 policy areas, P/I 15.4/1 only covers one provision, and the MDM SOP includes eight policy/procedure areas.

Section 5.08 is the only provision in the P/Is that covered mobile devices. P/I 15.4/1 sections 5.08 (a) and (b) provide the following:

5.08 Personal Computers, Smartphones, and Tablets:

(a) All business units must register all personal computers (PCs), smartphones and tablets with IT.

[7] An X in Table 1 indicates the documentation contained or covered the topic or issue listed in the Mobile Device Policy Area.

(b) Each PC, smartphone, and tablet must be imaged with the standard and approved Metro operating system (OS) image.

Cause and Impact of Inadequate Policies

This internal control deficiency occurred because IT management had not given sufficient attention to the mobile device program and policies. Many of the policies and processes surrounding mobile devices were intuitive and had not been formally communicated to WMATA departments and staff. Consequently, inconsistencies existed in the management and administration of the mobile devices program. These deficiencies have operational and monetary impacts as outlined in the findings detailed in this report.

Recommendation:

We recommend the GM/CEO:

1. Develop and implement comprehensive mobile device policies and corresponding SOPs that tie to WMATA's Mobile Device Strategy and best practices. (Action: Chief of Internal Business Operations) (Risk - Low)

FINDING 2 - WMATA DID NOT HAVE AN ACCURATE INVENTORY OF MOBILE DEVICES (Risk - High)

An accurate inventory of mobile devices is required for information security and to prevent fraud, waste, and abuse of WMATA property. However, neither AMB nor IT had an accurate inventory of mobile devices. This deficiency occurred because WMATA lacked a single point of accountability for mobile devices, had not updated the definition of sensitive items, misinterpreted the policy, and lacked standardized inventory item categories for mobile devices. As a result, WMATA could not account for its mobile devices. In fact, the 2015 Biennial Inventory provides that laptops valued at more than $950,000 could not be accounted for.

Requirement for Accurate Inventories

The *Mobile Security Companion to the CIS Critical Security Controls (Version 6)* provides "[o]ne must have knowledge of all devices used to access data and resources in the organization. Mobile devices aren't perpetually attached to the corporate network like other IT systems, so new methods need to be used to maintain the inventory."

Additionally, The National Institute of Standards and Technology Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (NIST SP 800-124) dated June 2013, section 4.4 provides "Operational processes that are particularly helpful for maintaining mobile device security, and thus should be performed regularly, include ... Keeping an active inventory of each mobile device, its user(s), and its applications."

WMATA Inventories of Mobile Devices

The AMB and IT maintain separate inventories of mobile devices. An AMB official stated AMB does not maintain an inventory of mobile phones, tablets, or laptops that are not capitalized.[8] An AMB official could only provide a list of laptops that had been purchased with capital funds. IT provided an inventory of the laptops, as well as a separate inventory of tablets and phones.

Reliability of Laptop/Mobile Device Inventories

The laptop, mobile phone and tablet inventories could not be relied upon.

Laptop Inventories - The AMB reported the inventory contained 1,115 laptops. However, the AMB inventory could not be relied upon because of duplicates and large differences with the IT inventory. Additionally, AMB had not standardized the inventory categories making it difficult to identify mobile devices and other IT equipment (Refer to Table 2).

[8] Capitalized Item – Item treated as nonexpendable that is capitalized by an appropriate entity of the gross actual or estimated cost of the item to a property account, per the PACPPM.

Table 2 - Laptop Inventory Evaluation

Category	AMB Inventory	IT Inventory	Variance
Total Number of Laptops	1,115	3,487	
Less Duplicates	(125)	0	
Less Non-Laptops	(222)	(42)	
Total Number of Laptops (Adjusted)	768	3,445	2,677

The IT reported 3,487 laptops. However, this inventory was inaccurate as it contained 42 tablets. In addition, an IT official stated the CompuTrace System[9] shows about 4,400 laptops as of May 2016. Therefore, no reliance can be placed on the IT laptop inventory.

Mobile Phones/Tablet Inventory - The AMB manager stated AMB does not track mobile phones and tablets. The IT phone inventory was reported at 2,952 which included 66 duplicate device identification numbers.

Causes for Lack of Accurate Inventory of Mobile Devices

The following internal control weaknesses contributed to the conditions cited in this finding.

- *Lack of single point of accountability* - AMB management believed IT was in a better position to track mobile devices. However, AMB did not have a formal agreement with IT that relieved AMB of its responsibility to track sensitive items.

- *Policy interpretation* - In accordance with the PACPPM, AMB was responsible for tracking "sensitive items" greater than $100, but misinterpreted the policy and only tracked capitalized laptops.

- *Out of date definition of sensitive items* - The definition of a "sensitive item" had not been updated in PACPPM, issued in June 1995. As such, the AMB policy did not have current examples of sensitive items which would include mobile phones, tablets, and laptops.

- *Lack of standardized categories* - AMB and IT had not standardized the categories for tracking various types of mobile devices. Offices used numerous and different categories to classify personal computers (PC) and laptops. As such, it is not always possible to distinguish whether the listed equipment was a laptop, PC, or other electronic equipment.

[9] The CompuTrace System is a management tool under development that tracks laptops by employee and location upon activation of the computer BIOS.

Why Is This Important

Without an accurate inventory of mobile devices, WMATA cannot be assured the mobile devices are in WMATA's possession, safeguarded or de-provisioned appropriately. According to results of the 2015 Biennial Inventory, WMATA could not locate 794 laptops.[10] The estimated replacement cost for laptops that could not be accounted for was $952,800.[11] The lack of adequate mobile device inventory control also could increase the opportunity for unauthorized disclosure of sensitive data and access to WMATA networks.

Recommendations:

We recommend the GM/CEO:

2. Determine whether AMB or IT will be responsible for the official inventory of "sensitive items" such as: laptops, tablets and mobile phones. (Action: Chief Financial Officer) (Risk - Medium)

3. Develop and implement policy instructions, SOPs, and/or agreements to ensure "sensitive items" greater than $100, are automatically tracked and inventoried as required by the PACPPM. (Action: Chief Financial Officer) (Risk - High)

4. Update the PACPPM to clarify the definition of a sensitive item and provide examples of items that should be tracked. (Action: Chief Financial Officer) (Risk - Medium)

5. Develop and implement mobile device equipment classifications, for inventory purposes, to allow for the easy identification of mobile devices. (Action: Chief Financial Officer and Chief of Internal Business Operations) (Risk - Low)

[10] Acquisition dates for the missing laptops ranged from January 2, 2013 to March 18, 2015.
[11] Laptop replacement cost estimate: 794 laptops at $1,200 each, total $952,800

FINDING 3 - MOBILE DEVICE MANAGEMENT SYSTEM SECURITY PARAMETER SETTINGS DID NOT FULLY COMPLY WITH WMATA CONFIGURATION STANDARDS (Risk - Low)

[redacted]

Mobile Device Parameter Setting Requirements

The MDM SOP, section 6, provides the mobile device platform and corresponding security parameter settings for Android, iOS, and Windows mobile operating systems. Appendix 1, Table 4 shows the WMATA configuration standards for each mobile operating system.

NIST SP 800-124, section 4.3 provides "[o]n a per-OS version basis, implementers should carefully review the default values for each mobile device setting and alter the settings as necessary to support security requirements ...." IT should formally document its review of MDM system security parameter settings to provide a basis for consistent operating system provisioning.

WMATA MDM Security Parameter Compliance

[redacted]

[redacted]

[12] IBM® MaaS360® Mobile Device Management is the product WMATA uses to manage its mobile devices. MaaS360® ". . . helps simplify mobile device management by providing visibility and control of smartphones and tablets in the enterprise. The software supports devices such as iPhone, iPad, Android and Windows Phone."

[redacted]

Causes for Configuration Non-Compliance

[redacted]

Why Is This Important

Noncompliance with WMATA configuration standards increases the risk and opportunity for security breaches, data exposure, and other exposures associated with each specific parameter.

Recommendations:

We recommend the GM/CEO:

6. Conduct a risk assessment on the mobile device security parameter settings to determine the relevant risk of each security parameter and the mitigating strategy. (Action: Chief of Internal Business Operations) (Risk - Low)

7. Based on a risk assessment and best practices, develop and implement comprehensive mobile device security parameter standards for each supported mobile device operating system. (Action: Chief of Internal Business Operations) (Risk - Low)

FINDING 4 - MOBILE PHONE PLAN SELECTION AND PHONE PLAN UTILIZATION WERE NOT OPTIMIZED (Risk - Medium)

WMATA did not always take advantage of opportunities to lessen mobile phone charges associated with phone usage and de-provisioning.[13] This deficiencies occurred because of poor phone plan administration and monitoring, as well as inadequate corporate guidance. As a result, WMATA may have incurred approximately $102,100 in additional cost for mobile phone service.

Mobile Phone Utilization Requirements

P/I 15.18/1, Voice and Data Communication, dated January 14, 2016, section 4.02 provides "[t]he Department of Information Technology (IT) is responsible for approving, procuring, managing, controlling and maintaining VDCT [Voice and Data Communication Technology] ...."

In pertinent parts, P/I 15.18/1 section 4.02 provides that IT is responsible for:

(a) Establishing criteria for issuing VDCT to Metro staff
(b) Negotiating VDCT contracts and pricing plans
(e) Ensuring VDCT charges are proper and in accordance with contracts and agreements with VDCT providers
(f) Developing and maintaining standards for IT-managed VDCT

Mobile Phone Utilization and Plan Selection

Phone Plans - WMATA did not always minimize charges for voice usage with less than 52 voice minutes.[14] For voice usage less than 52 minutes, a $34.99 per month plan is available. OIG identified 260 mobile phones that used 52 voice minutes or less, but were still on a $48.07 plan.[15]

An IT manager stated employees initially were placed on the higher cost plan, in error, but should have been placed on the lower cost plan. P/I 15.18/1 does not contain provisions that require mobile phone service plan optimization analysis and reviews. Further, IT had not developed an SOP covering optimization analysis processes. As a result, WMATA incurred approximately $40,800 for phone service that could have been avoided.

No or Low Voice and Data Usage - From April 1, 2015 to March 31, 2016, 61 mobile phones either had no or low usage. Twenty nine mobile phones had no voice and no data activity[16] and 32 mobile phones had low activity over the same period.[17]

[13] De-Provisioning – The act of removing access from a person leaving the company, changing jobs, or no longer needing it.
[14] The $34.99 plan cost $0.25 a minute and the $64.99 voice plan includes the first 400 voice minutes and $0.25 a minute thereafter.
[15] The $64.99 plan was reduced by 25%, corporate discount, to $48.07.
[16] No voice or data activity means zero voice minutes, zero non-peak minutes, and zero data used.
[17] Low activity means five voice minutes or less and no data used.

This occurred because WMATA had not implemented a formal departmental mobile phone re-certification policy and corresponding processes to periodically determine whether WMATA employees had a continual need for a mobile phone. As a result, WMATA may have incurred approximately $24,100 in service plan cost for those mobile phones.

The IT manager stated, in consideration of budget constraints and cost savings requirements, IT had begun to review mobile device usage. The IT manager prepared a comprehensive plan[18] to save about $800,000 on the mobile phone program. The IT manager stated in July 2016, IT began to examine which mobile phones should be moved from the higher cost mobile phone plans to the lower cost plans. Additionally, the IT manager stated IT was also in the process of identifying mobile phones with no usage and low usage. The IT manager also stated IT planned to coordinate with the departments to determine which mobile phones service could be discontinued. The IT manager stated that the plan had been completed. However, periodic monitoring of mobile phone usage and service plans should be conducted.

De-Provisioning and Un-Enrollment Process

IT had not discontinued the service of phones issued to former employees. Specifically, at the time of this audit, 41 former employees were assigned 92 mobile phones. For example, the former [redacted], who left WMATA in August 2015, was assigned 26 mobile phones. Another example, the former [redacted], who left WMATA in March 2016, was still assigned 19 mobile phones.

According to the MDM SOP section 9 "[w]hen a WMATA employee leaves the company, [WMATA], the employee or HR returns the mobile device to NCS [Network Communication Services]." Afterwards, the IT team is responsible for wiping the mobile device and deactivating the device and service.

This occurred because the MDM SOP is departmental and does not have WMATA-wide distribution; as such, the MDM SOP may not be known to all departments or staff who manage or use mobile devices. Further, the employee exit and de-provisioning processes are not under the control of one group; therefore, lapses and gaps in the process occur and go undetected.

Consequently, WMATA may have incurred approximately $37,200 to keep mobile phones active that were assigned to former employees. These devices, potentially, could connect to WMATA's infrastructure and be used to gain unauthorized access. Further, the data that resides on the mobile devices could be subject to unauthorized disclosure and use.

[18] The OIG received the plan entitled FY16 Mobile Device Price Plans and Cost on August 22, 2016.

Why Is This Important

These deficiencies may have caused WMATA to incur approximately $102,100[19] in cost that could have been avoided and put to better use.

Recommendations:

We recommend the GM/CEO:

8. Develop and implement WMATA Policy Instructions that describe phone service and plan optimization requirements, as well as provisions for de-provisioning mobile devices. (Action: Chief of Internal Business Operations) (Risk - Medium)

9. Develop and implement departmental SOPs that includes, at a minimum, provisions for: (1) conducting routine and periodic review of mobile device plans, (2) discontinuing mobile device services because of no or low usage, and (3) conducting periodic certification of departmental mobile device needs. (Action: Chief of Internal Business Operations) (Risk - Medium)

10. Obtain and de-provision mobile phones issued to former employees as required by the MDM SOP. (Action: Chief of Internal Business Operations) (Risk - Low)

[19] The monetary impact of $102,100 includes $40,800 in plan savings; $24,100 in voice and usage savings; and $37,100 in savings for active phones of former employees.

FINDING 5 - CONTROLS OVER REMOVABLE STORAGE DEVICES WERE INADEQUATE (Risk - Medium)

WMATA had not implemented adequate administrative and operational controls over removable storage devices. This condition occurred because of insufficient management attention to addressing risks involving removable storage devices.[20] The lack of controls over removable devices increases the risk and opportunity for data loss and compromise of WMATA systems.

Removable Storage Control Requirements

WMATA developed six requirements relative to removable storage devices cited throughout several P/Is; however, only one requirement was implemented. Additionally, WMATA had also not implemented, at a minimum, six other best practices as promulgated by CIS, NIST, and U.S. CERT (Refer to Table 3).[21]

Table 3 - Status of Removable Storage Device Policies/Implementation

No.	Controls Over Removable Storage Devices (Examples)	Policy Instruction or Best Practice	Control Implemented
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[20] Refers to as electronic storage media that is portable.

[21] Center for Internet Security is " . . . a not-for-profit organization whose mission is to enhance cyber security readiness and response of public and private sector entities."

[22] United States Computer Emergency Readiness Team

Causes for Inadequate Controls

This condition was caused by insufficient management attention in addressing risks involving removable storage devices. An IT official stated a risk assessment on removable storage device vulnerabilities had not been conducted. Additionally, IT staff were not aware of the policy requirements relative to removable storage devices. In response to our inquiry to whether WMATA had developed policies and procedures over removable storage devices, IT responded "No." Subsequently, in response to further inquiry, an IT official stated "IT is in the planning stages of developing a strategy for managing removable devices."

Why Is This Important

The lack of controls over the administration and operation of removable storage devices increases WMATA's risk and likelihood of experiencing data loss, unauthorized access to critical and sensitive data, and exposure to viruses, Trojans, worms, and other computer vulnerability attacks.

Recommendations:

We recommend the GM/CEO:

11. Conduct a risk assessment on removable storage devices to determine the vulnerabilities and exposures to WMATA's network and system environments. (Action: Chief of Internal Business Operations) (Risk - Medium)

12. Centralize existing removable storage device requirements and update removable storage device policies, procedures and standards to include relevant best practices and provisions to limit or prevent risk assessment vulnerabilities. (Action: Chief of Internal Business Operations) (Risk - Medium)

13. Commensurate with revised policy instructions, develop and implement automated controls to detect the use of removable storage devices and mitigate vulnerabilities. (Action: Chief of Internal Business Operations) (Risk - Medium)

FINDING 6 - MOBILE DEVICE SECURITY AWARENESS TRAINING NEEDS IMPROVEMENT (Risk - Low)

WMATA's basic security awareness training curriculum did not adequately address mobile device issues. IT management believed the training was adequate, as such, IT had not taken actions to create a mobile device security awareness training curriculum or to enhance the current security awareness training curriculum. The lack of a robust mobile device training program increases the likelihood that employees will misuse the device or subject the device to exploits and fraudulent activity.

Mobile Device Training Requirements

The *ISACA Mobile Computing Security, Audit and Assurance Program* provides "[e]mployees and contractors utilizing enterprise equipment or receiving or transmitting enterprise sensitive information receive initial and ongoing training relevant to the technology assigned to them." Additionally, ISACA provides the training should be:

- tailored to reflect current technologies and enterprise policies
- required prior to the issuance of the device, and
- documented and monitored.

Mobile Device Training Adequacy

The OIG reviewed and completed *The Basic Security Awareness Training 2015.*[23] *The Basic Security Awareness Training 2015* is a general and basic security awareness training and is not specifically tailored for mobile devices. Numerous lapses and gaps in the topics exist in WMATA's general security awareness training, such as Mobile Device Definition, Acceptable Use, and Password Security. WMATA's current security awareness training versus industry best practices, as mentioned in publications issued by ISACA, NIST, and CIS, are shown on Diagram 3.

[23] P/I 15.14/1, section 3.03 provides that "IT Security Awareness & Training – A general training program that provides an individual with the basic knowledge to support Metro in maintaining network security. Topics include: network acceptable use, password practices, application maintenance, virus protection, anomaly reporting practices and typical threat awareness."

Diagram 3 - WMATA's Basic Security Awareness Training Comparison to Industry Standards for Mobile Devices

WMATA Basic Security Awareness Training 2015

- Secure mobile data devices, faxes, and voicemail
- Being vigilant in protecting any sensitive information you manage on mobile devices
- Properly dispose of sensitive information on removable media (e.g., USB drives, Micro SD cards, DVDs, or hard drives, etc.)
- Other Phishing Attack Vectors
- Attaching unknown USB Devices to networks

- VS -

Topics in Security Awareness Training

- Mobile Device Definition
- Acceptable Use
- BYOD Considerations
- Email Security or Anti-Phishing
- URL Training
- Data Protection and Destruction
- Mobile Application Security
- Mobile Device Security
- Password Security
- Physical Security
- Safe Social Networking
- Safer Web Browsing
- Security Beyond the Office
- Security Essentials
- Social Engineering
- Compliance Training

Cause for Inadequate Mobile Device Training

P/I 15.14/1, section 5.00 requires all WMATA staff to receive initial and on-going IT security awareness training. However, WMATA did not require WMATA employees receive mobile device security/awareness training prior to being issued a mobile device. IT responded "[t]he current Security Awareness Training covers all security topics including mobile devices." IT Management believed the general security awareness training was adequate to address mobile device awareness and security. As such, IT Management did not see the need to change the current security awareness training.

Why Is This Important

Training is a critical control needed to minimize resource misuse and promote process consistency. The lack of adequate mobile device security awareness training, increases the chances of mobile device misuse, data breaches/loss, malware and virus contamination, and fraudulent activities.

Recommendation:

We recommend the GM/CEO:

14. Based on best practices for mobile device security awareness training, enhance WMATA's current Mobile Device Security Awareness Training curriculum or develop a mobile device awareness/training curriculum specifically for WMATA employees who are issued mobile devices. (Action: Chief of Internal Business Operations) (Risk - Low)

CONSOLIDATED LIST OF RECOMMENDATIONS

1. Develop and implement comprehensive mobile device policies and corresponding SOPs that tie to WMATA's Mobile Device Strategy and best practices. (Action: Chief of Internal Business Operations) (Risk - Low)

2. Determine whether AMB or IT will be responsible for the official inventory of "sensitive items" such as: laptops, tablets and mobile phones. (Action: Chief Financial Officer) (Risk - Medium)

3. Develop and implement policy instructions, SOPs, and/or agreements to ensure "sensitive items" greater than $100, are automatically tracked and inventoried as required by the PACPPM. (Action: Chief Financial Officer) (Risk - High)

4. Update the PACPPM to clarify the definition of a sensitive item and provide examples of items that should be tracked. (Action: Chief Financial Officer) (Risk - Medium)

5. Develop and implement mobile device equipment classifications, for inventory purposes, to allow for the easy identification of mobile devices. (Action: Chief Financial Officer and Chief of Internal Business Operations) (Risk - Low)

6. Conduct a risk assessment on the mobile device security parameter settings to determine the relevant risk of each security parameter and the mitigating strategy. (Action: Chief of Internal Business Operations) (Risk - Low)

7. Based on a risk assessment and best practices, develop and implement comprehensive mobile device security parameter standards for each supported mobile device operating system. (Action: Chief of Internal Business Operations) (Risk - Low)

8. Develop and implement WMATA Policy Instructions that describe phone service and plan optimization requirements, as well as provisions for de-provisioning mobile devices. (Action: Chief of Internal Business Operations) (Risk - Low)

9. Develop and implement departmental SOPs that includes, at a minimum, provisions for: (1) conducting routine and periodic review of mobile device plans, (2) discontinuing mobile device services because of no or low usage, and (3) conducting periodic certification of departments mobile device needs. (Action: Chief of Internal Business Operations) (Risk - Medium)

10. Obtain and de-provision mobile phones issued to former employees as required by the MDM SOP. (Action: Chief of Internal Business Operations) (Risk - Medium)

11. Conduct a risk assessment on removable storage devices to determine the vulnerabilities and exposures to WMATA's network and system environments. (Action: Chief of Internal Business Operations) (Risk - Medium)

12. Centralize existing removable storage device requirements and update removable storage device policies, procedures and standards to include relevant best practices and provisions to limit or prevent risk assessment vulnerabilities. (Action: Chief of Internal Business Operations) (Risk - Medium)

13. Commensurate with revised policy instructions, develop and implement automated controls to detect the use of removable storage devices and mitigate vulnerabilities. (Action: Chief of Internal Business Operations) (Risk - Medium)

14. Based on best practices for mobile device security awareness training, enhance WMATA's current Mobile Device Security Awareness Training curriculum or develop a mobile device awareness/training curriculum specifically for WMATA employees who are issued mobile devices. (Action: Chief of Internal Business Operations) (Risk - Low)

SUMMARY OF MANAGEMENT'S COMMENTS

WMATA provided written comments to this report on November 10, 2016, (see Appendix C) and on November 15, 2016 (see Appendix D). WMATA management fully concurred with our findings and recommendations. The Chief of Internal Business Operations agreed to develop a comprehensive mobile device program that was responsive to our findings and recommendations. The CFO agreed to implement internal controls over the custody and protection of mobile devices.

Appendix A

OBJECTIVE, SCOPE AND METHODOLOGY

Objective

The audit objective was to determine whether WMATA had implemented adequate security controls over the management, administration and operation of mobile computing devices, (e.g., smartphones, notebooks, PDA's, thumb drives, and laptops). Specifically, we reviewed the existence and completeness of the following control and process areas:

- Internal, general and application controls over the mobile environment,
- Data Protection,
- Data Isolation,
- Monitoring,
- Identity and Authorization, and
- Privacy and Protection.

Scope

Our scope included a review of WMATA-owned mobile devices issued to WMATA employees. Our initial scope included bring your own device (BYOD). However, during the course of our audit, we determined WMATA did not support BYOD. Our review commenced on February 12, 2016 and fieldwork officially ended on August 2, 2016.

Further, we determined mobile devices could, for example, include: smartphones, notebooks, PDAs, thumb drives, and laptops. However, we limited our review to mobile phones, laptops, tablets, and removable storage devices. Our review of mobile devices included an assessment of the general, application, and internal controls over the mobile devices. Additionally, we reviewed mobile phone voice and data usage as well as a review of various mobile phone service plans.

Methodology

To accomplish our audit objective, we: (1) reviewed WMATA mobile device P/Is and SOPs; (2) interviewed managers and staff members from CFO, MITS, NCS, and DCI; (3) analyzed relevant documentation; (4) examined various inventories of mobile devices; (5) obtained and reviewed configuration and parameter settings for mobile devices, (6) examined security and awareness training material; (7) examined mobile phone data and plan information from Verizon for the period of April 1, 2015 to March 31, 2016, and (8) reviewed relevant manufacturer and industry best practices and standards.

To assess the reliability of data we performed the following: (1) reviewed the data to identify data anomalies, (2) reviewed information about the systems that produced the data, and (3) interviewed agency officials knowledgeable about the data. Additionally, we performed tests to determine whether the various data conformed to source documents. To a large degree, the data utilized to support the findings and conditions contained in this report was sufficiently reliable. However, as detailed in Finding 2, we could not sufficiently rely on the mobile device inventories.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards* appropriate to the scope. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

OIG held an Exit Conference on August 31, 2016, to discuss the findings from the audit with management personnel and representatives from the IT and CFO, respectively.

Appendix B

Table 4 - Mobile Device Configuration Standards and MDM System Security Parameter Settings

OPERATING SYSTEM	FIELD SETTING	PARAMETER	WMATA STANDARD	MDM SETTING[24]	COMPLIED
ANDROID O/S	[redacted]				
APPLE iOS	[redacted]				

[24] Android Devices were the Samsung Note 4, MTPD Tablets, and MRPD Note 3. IOS Devices were iPhones or iPads owned by the WMATA Board, General Manager's Office or Safety Department. Window Devices were Windows 8 Phones and Windows Phones owned by the Office of Public Relations.

OPERATING SYSTEM	FIELD SETTING	PARAMETER	WMATA STANDARD	MDM SETTING[24]	COMPLIED
WINDOWS O/S	[redacted]				

Appendix C

M E M O R A N D U M

SUBJECT: Response to Evaluation Report OIG-17-004 Audit of WMATA's Mobile Computing Security Program

DATE: November 10, 2016

FROM: AGM IT/CIO - Kevin Borek

THRU: CIBO - John Kuo

TO: GM/CEO – Paul Wiedefeld

The following represents the Chief Information Officer's Corrective Action Plan (CAP) in response to OIG's *Audit of WMATA's Mobile Computing Security Program*. Eleven of the fourteen recommendations outlined in the audit are assigned to or require direct action from IT. These recommendations are listed below:

OIG Recommendation One:
Develop and implement comprehensive mobile device policies and corresponding SOPs that tie to WMATA's Mobile Device Strategy and best practices.

OIG Recommendation Five:
Develop and implement mobile device equipment classifications, for inventory purposes, to allow for the easy identification of mobile devices.

OIG Recommendation Six:
Develop and implement mobile device equipment classifications, for inventory purposes, to allow for the easy identification of mobile devices.

OIG Recommendation Seven:
Based on a risk assessment and best practices, develop and implement comprehensive mobile device security parameter standards for each supported mobile device operating system.

OIG Recommendation Eight:
Develop and implement WMATA Policy Instructions that describe phone service and plan optimization requirements, as well as provisions for de-provisioning mobile devices.

Washington Metropolitan Area Transit Authority

OIG Recommendation Nine:
Develop and implement departmental SOPs that includes, at a minimum, provisions for: (1) conducting routine and periodic review of mobile device plans, (2) discontinuing mobile device services because of no or low usage, and (3) conducting periodic certification of departments mobile device needs.

OIG Recommendation Ten:
Obtain and de-provision mobile phones issued to former employees as required by the MDM SOP.

OIG Recommendation Eleven:
Conduct a risk assessment on removable storage devices to determine the vulnerabilities and exposures to WMATA's network and system environments.

OIG Recommendation Twelve:
Centralize existing removable storage device requirements and update removable storage device policies, procedures and standards to include relevant best practices and provisions to limit or prevent risk assessment vulnerabilities.

OIG Recommendation Thirteen:
Commensurate with revised policy instructions, develop and implement automated controls to detect the use of removable storage devices and mitigate vulnerabilities.

OIG Recommendation Fourteen:
Based on best practices for mobile device security awareness training, enhance WMATA's current Mobile Device Security Awareness Training curriculum or develop a mobile device awareness/training curriculum specifically for WMATA employees who are issued mobile devices.

IT's Response
Due to the scope and complexity of these issues noted by OIG, IT will be developing an overarching mobile device management program. The development of this program to address these inter-related issues will be driven through two main components:

1. The development of a comprehensive mobile device policy and associated processes.

2. To supplement this policy and associated processes, WMATA IT will also be issuing an RFI to vendors to identify potential costs, activities and timelines needed to develop and implement a mobile device management program that is in line with OIG's recommendations.

IT will have the policy developed and RFI issued to vendors by *November 1, 2017*.

Appendix D

M E M O R A N D U M

SUBJECT: Response to OIG Evaluation Report No.17-04 – Mobile Computing Security Program

DATE: November 15, 2016

FROM: CFO – Dennis Anosike

THRU: GM/CEO – Paul J. Wiedefeld

TO: OIG – Helen Lew

The following represents the Chief Financial Officer's Corrective Action Plan (CAP) in response to OIG's Evaluation of WMATA's *Mobile Computing Security Program*. Three of the fourteen recommendations are assigned to the Chief Financial Officer (CFO), and one recommendation requires joint action from the CFO and IT.

OIG Recommendation 2
Determine whether AMB or IT will be responsible for the official inventory of "sensitive items" such as: laptops, tablets and mobile phones.

Management's Response:
Management accepts the above recommendation. IT will be responsible for the official inventory of "sensitive items" such as laptops, tablets and mobile phones.

OIG Recommendation 3
Develop and implement policy instructions, SOPs, and/or agreements to ensure "sensitive items" greater than $100, are automatically tracked and inventoried as required by the PACPPM.

OIG Recommendation 4
Update the PACPPM to clarify the definition of a sensitive item and provide examples of items that should be tracked.

Management's Response for Recommendations 3 & 4:
Management accepts the above recommendations with exception to assigning value to sensitive items as suggested in recommendation 3. Items are either sensitive or they are not. The PACPPM will be updated to clarify the definition of a sensitive item as well as provide examples of items that should be tracked. Management will also develop and implement policy instructions, SOPs, and/or agreements to ensure "sensitive items" are automatically tracked and

Washington Metropolitan Area Transit Authority

inventoried as required by the PACPPM. Both CAPs will be completed by November 1, 2017.

OIG Recommendation 5
Develop and implement mobile device equipment classifications, for inventory purposes, to allow for the easy identification of mobile devices.

Management's Response:
Management accepts this recommendation and will work with IT in developing a comprehensive mobile device policy with associated processes, which includes supporting their efforts in issuing an RFI to identify potential costs, activities and timelines needed to develop and implement a mobile device management program in line with OIG's recommendations. As IT indicated in their response, the policy will be developed and RFI issued by November 1, 2017.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: wmata-oig-hotline@verizon.net

Telephone: 1-888-234-2374

Address: WMATA
Office of Inspector General
Hotline Program
600 5th Street, NW, Suite 3A
Washington, DC 20001