M E M O R A N D U M

FINAL AUDIT REPORT WITH RECOMMENDATIONS
Information Technology No. 12-002

SUBJECT: Review of WMATA's Software/ Hardware Acquisition Process

DATE: May 25, 2012

FROM: OIG – Helen Lew /S/

TO: DGMA/CFO – Carol Kissal

This **Final Audit Report** entitled, *Review of WMATA's Software/Hardware Acquisition Process,* presents the results of our audit. The objectives of the audit were to determine whether the Washington Metropolitan Area Transit Authority (WMATA) is: (1) effectively managing the software and hardware acquisition process; and (2) making sound business management decisions in the acquisition of software and hardware.

Background

Information Technology Architecture Standards - In 2009 the Department of Information Technology (IT) developed an Information Technology Architecture Standards and Services Guide for WMATA; this Guide was updated in 2011. The Guide is a roadmap for program managers and IT professionals to align their plans and acquisitions with WMATA's comprehensive technology strategy. The Guide also establishes software and hardware standards and describes centralized services provided by the IT department. It is intended to help staff coordinate and communicate more closely with the IT department regarding information technology projects. IT established an Architecture Review Board[1] (ARB) on July 22, 2008, to complete IT standards. IT standards reduce overall

[1] The ARB's mission is to assure architecture quality in WMATA's IT systems throughout their lifecycles, with emphasis on the planning and development phases. The ARB's primary focus is maximizing the value of WMATA's capital IT investments by establishing standards between offices, common services, and infrastructure.

costs, streamline IT operations, and improve efficiency by optimizing the number of platforms the organization is required to support. When the Information Technology Architecture Standards and Services Guide (Guide) is used to make software and hardware purchases, WMATA can expect to realize the following benefits:

- Increase interoperability of systems
- Reduce complexity of WMATA's infrastructure to facilitate easier systems integration, easier upgrade paths for new product versions, and higher reliability
- Reduce acquisition costs by leveraging buying power and negotiating volume discounts
- Reduce support costs by allowing WMATA to leverage its technical staff
- Improve customer service by facilitating easier and more complete integration of real-time customer information and alerts
- Improve management of software/hardware assets
- Improve safety by facilitating easier communication of emergency and risk information

Additionally, program managers and IT professionals should refer to the Guide to determine if there are established product guidelines to follow. This applies to enterprise licenses and/or buying agreements for most common IT products.

ARB standards govern all new IT purchases (software/hardware) and upgrades. These standards span all areas of the automated environment, ranging from desktop applications to server applications, databases, utilities, business applications, network management, and computer hardware configurations.

Software and Hardware Governance

WMATA Policy and Procedures - Information Technology Investment Process, Policy Instruction (P/I) 15.2/0, dated October 2, 2001, established policy to ensure IT investments, including non-IT programs with an IT component or sub-component, are managed to directly support WMATA's strategic mission(s) and business goals.

According to WMATA's Policy/Instruction (P/I) 8.0, section 8.5/1, dated June 27, 2002, (Procurement of Administrative EDP Equipment and Services), WMATA is to establish controls on the acquisition of network servers, personal computers (PCs), PC peripheral equipment and software to ensure those procurements are compatible with existing network infrastructure and technically sound. Offices involved in the above acquisitions should prepare a Computer Authorization for Expenditure (CAFÉ). The CAFÉ must contain a justification for the procurement, the budgeted funding source, and if applicable, system configuration information. The CAFÉ is submitted to IT along with the system configuration proposal, or a request for IT to configure, for approval.

WMATA's P/I section 8.11/0, section 1.00, dated May 29, 2008, (Purchase Card Policy), states it is the policy of WMATA "to use purchase cards as operationally practical for authorized Metro requirements." WMATA purchase cards may be used for:

(a) Purchases at or below $5,000 for non-federally funded requirements
(b) Orders against established contracts or purchase orders up to the simplified acquisition threshold of $100,000

Conversely, Section 10.10 of P/I 8.11/0 for "Unauthorized (Prohibited) Use of Card" states the purchase card is strictly prohibited for use (among other things) for the following:

"IT equipment, systems, and services (i.e., (a) computer racks; (b) data circuits; (c) databases or data services; (d) firewalls; (e) information technology services; (f) large display screens (LED/LCD); (g) modems; (h) network-capable devices (any device connected to Metro's data network); (i) network printers; (j) network switches; (k) personal computers (laptops and desktops); (l) personal digital assistants (PDA); (m) servers; (n) software (network application and operating system); (o) routers; (p) telephone sets; (q) telephone systems; and (r) wireless network access points)."

WMATA's Policy Memorandum No. 08-08, dated September 3, 2008, requires the Assistant General Manager (AGM) of IT to approve all enterprise-wide and departmental information technology and telecommunications systems and services procurements over $25,000.

IT developed a Portfolio Management and Business Plan Initiation Process, version 1.0, dated February 18, 2011. This process was developed by IT as policy for software and hardware purchased for IT managed System Development Life Cycle (SDLC) projects. This policy is not a WMATA-wide policy. The policy requires IT to:

- Align the IT program/project to the WMATA and IT strategic initiatives
- Complete the business case and cost benefit analysis
- Create/manage a project portfolio
- Secure funding through a business plan initiation (BPI)
- Establish/update project services

Audit Results

We determined WMATA is not effectively managing its software and hardware acquisition process. Specifically, the IT Department does not have authority-wide oversight over WMATA's software and hardware acquisition process, and IT and the Office of Procurement & Materials (PRMT) cannot fully account for all software and hardware acquisitions. We also determined before February 18, 2011, IT was not making sound business management decisions in the acquisition of software and hardware. IT was not consistently providing business justifications; including cost benefit analysis, expected outcome, and deployment timeline for the acquisition and implementation of some software. However, we found IT now has implemented a process to better document its management decisions. This new process is limited to acquisitions by IT and is not a WMATA-wide requirement.

We also raised concerns regarding: (1) inadequate verification of data removed from computer hard drives prior to public auction, (2) Microsoft Enterprise discount program for Microsoft Office Suite was not communicated to all WMATA employees and (3) some IT equipment and computer accessories purchased by IT are stored for two or more years after acquisition. These matters are discussed in the "Other Matters of Concern" section of this report.

Based on the above findings, we made six recommendations to the Deputy General Manager Administration/Chief Financial Officer's (DGMA/CFO).

In the DGMA/CFO's May 15, 2012 revised response to a draft of this report, she generally agreed with the findings and four of the six recommendations. The DGMA/CFO partially disagreed with Finding 1, as it relates to OIG's assessment of the potential system vulnerability to WMATA. Management also disagreed with Recommendation 1.1 because they believe the OIG solution articulated an overly prescriptive solution to identify potential purchases. Management deemed

this solution to be impractical to implement and enforce and estimated that it would cost roughly 700K in software development to execute in PeopleSoft. Management also disagreed with Recommendation 2.1, stating WMATA operates in a decentralized management mode, making it difficult to impose standardized methodologies for project management across the entire organization. Management indicated that "IT-like" projects that are not managed by IT and pose no risk to the corporate network, because those projects do not touch the network, do not necessarily have to use the methodologies developed by IT. The complete text of the DGMA/CFO response is included as Attachment 1 to this report.

We disagree with Management's comments regarding our assessment of the potential system vulnerability to WMATA and that they have sufficient controls in place to address software and hardware compliance. System vulnerabilities are weaknesses or design flaws in the software and hardware installed on a server or client that can be exploited by an intruder to gain access to the network. Failure to comply with WMATA's policy and procedures and IT standards increase the risk of system vulnerabilities occurring. We also disagree with Management that Recommendation 1.1 is an overly prescriptive solution to identify potential purchases, impractical to implement, and an unnecessary expense. Management already acknowledged in its comments that PeopleSoft currently captures software and hardware purchases through account codes. We agree with Management that as long as the requestor identifies the procurements properly, reporting can be generated on these specific codes to review. Accordingly, Management may want to revise applicable policy and procedures to require requesting offices/departments to ensure that their staff properly code software and hardware acquisitions. Lastly, Recommendation 2.1 is focused on those "IT-like" acquisitions that do touch the network and/or require IT assistance or support. It is important that these types of acquisitions be coordinated with IT.

FINDING 1: WMATA Has Not Effectively Managed Its Software And Hardware Acquisition Process

We found IT and PRMT do not have authority-wide oversight over WMATA's software and hardware acquisition process and could not fully account for all software and hardware acquisitions. We requested from IT, a listing of all WMATA software and hardware acquisitions for FY 2010 and FY 2011. IT, however, could only provide the listing of software and hardware that IT purchased for its managed projects. Personnel in the Office of Project Management Operations (PMO) stated they do not know all WMATA-wide software and hardware purchases.

We also requested PRMT to provide us with a list of WMATA's software and hardware acquisitions for FY 2010 and FY 2011. PMRT could only provide a list of software and hardware items purchased for IT managed projects.

At the time of our audit, IT and PRMT had not established and implemented an authority-wide coordinated approach for tracking and controlling software and hardware acquisitions. According to IT personnel we interviewed, the departments are not held accountable to adhere to policies and/or procedures related to software and hardware acquisitions. There is no enforcement mechanism to ensure compliance with existing IT acquisition standards, policies and procedures.

For example, we reviewed the PeopleSoft Procurement Module, which tracks all procurement records, and found there is no specific account code utilized to identify and track software and hardware purchases. We confirmed our observations with the IT PMO. WMATA software and hardware acquisitions were buried in other types of acquisitions. Without implementing or identifying specific account codes or other tracking mechanism in the PeopleSoft system, IT cannot adequately identify, enforce policy, and account for all WMATA software and hardware acquisitions.

There is no official tracking of WMATA-wide IT related acquisitions by the various departments. However, with the help of the Data Center & Infrastructure office, we were able to identify several authority-wide software and hardware purchases made in violation of policies requiring IT review and approval. For example, we found:

- Some IT software and hardware acquisitions were made without using the required CAFÉ system
- Some software and hardware acquisitions did not comply with WMATA's Information Technology Standards and Services Guide
- WMATA did not always follow purchase card procurement policies, and
- A software and hardware acquisition above $25,000 had not been approved by the AGM of IT, as required

Software and hardware acquisitions made outside of the CAFÉ system, as well as non-standard software and hardware acquisitions could result in incompatible software and hardware incompatibilities within the IT infrastructure and possibly lead to system vulnerability issues. These issues could also have a serious impact on the development and maintenance of WMATA's current IT infrastructure. In addition, these acquisitions could result in unnecessary expenditures for IT support.

The following sections discuss the deficiencies we found under Finding #1:

Some IT software and hardware acquisitions were made without using the CAFÉ system - A CAFÉ is used to ensure procurements, such as network servers, personal computers, PC peripheral equipment and software, are compatible with existing network infrastructure and technically sound. The CAFE must contain information justifying the procurement (acquisition), and identifying the budgeted funding source and system configuration. The CAFÉ is submitted along with the system configuration proposal or request to configure for IT approval. IT determines if the equipment requested complies with the network configuration requirements. The Business Administration Manager, Office of Project Management Operations, and the Chief Project Management Officer informed us that all requests for IT acquisitions require a CAFÉ.

Software and hardware acquisitions made outside of the CAFÉ system could result in incompatible software and hardware within the IT infrastructure and possibly lead to system vulnerability issues.

To determine whether WMATA offices prepared a CAFÉ, as required, we asked the IT Data Center & Infrastructure (DCI) Inventory Specialist to provide us with supporting documentation of all CAFÉ purchases from December 2010 to August 2011. The Inventory Specialist provided us with the Property Transaction Requests[2] (PTRs) they had for software and hardware acquisitions for the period we requested. The PTR's list acquisitions that have been bar-coded in the fixed asset system; they provided us with the best documentation of the universe of IT related acquisitions. We reviewed 210 items on the 49 PTR's provided to us. We found several deficiencies, such as non-CAFE IT software and hardware acquisitions, non-standard IT software and hardware acquisitions, and IT

[2] According to the Office of Accounting Procedures Manual, the PTRs are the primary source document for transactions affecting capital and non-capital assets that can be bar-coded.

purchase card acquisitions in violation of the purchase card policy (See Tables 1 through 3 below). IT personnel informed us some offices do not always comply with the policy. The Acting Chief of Data Center and Infrastructure stated there appears to be a lack of compliance and enforcement of the policy Authority-wide. In addition, the Business Administration Manager, IT PMO, stated he has verbally reported offices that have circumvented the CAFÉ process in the past. In most cases, IT would send a notification to the violating office, but it would eventually agree to provide IT support.

Table 1 depicts information provided by the Data Center and Infrastructure office of some software and hardware purchases made by offices within the Transit Infrastructure and Engineering Services Department, which were outside the CAFÉ system.

Table 1- WMATA Non-CAFE IT Software And Hardware Acquisitions

Item Purchased	Office Code	Acquisition Date	Quantity	Unit Cost	Value
Dell Optiplex 780	12310	05/25/2011	45	$847.00	$38,115.00
Dell P2011H Monitor	12310	05/25/2011	44	$169.00	$7,436.00
Server R610	12310	05/18/2011	6	$7,280.00	$43,680.00
Dell-Optiplex-380	31000	01/25/2011	5	$699.00	$3,495.00
Dell-Inspiron-N1150	39500	07/18/2011	7	$699.99	$4,899.93
Total Value					**$97,625.93**

Some software and hardware acquisitions were not in compliance with WMATA's Information Technology Standards – We found several instances where WMATA made software and hardware purchases that did not comply with established standards. The Information Technology Standard and Services Guide provides guidance on approved IT products, standard version numbers, and sourcing options. For example, Microsoft Windows is the approved desktop

operating system, XP Professional is the version, and the Data Center & Infrastructure Desktop Customer Service is the sourcing option. The Guide is to be applied when a department/office makes IT purchases, or plans IT projects to ensure acquisitions are in line with WMATA standards.

Table 2 lists some instances of non-standard software and hardware purchases we found during our audit.

Table 2 - WMATA Non-Standard IT Software And Hardware Acquisitions

Item Purchased	Office Code	Acquisition Date	Quantity	Unit Cost	Value
Citizen Thermal Printer	12310	05/13/2011	44	$375.00	$16,500.00
Focus Scanner	12310	05/13/2011	46	$525.00	$24,150.00
Dell P2011H Monitor	12310	05/25/2011	44	$169.00	$7,436.00
F5 Networks (F5 BIG IP GTM)	84700	01/18/2011	2	$24,590.00	$49,180.00
Apple Mac Pro QC XEON	62100	06/20/2011	2	$2,723.95	$5,447.90
Microsoft Office Home & Business 2011 (Mac)	62100	06/20/2011	4	$206.95	$827.80
Apple 27 LED Cinema Display	62100	06/20/2011	3	$921.98	$2,765.94
Adobe Design STD CS5 F/Mac (WEB)	62100	06/20/2011	2	$1,196.18	$2,392.36
Apple Mac Book[3]	84700	01/3/2011	1	$2,494.00	$2,786.00
Total Value					**$111,486.00**

[3] Includes Microsoft Office Home & Business 2011 (Mac)

Control Objectives for Information and related Technology (COBIT),[4] Acquisition and Implementation, §AI5.1, provides "management develop and follow set procedures and standards that are consistent with the business organization's overall procurement process and acquisition strategy to ensure the acquisition of IT-related infrastructure, facilities, software, hardware and services satisfies business requirements." Failure to follow established standards and policies may result in additional costs and inefficiencies in optimizing the number of platforms the organization is required to support.

WMATA did not always follow purchase card procurement policies – We found several instances during our review of the PTR's where department personnel used WMATA purchase cards to purchase IT software and hardware in violation of Purchase Card P/I, 8.11/0 §10.10. Table 3 below lists some examples of IT software and hardware acquisitions made with the purchase cards.

The PRMT Purchase Card Administrator (PCA) for purchase cards told us the department approving officials should be reviewing all purchase card transactions. The PCA stated while PRMT conducts periodic reviews of purchase card transactions, it is difficult to review all purchase card transactions to ensure compliance with the purchase card policy. He also stated IT related purchases using a purchase card should only be made by IT (P/I 8.11/0, section 13.07). PRMT personnel informed us they have verbally recommended department personnel consult with IT prior to purchasing IT-related items with a purchase card; however, there have been inconsistencies with this practice.

[4] COBIT is a group of generally applicable and accepted standards for good practice for IT controls

Table 3 - IT Purchase Card Acquisitions In Violation Of Policy Instruction 8.11/0

Item Purchased	Office Code	Acquisition Date	Quantity	Unit Cost	Value
Dell-Inspiron-N1150 computers	39500	07/18/2011	7	$699.99	$4,899.93
Dell-Optiplex-380 computers	31000	01/25/2011	5	$699.00	$3,495.00
Dell-Precision-T3500 computer	31000	01/25/2011	1	$1,098.00	$1,098.00
Total Value					**$9,492.93**

According to the IT Business Administration Manager, IT would not know department personnel used the purchase card for IT purchases unless they notify IT. Failure of departments to comply with Purchase Card Policy (P/I, 8.11/0 §10.10) and procedures has resulted in improper and questionable purchases.

The AGM of IT had not approved all software and hardware acquisitions valued above $25,000 - WMATA Policy Memorandum No. 08-08, dated September 3, 2008, reinforced the requirement that "all enterprise-wide and departmental information technology and telecommunications systems and services procurements over $25,000 require the signature of the AGM of the Department of Information Technology." This Policy Memorandum also assigns responsibility for the Contract Administrator to informed "his/her customer that approval of the AGM is necessary before any procurement activity may take place, even though funding may have been allocated."

We asked the Chief Procurement Officer to provide a list of IT procurements above $25,000 submitted to the AGM of IT for approval during fiscal years 2010 and 2011. The Chief Procurement Officer could not provide any IT procurements above $25,000 submitted to the AGM of IT for approval during that period. We

asked the AGM of IT if he had approved any IT procurements above $25,000 for FY 2010 and FY 2011. He provided two approvals for IT procurements above $25,000. He stated these were the only two approvals PRMT requested. The two IT procurements were budgeted for fiscal year 2012. The AGM of IT informed us that IT does not know of software and hardware purchases above $25,000 unless PRMT requests approval and forwards the requisitions accordingly.

From the PTR list provided by the IT Data Center & Infrastructure Office, we found several solicitations with a procurement value of approximately $81,000 that did not have AGM of IT approval. The solicitations were for personal computers and servers purchased in May 2011 utilizing Purchase Order (PO) number 5112011.

The failure to have adequate oversight and enforcement of procedures for acquiring software and hardware could also result in improper, wasteful and questionable purchases.

Recommendations:

We recommend the Deputy General Manager of Administration/Chief Financial Officer:

1.1 Direct the CIO to work with PRMT to implement PeopleSoft application controls, such as specific account codes that will identify and track software and hardware procurements and implement controls to ensure this process is followed.

1.2 Direct the CIO and Chief Procurement Officer to develop adequate controls to monitor and enforce compliance with current IT procurement policies and procedures and to effectively monitor WMATA-wide software and hardware purchases.

Management Comments

The DGMA/CFO partially agreed with Finding 1, as it relates to the inefficiencies of managing IT in a decentralized business management environment. However, Management strongly disagreed with OIG's assessment of the potential system vulnerability to WMATA. Management agreed there should be proper controls over software and hardware procured for deployment on WMATA's primary IT-supported network, both for fiduciary accountability and to reduce the potential for network and resource vulnerabilities. Management believes the finding requires them to create a single, enterprise-wide procurement span of control in Peoplesoft with prescriptive codes and workflows in order to achieve this objective.

Management also disagreed with Recommendation 1.1 because it articulates an overly prescriptive solution to identify potential purchases, which Management deems impractical to implement and enforce. IT estimated that it would cost roughly 700K in software development to execute the referenced OIG proposal in PeopleSoft. Management believes this is impractical and would be an unnecessary expense because the vast majority of IT procurements are currently using the IT-established processes and procedures. Management also believes the responsibility for policy enforcement is improperly weighted towards IT and PRMT in the OIG recommendations and too little enforcement obligation is placed upon the procuring organizations.

Management agreed with Recommendation 1.2. but believed sufficient controls are either in place or under development to address software and hardware compliance.

OIG's Comments

We disagree with Management's comments regarding our assessment of the potential system vulnerability to WMATA and that they have sufficient controls in place to address software and hardware compliance. Our audit found (1) some IT software and hardware acquisitions were made without using the required CAFÉ system and (2) some software and hardware acquisitions were not in compliance with WMATA's IT standards. Failure to comply with WMATA's policy and procedures for software and hardware acquisitions and IT standards increase the risk of system vulnerabilities occurring. System vulnerabilities are weaknesses or design flaws in the software and hardware installed on a server or client that can be exploited by an intruder to gain access to the network.

We also disagree with Management that Recommendation 1.1 articulates an overly prescriptive solution to identify potential purchases and is impractical to implement and an unnecessary expense. Management acknowledged in its comments that PeopleSoft currently captures software and hardware purchases through account codes (50499680 - M&S Software and 5049940 - PC Equipment). We agree with Management that as long as the requestor identifies the procurements properly, reporting can be generated on these specific codes to review. Accordingly, Management may want to revise applicable policy and procedures to require requesting offices/ departments to ensure that their staff properly code software and hardware acquisitions.

Finding 2: IT Is Making Better Business Management Decisions In The Acquisition Of Software And Hardware, But Other WMATA Departments/Offices Are Not

We found that prior to February 18, 2011, IT had not consistently provided justifications, including cost benefit analysis, expected outcomes, and deployment timelines for the acquisition and implementation of software.

However, in February 2011, IT issued a Portfolio Management and Business Plan Initiation Process which applies only to software and hardware purchased for IT managed System Development Life Cycle (SDLC) projects. This internal departmental policy requires IT to complete a business case and perform a cost/benefit analysis on the reason for the purchase, expected solutions, deployment timeline, cost and labor, estimated benefits and savings associated with the purchase. We selected 2 out of 10 software acquisitions made after February 18, 2011, and was satisfied IT had followed the new process.

We asked the PMO Chief if the new process is required for WMATA-wide software and hardware projects where IT is not involved. She stated the Portfolio Management and Business Plan Process is only a requirement for IT managed SDLC projects. We did not find a Policy Instruction requiring departments to use IT's or similar processes for software and hardware projects.

The failure to require WMATA-wide business plans and processes for acquiring software and hardware can result in improper, wasteful and questionable purchases.

Recommendation:

We recommend the Deputy General Manager of Administration/Chief Financial Officer:

2.1 Direct the CIO to develop a P/I requiring all departments/offices within WMATA to coordinate acquisition and implementation of software and hardware projects with IT and follow IT's Portfolio Management and Business Plan Initiation Process or similar process for software and hardware acquisition and implementation.

Management Comments

Management agreed with Finding 2 as it relates to IT practices but had no knowledge of the quality of project management outside of IT projects and therefore, no opinion.

Management disagreed with Recommendation 2.1. Management stated WMATA operates in a decentralized management model, making it difficult to impose standardized methodologies for project management across the entire organization. Management has many "IT-like" projects throughout the Authority that are not managed by IT, but pose no risk to the corporate network because those project do not touch the network. These IT-like projects do not necessarily have to use the methodologies developed by IT, but IT's methodology could serve as a template for the development of their own processes.

OIG's Comments

We agree with Management that there are "IT-like" projects throughout the Authority that are not managed by IT and pose no risk to the network. Our recommendation is focused on those IT-like acquisitions that do touch the network and/or require IT assistance or support. For example, IT was not aware that some of the software and hardware acquisitions we identified during our audit required their assistance and support to operate correctly. Management may want to emphasize to all offices/departments the importance of coordinating with IT on all software and hardware acquisitions that affect the network and server environment or that involves IT assistance or support.

OTHER MATTERS OF CONCERN

During our audit, we identified three matters of concern: (1) inadequate verification of data removed from computer hard drives prior to public auction, (2) Microsoft Enterprise discount program for Microsoft Office Suite is not communicated to all WMATA employees, and (3) some IT equipment and computer accessories purchased by the IT department and are stored for two or more years after acquisition. Each of these matters of concern is discussed below.

Inadequate verification of data removed from computer hard drives prior to public auction – The IT DCI office uses a software application to remove data from the hard drives of surplus computers before they are sent to WMATA's Landover warehouse for public auction. During our audit, we observed an IT DCI contractor removing data from a hard drive and not verifying whether the data was completely removed.

We randomly selected three hard drives from WMATA's Landover warehouse to determine the adequacy of the data removal process. We reviewed software the IT DCI office used to remove data from the hard drives. We found the contractor was not using the data removal technology properly to effectively remove data from WMATA's hard drives. We used simple, low-cost data retrieval software available on the Internet to retrieve sensitive data such as a resume from two hard drives destined for public auction. We immediately informed IT DCI personnel of our finding on October 16, 2011. IT DCI personnel promptly responded the next day and sent a memo stating they would use new technology to completely remove all data from WMATA's hard drives intended for surplus.

We randomly picked a sample of 3 hard drives after the new technology was purchased and tested the hard drives intended for surplus. We found the data on the hard drives were adequately removed.

WMATA help desk Handbook states "surplussing" will be conducted on a weekly basis and consist of two operations: wiping, and surplussing. The wiping consists of removing all information from an asset's hard drive; surplussing consists of the physical removal of inactive IT assets from the active inventory. The logistician is responsible for ensuring each operation is completed and will report directly to the Help Desk Manager on the success of the operations. In addition, a Property Transaction Record will be prepared, indicating its removal and assigning it to the proper category prior to an asset's removal.

COBIT Framework for IT Governance and Control (Control DS11.4 Data Management on Disposal) requires IT to define and implement procedures to prevent access to sensitive data and software from equipment or media when they are disposed of or transferred to another use. Such procedures should ensure data marked as deleted or to be disposed cannot be retrieved. Failure to properly use the data removal technology and verifying the completeness of the data removed from hard drives increase the risk that critical and sensitive business data stored on surplus computers is compromised and used for illegal purposes.

Recommendation:

We recommend the Deputy General Manager of Administration/Chief Financial Officer:

3.1 Direct the CIO to implement procedures and controls to verify hard drives are adequately wiped before surplussing and to periodically test the data removal process to ensure compliance.

Management Comments

Management concurred with this finding and agreed with recommendation 3.1 which directs the CIO to implement procedures and controls to verify hard drives are adequately wiped and tested before surplussing. Management indicated they have already implemented procedures and controls as indicated in the draft report.

OIG's Comments

We agree that management purchased new technology to remove data from WMATA's hard drives intended for surplus. However, we disagree that management has implemented controls to test and periodically verify that the hard drives are adequately wiped and tested before surplussing. Management needs to implement procedures and controls for the verification and testing process.

IT Microsoft Enterprise discount program for Microsoft Office Suite is not communicated to all WMATA employees - We found IT did not make the Microsoft Enterprise discount program for the Microsoft Office Suite known to all WMATA employees. Although the discount program does not increase WMATA's overall cost, the program allows employees to purchase the Microsoft Office Suite for $20, a significant discount from the retail price. The purpose of the Microsoft Enterprise program is to encourage employees to purchase the Microsoft Office Suite and avoid fines and penalties associated with pirating of software.

Recommendation:

We recommend the Deputy General Manager of Administration/Chief Financial Officer:

3.2 Direct the CIO to make the Microsoft Enterprise discount program for the Microsoft Office suite known to all eligible WMATA employees.

Management Comments

Management concurred with this finding and agreed with recommendation 3.2 to make the Enterprise discount program for the Microsoft Office suite known to all eligible WMATA employees. IT will work with HR to publicize this in the employee discount section on WMATA intranet.

OIG's Comments

The corrective actions taken or planned by management should address our recommendations if properly implemented.

Some IT equipment and computer accessories purchased by the IT department had been sitting unused in the IT storage room for two or more years after acquisition – During our audit we discovered three paper feeders purchased for $2,688 on November 20, 2009 (PO number: 0000042305), and 11 Dell 20 inch monitors purchased for approximately $2,200 on April 17, 2009, that were still in storage as of August 31, 2011. After bringing the discovery to their attention, the IT DCI team immediately redistributed and/or deployed the items to different PC replacement projects.

Recommendation:

We recommend the Deputy General Manager of Administration/Chief Financial Officer:

3.3 Direct the CIO to develop and implement controls to ensure IT equipment and computer accessories purchased are distributed and/or deployed in a timely manner.

Management Comments

Management concurred with this finding and agreed with recommendation 3.3. Management "has instituted a procedure where by equipment that is ordered by other departments and accepted after 30 business days, and after 3 attempts to contact to [sic] the purchasing department, will be redeployed to other business units that have a need for the equipment. This will eliminate the problem of equipment being purchased and not utilized in a timely manner.

OIG's Comments

The corrective actions taken or planned by management should help address our recommendations if properly implemented.

Objectives, Scope and Methodology

The objectives of the audit were to determine whether (1) WMATA is effectively managing its software and hardware acquisition process and (2) WMATA is making sound business management decisions in the acquisition of software and hardware. WMATA did not have a tracking mechanism in place for tracking all software and hardware acquisitions. To accomplish our audit objectives, we reviewed 210 WMATA IT purchases listed on the Property Transaction Requests that IT maintained during the period of FY 2010 and FY 2011 for some software and hardware acquisitions. We also sampled and verified 2 out 10 software acquisitions made by IT after February 18, 2011.

We reviewed CAFÉ purchases identified for the period of our scope. We reviewed previous OIG work and collected information pertaining to software acquisitions. We used the following methodology in gathering data and conducting tests: (1) conducted interviews with key responsible IT, PRMT and Office of Chief Financial Officer (CFO) personnel; (2) reviewed WMATA's procurement process and documentation; (3) conducted physical walkthroughs of three WMATA sites (IT storage room, Stone Straw Building, and Open Materials Storage Facility); (4) reviewed other documentation (invoices, PTR's, business plan initiation forms (BPI's), and purchase orders) and (5) conducted follow-up interviews as needed. We also reviewed IT policy and new processes related to our objectives and scope, including the Portfolio Management and Business Plan Initiation Process and policy instructions.

We tested three hard drives that were destined for public auction to determine the adequacy of the data removal process. We reviewed the Microsoft Office Suite program.

We held an exit conference on February 9, 2012, to discuss the findings and recommendations derived from the audit with management personnel. We conducted our audit in accordance with *Government Auditing Standards* appropriate to our scope. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program activity or function under audit. An audit includes assessment of applicable internal controls and compliance requirement of laws and regulations when necessary to satisfy our audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

Administrative Matters

Corrective actions proposed (resolution phase) and implemented (closure phase) by the affected Departments/Offices will be monitored and tracked through the Office of Inspector General's Audit Accountability and Resolution Tracking System. OIG policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items and targeted completion dates necessary to implement final corrective actions on the findings and recommendations contained in this report.

We appreciate the cooperation and assistance extended by your staff during the audit. Should you or your staff have any questions, please contact Andrew Clemmons, Assistant Inspector General for Audits on (202) 962-1014, or me on (202) 962-2515.

Attachment

cc: GM/CEO - R. Sarles
CHOS - S. Pant
CIO/IT - K. Borek
DGMO - D. Kubicek
PRMT - H. Obora
COUN - C. O'Keeffe

Attachment 1

M E M O R A N D U M

SUBJECT: IT No. 12-002: Review of WMATA's Software/Hardware Acquisition Process

DATE: May 15, 2012

FROM: DGMA/CFO – Carol Dillon Kissal

TO: OIG – Helen Lew

The subject draft report, IT No. 12-002: Review of WMATA's Software/Hardware Acquisition Process, was issued on March 6, 2012. WMATA management provided a formal response dated March 27, 2012 and upon further discussion with the Office of Inspector General (OIG) provides a revised response as noted below.

OIG Recommendations

Finding 1 – WMATA Has Not Effectively Managed Its Software and Hardware Acquisition Process

Recommendation:
We recommend that the Deputy General Manager of Administration/Chief Financial Officer:

1.1 Direct the CIO to work with PRMT to implement PeopleSoft application controls, such as specific account codes that will identify and track software and hardware procurements and implement controls to ensure this process is followed.

1.2 Direct the CIO and Chief Procurement Officer to develop adequate controls to monitor and enforce compliance with current IT procurement policies and procedures and to effectively monitor WMATA-wide software and hardware purchases.

Management Response:

1.1 and 1.2

IT and PRMT partially agree with Finding 1, as it relates to the inefficiencies of managing IT in a decentralized business management environment. However, IT strongly disagrees with the assessment of potential vulnerability for reasons described within this response. IT and PRMT also disagree with Recommendation 1.1, as it articulates an overly prescriptive

solution to identify potential purchases, which is deemed impractical to implement and enforce. IT and PRMT also believe that the responsibility for policy enforcement is improperly weighted towards IT and PRMT in the IG recommendations and that too little enforcement obligation is placed upon the procuring organizations. IT and PRMT agree with Recommendation 1.2.

IT and Procurement agree that there should be proper controls over software and hardware procured for deployment on WMATA's primary IT-supported network, both for fiduciary accountability and to reduce the potential for network and resource vulnerabilities. However, the IG presumption in the audit finding is that it is necessary to create a single, enterprise-wide procurement span of control in Peoplesoft with prescriptive codes and workflows in order to achieve this objective. The IG also presumes a span of control within IT to enforce compliance with current policies that doesn't exist in a complex, decentralized management environment such as WMATA. IT and PRMT do not believe that Recommendation 1.1 would be practical and also believe that current and future planned activities provide an adequate level of control (already meeting the intent of Recommendation 1.2) in this organizational environment.

Recommendation 1.1
IT estimates that it would cost roughly 700K in software development to execute the referenced IG proposal in PeopleSoft. IT and PRMT believe that this is impractical and would be an unnecessary expense, because the vast majority of IT procurements are currently made using the IT-established processes and procedures and those that are not are eventually captured via network monitoring controls.

Also, the IG-proposed process would not prevent individuals from bypassing the system through the use of non-IT codes or making off-book purchases with P-cards. IT and PRMT believe that proper procurement enforcement first rests with the initiating department and it is the department manager's obligation to follow established policy and procedures. Unless IT procurement is centralized, the responsibility for properly coding a procurement and identifying the IT components rests with the originator and not Procurement, nor IT.

Although most IT procurements are made using established processes and without issue, occasionally items are purchased as a part of a larger contract or outside of established processes. Items that are not compliant with IT policy are identified and denied connectivity via network controls if appropriate (described further in this response). Finally, all of the referenced purchases noted in the audit report were either known prior to purchase (Apple products for Customer Service) or items purchased as a part of a larger contract and eventually were processed by IT prior to commissioning.

Although IT has no exact figure of how much equipment is purchased outside of established policy (for the reasons described), it is believed to be very small and generally printers or peripheral devices purchased by the departments, which pose little to no risk to the Authority. Also, personal printers and scanners are eventually going to be displaced as a part of a managed print services initiative that is being launched in 2012, which will reduce the future opportunity to purchase items outside of established policy.

In summary, a single, enterprise-wide span of IT procurement control would only work within a complimentary business environment, where funding, incentives and penalties were aligned within a common organizational framework. It is impractical, therefore, for IT to enforce compliance in the described manner, since WMATA operates in a decentralized model. Additional procurement policy enforcement needs to be placed within the procuring organizations, as there is no practical mechanism for it to be further enforced by IT or PRMT.

Recommendation 1.2:
IT and PRMT agree with Recommendation 1.2, but believe that sufficient controls are either in-place or under development to address software and hardware compliance.

IT recognizes the limitations of direct enforcement capability as described in Recommendation 1.1 and either has or is developing both administrative and technical controls that adequately address both fiduciary and systematic risk. It is a multi-pronged approach incorporating a reasonable level of financial control, policy/procedure, inventory management and specific systematic tools/procedures as described below:

Administrative Controls

PeopleSoft:
Software and hardware purchases that are properly coded are currently captured in PeopleSoft. In reviewing current procurement processes and general ledger accounts, IT and PRMT believe that adequate controls exist in the use of accounts specifically for hardware and software, 50499680 – M&S Software and 50499940- PC Equipment. IT procurements are initiated and accounting codes assigned by the requestor to the appropriate classification within PeopleSoft. As long as the requestor identifies the procurements properly, reporting can be generated on these specific codes to review Authority-wide purchases based upon these classifications and purchases can be traced back to specific requestors.

Hardware and peripheral equipment purchases are also bar-coded and tracked within the PeopleSoft fixed asset module. Each office property

custodian is required to complete the PTR form and submit a copy to both Accounting and IT for tracking. The last Authority-wide bi-annual fixed asset inventory was conducted in the fall of 2010. The next audit is scheduled for the fall of 2012.

Policies and Instructions:
In addition to the PeopleSoft control referenced above, below is a list of some additional processes and P/Is related to the procurement, deployment and management of IT assets within the Authority:

- Related Policies and Instructions (P/Is):
    - **P/I 15.9 Network Connectivity** – stipulates that PCs connected to WMATA network must use the IT issued standard image. This image does not allow for a regular user to modify or install software without IT assistance. All WMATA business related software is preloaded onto all PCs that IT deploys to WMATA. Any additional software that is required will be coordinated through IT for centralized deployment and management.
    - **P/I 15.15 Software License and Digital Rights Management** – stipulates that only properly licensed software that is for approved WMATA business use is to be installed on WMATA PCs.
    - **P/I 15.20 Procurement of Administrative Information Technology Equipment and Software**, approved on 3/5/2012, requires all hardware and software to be requested through the café system which triggers an IT review and approval This approval signifies that the technology purchase is compatible with IT standard configuration and with network and security requirements. ***As a result of this audit, clarification of the enforcement responsibility will be revised to indicate that the initiator of the procurement is responsible for ensuring that any IT purchase has the appropriate IT review and approval.***

Technical Controls

Network Access Control:
WMATA IT Security monitors the WMATA network for changes to its infrastructure and software on WMATA owned and managed personal computers (PCs). All WMATA managed PCs are required to be part of the network domain and have a standard image. This includes appropriate antivirus, anti-spyware, and other required security software and maintenance of the latest operating system and application software patches.

In the current environment, any hardware that is connected to the network that does not meet this criteria or is unregistered, or unknown, is tagged as a non-compliant device via Network Access Control (NAC). When a system is identified as non-compliant on the WMATA network, IT Security identifies the system and electronically "disconnects" the device from the network or services as appropriate. This can be done in a matter of minutes if necessary. While performed manually today, NAC processes will be automated in FY 2013, which will require / enforce network identification, authentication, and authorization of any device that attempts to connect to WMATA's network without manual intervention. If the device does not meet the criteria set forth by IT Security for access to the network, the device will be considered a non-compliant device and will be automatically denied access, including any purchased hardware that is not processed by IT without the IT standard image and requisite software, unless justifiable exceptions are negotiated between IT and the requesting departments.

There are justifiable reasons to allow non-compliant systems on the corporate network, including the need to run legacy systems, proprietary applications and contractor-supplied solutions. Today, there are approximately 12,000 independently addressable devices on WMATA's IT-managed network, with only 124 identified as being non-compliant (1.03%). These are known devices (i.e. legacy computers, contractor computers, etc.) and as such, do not materially impact systems vulnerability. IT assumes that even after NAC automation is deployed, there will always be some exceptions operating in the network. Managing these exceptions is consistent with best industry practice.

System Center Configuration Manager:
Another automated tool that is currently being deployed (June 2012) is Microsoft's System Center Configuration Manager (SCCM). This is a centrally managed automatic software inventory collection tool and will provide real time visibility of the software installed on all managed systems. The tool provides functionality for Application Delivery, Mobile Device Management, Virtual Desktop Management, Endpoint Protection, Compliance & Settings Management, Software Update Management, Operating System Deployment, Asset Intelligence, and Inventory.

SCCM allows the creation of a baseline for "desired configuration state", and then ensure that all user devices comply with that baseline through either auto remediation or alerts as it monitors and controls baseline drift. SCCM also assists with delivering and managing updates to IT systems across the enterprise. IT administrators can deliver updates of Microsoft products, third-party applications, hardware drivers, and system BIOS to a variety of devices, including desktops, laptops, servers, and mobile devices.

The implementation of SCCM, NAC and other IT controls will provide many layers of protection from unwelcomed, un-patched and unmanaged devices accessing the WMATA corporate network and these are deemed to be adequate controls in this environment.

In summary regarding Finding 1, IT and PRMT have been taking aggressive steps to ensure that all hardware and software that are being used on WMATA's corporate network are properly purchased and used are in accordance with established standards and guidelines. As in all large organizations, compliance is never 100% complete and risk management evolves with the underlying technology and needs of the organization. IT will continue to improve upon these controls as described in this response and the prescriptive solutions proposed by the IG would undermine this effort, rather than enhance it.

Finding 2 – IT is Making Better Business Management Decisions In The Acquisition Of Software And Hardware, But Other WMATA Departments/Offices Are Not

Recommendation:
We recommend that the Deputy General Manager of Administration/Chief Financial Officer:

2.1 Direct the CIO to develop a P/I requiring all departments/offices within WMATA to coordinate acquisition and implementation of software and hardware projects with IT and follow IT's Portfolio Management and Business Plan Initiation Process or similar process for software and hardware acquisition and implementation.

Management Response:

IT agrees with Finding 2 as it relates to IT practices, but has no knowledge of the quality of project management outside of IT projects and therefore, no opinion. IT disagrees with Recommendation 2.1.

Recommendation 2.1
As previously noted, WMATA operates in a decentralized management model, making it difficult to impose standardized project management methodologies across all organizations. Where major IT corporate investments are being made, such as in Maximo upgrades, PeopleSoft (Finance and HCM), Safety Management System and major network upgrades, IT coordinates with other departments and the standard IT project/portfolio management methodologies

are deployed. This represents the bulk of the IT projects across the Authority in terms of investment.

In the cases where IT is involved peripherally with a project and not the principle sponsor (like the Shepherd Parkway Bus Garage, the Clever Device bus on-board equipment project or the Security Grant Camera Program), IT imposes a standard methodology, but just for the IT portion of the project that touches the corporate network.

There are also many "IT-like" projects throughout the Authority that are not managed by IT, but pose no risk to the corporate network, because they don't touch it, (like Rail automation projects, building security/alarming, fire protection systems, etc.). Many of these projects are not even visible to IT and are managed independently by the Bus and Rail engineering organizations. IT has no opinion or knowledge of the management practices imposed over these projects.

In summary, all IT projects that touch the corporate network are managed using IT-established project and portfolio management strategies to reduce programmatic risk. However, there are many "IT-like" projects around the authority managed outside of this framework, but these projects do not pose risk to the corporate network, since they are closed systems.

Each organization needs to develop its own methodologies to manage projects and reduce risk. They do not necessarily have to all use the methodologies developed by IT, but these could serve as a template for the development of their own processes if required. IT has made its portfolio management and business plan initiation process available to all WMATA.

OTHER MATTERS OF CONCERN

Recommendation:
We recommend that the Deputy General Manager of Administration/Chief Financial Officer:

3.1 Direct the CIO to implement procedures and controls to verify hard drives are adequately wiped before surplussing and to periodically test the data removal process to ensure compliance.

3.2 Direct the CIO to make the Microsoft Enterprise discount program for the Microsoft Office suite known to all eligible WMATA employees.

3.3 Direct the CIO to develop and implement controls to ensure IT equipment

and computer accessories purchased are distributed and/or deployed in a timely manner.

Management Response:

3.1 **IT agrees with recommendation 3.1 and has already implemented a solution to address this recommendation as indicated in the report.** .

Recommendation 3.1 directs the CIO to implement procedures and controls to verify hard drives are adequately wiped before surplussing and to periodically test the data removal process to ensure compliance. IT P/I 15.12 "Data Sensitivity" established and provides guidance on proper deletion and/or destruction of media prior to media (hard drives, USBs, DVDs) disposal. Additionally, IT acquired industrial strength deqaussers for use in destroying hard drives prior to disposal. The media are tested to verify that they are unreadable and unrecoverable.

3.2 **IT agrees with recommendation 3.2 which states that the CIO should make the Enterprise discount program for the Microsoft Office suite known to all eligible WMATA employees.**

IT will work with HR to publicize this in the employee discount section of the WMATA intranet.

3.3 **IT agrees with recommendation 3.3 and has implemented a solution to address this recommendation.**

Recommendation 3.3 states that the CIO should develop and implement controls to ensure IT equipment and computer accessories are distributed and/or deployed in a timely manner. As stated in the report, IT immediately deployed the items in its possession to various PC replacement projects. IT has also instituted a new procedure to ensure timely distribution of equipment. Any equipment that has been ordered and accepted after thirty (30) business days and has not been claimed by purchasing department after three (3) contact attempts, will be redeployed to other business units that have a need for the equipment.