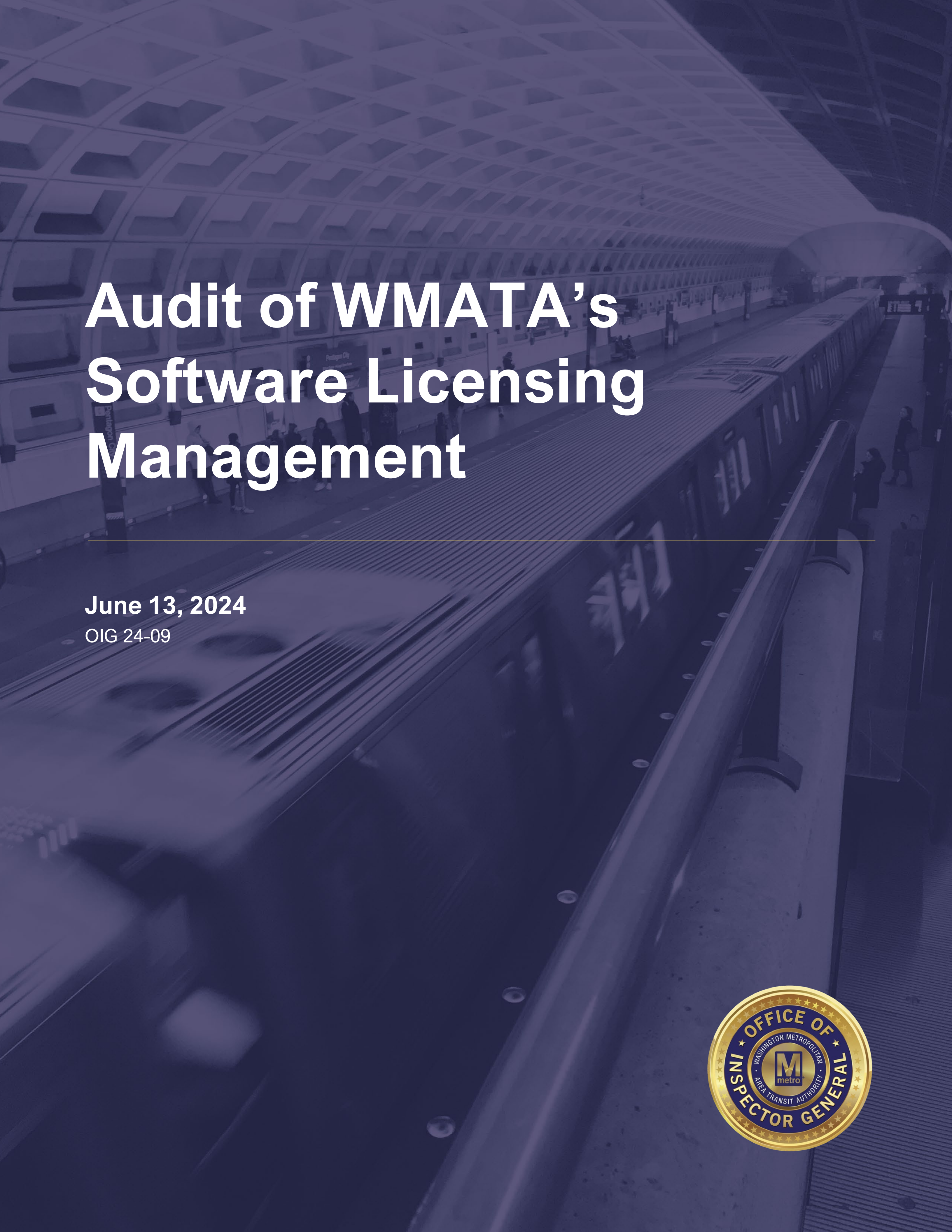


Audit of WMATA’s Software Licensing Management

June 13, 2024

OIG 24-09

Executive Summary

Audit of WMATA's Software Licensing Management

June 13, 2024
OIG 24-09

Introduction

Washington Metropolitan Area Transit Authority's (WMATA) Digital Modernization (DM) is responsible for the digital transformation and continual modernization of WMATA's technological infrastructure. This infrastructure supports WMATA's operations, enabling the organization to provide safer, more reliable service to its customers and a collaborative work environment for WMATA's employees. DM manages all of WMATA's digital assets, including software.[1]

Objective

Determine whether DM has established adequate controls to manage WMATA's software licenses.

Findings

OIG found that DM can improve its management of software licensing and assets by strengthening controls in the following areas:

- Software licensing optimization and utilization management,
- Software lifecycle tracking, and
- Monitoring and detecting software and hardware purchases made with WMATA purchase cards.

These control weaknesses limit DM's ability to effectively and efficiently account for, monitor, and manage software and software license costs, utilization, and optimization. These weaknesses could result in non-compliance with software contract terms, unnecessary expenditures, and increased exposure to cybersecurity vulnerabilities.

Perspective

DM's software management outlook appears promising as the newly appointed Chief Digital Officer recognizes the necessity of centralizing financial control over software assets. This recognition reflects an initiative to optimize resources and reinforce fundamental program policies. DM stated an enterprise software license project is underway. The goal is to grant employees appropriate access to technology and applications. Also, software management provides DM with the necessary visibility and

[1] *WMATA'S Cybersecurity Policy Manual, Version 1.1*, dated August 9. 2022, Policy Instruction 15.28/0, section 2.02 provides " . . . includes information technology, operational technology, communication technology, and Internet of Things (IoT), as managed through all forms of hardware, software, and firmware owned or operated within Metro."

controls to effectively manage software cost, utilization, and optimization of assets. However, a definite timeline has yet to be set to complete this project.

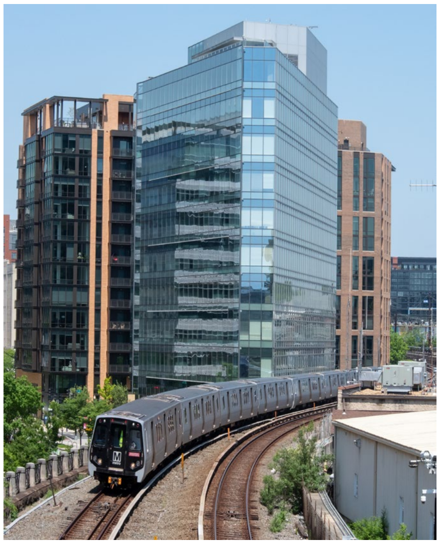


Table of Contents

Background

What is Digital Modernization (DM) - DM is led by the Chief Digital Officer (CDO). DM supports WMATA's strategic goals of safety, reliability, talented teams, and operational efficiency by providing information technology services, strategic planning, continual improvement, and decision support services. Policy Instruction 15.25/1, section 4.01(k) states the Chief Digital Officer is responsible for "establishing ownership and responsibility for the proper operation and cybersecurity of all enterprise-wide technology assets...." This responsibility includes the management of one particular "technology asset," software, and its respective lifecycle.[2]

Cost of Software and Maintenance Services - According to DM, for FY 2023, WMATA spent approximately $30 million on software and service maintenance contracts, anticipates spending $47.7 million in FY 2024, and anticipates spending $57.1 million in FY 2025 (*refer to Table 1*).

Table 1. Software and Software Maintenance Contracts: Actual Costs and Projected Costs

Category	FY 2023	Original FY 2024	Current FY 2024	FY 2025
Services Service Contracts (Software Maintenance)	$29,174,597	$32,540,098	$46,989,018	$56,432,715
Software Cost	$699,499	$349,963	$706,388	$672,801
TOTALS	**$29,874,096**	**$32,890,060**	**$47,695,406**	**$57,105,516**

According to DM's data, from FY 2023 to FY 2025, software service contract costs are projected to increase by 93.4 percent. However, software costs are expected to decrease by 3.8 percent.

WMATA's 2023 Financial Statements Audit - In November 2023, OIG issued the *Audit of WMATA's Financial Statements for Fiscal Years 2022 and 2023*. The report states:

> The Authority adopted the provisions of Governmental Accounting Standards Board Statement No. 96 (GASB 96), Subscription-Based Information Technology Arrangements, which provides guidance on the accounting and financial reporting for subscription-based

[2] Information Systems Audit and Control Association (ISACA) provides "Software life cycle - Period of time, beginning when a software product is conceived and ending when the product is no longer available for use. The software life cycle is typically broken into phases, denoting activities, such as requirements, design, programming, testing, installation, operation and maintenance. It contrasts with software development process." https://www.isaca.org/resources/glossary#glossl

"As a globally recognized leader in IS/IT for over 50 years, ISACA is a professional membership organization committed to the advancement of digital trust by empowering IS/IT professionals to grow their skills and knowledge in audit, cybersecurity, emerging tech and more." https://www.isaca.org/about-us

> information technology arrangements (SBITAs) for governments.[3] As a result of the GASB 96 implementation, total assets and total liabilities as of June 30, 2022, increased by $20.6 million and $19.9 million, respectively.

As of December 2023, WMATA has 63 SBITAs totaling $45.6 million.

Prior Reports

Audit of WMATA's Software Asset Management Program (SAM) - In June 2019, OIG issued its *Audit of WMATA's Software Asset Management Program* (SAM). The audit report stated:

> WMATA has not implemented a comprehensive SAM Program capable of managing software assets across the enterprise. WMATA developed some policies, informally assigned responsibilities, and conducted some scanning. However, other critical program requirements, including a software risk assessment, software resources, software inventory controls, detailed standard operating procedures, and quality assurance controls, were not implemented. The Information Technology (IT) Department did not have a comprehensive SAM program because they first needed to centralize financial control of IT assets, better align IT resources, and develop baseline program policies. A comprehensive SAM program would allow WMATA to fully manage software, and lessen WMATA's risks of exposure to cyberattacks, data breaches, and other exploits.

The prior OIG report found that WMATA had yet to implement a comprehensive SAM Program capable of providing managers the necessary information to make decisions about the lifecycle of software. Numerous actions need to take place to implement this program. To date, DM is still implementing a holistic Information Technology Asset Management (ITAM) Program to address the SAM-related issues identified by OIG.

[3] GASB 96 provides ". . .guidance on the accounting and financial reporting for SBITAs for government end users (governments)." A SBITA is defined as a contract that conveys control of the right to use another party's (a SBITA vendor's) information technology (IT) software, alone or in combination with tangible capital assets (the underlying IT assets), as specified in the contract for a period of time in an exchange or exchange-like transaction.

Finding 1: Lack of a Management Information System

Synopsis

DM does not have a centralized Management Information System (MIS) to manage software administration (technology).[4] DM has an outstanding Corrective Action Plan (CAP) for not having implemented an ITAM. DM has yet to implement an appropriate MIS or other technological infrastructure. DM's lack of an enterprise-wide software management system impacts (1) software planning, (2) operational efficiency, (3) IT safety and security, and (4) quality assurance/compliance activities. These impacts could result in excess spending, non-compliance with GASB 96, and increased cybersecurity exposures.

Condition

DM has yet to implement the appropriate MIS or other technological infrastructure capable of (1) collecting the relevant software lifecycle Key Performance Indicator (KPI) data and (2) reporting on software utilization/optimization. OIG made several observations that demonstrate the need for improvement in systems to manage software. Details of these observations are provided in the following paragraphs.

Software Management Observations - The following examples demonstrate the need for improvements in control of software and software service management and administration:

- To determine how DM managed software licenses, OIG requested basic software characteristic data from the Contracting Officer’s Technical Representative (COTR). For example, for Microsoft E3 and E5 licenses (versions E3 and E5), OIG requested (1) the number of licenses purchased, (2) the number of licenses issued, (3) billing provisions, and (4) the respective contracts.[5] The responsible COTR stated that OIG should contact a manager in the DM Cybersecurity Department. Under the present system, this COTR is responsible for managing this information. However, the COTR could not readily provide the requested information for the E3 and E5 software. In a subsequent interview, the COTR stated he did not track optimization and utilization (*refer to Finding 2 of this report*).

[4] This finding addresses one (technology) of the three infrastructure requirements necessary to manage software licenses. The other two requirements, people and process, will be discussed in Finding 2 of this report.

[5] Microsoft offers several enterprise plans for 365. Each plan has different benefits over the others and delivers benefits to match the needs of users and organizations. Microsoft 365 E3 contains the Office productivity suite and core security solutions. An E5 license is more complete than E3, covering Office 365 Enterprise, Windows 10/11 Enterprise, and Enterprise Mobility + Security technologies.

- COTRs use Excel and other end-user systems to track software license data characteristics. However, DM had not assessed whether the internal controls, access controls, and other security controls were adequate. Consequently, DM cannot attest to the reliability of the data contained in these various systems. Further, while COTRs are provided instructions on how to perform COTR functions they stated DM had not provided them specific training on managing software licenses and tracking/reporting on optimization and utilization. More details of this finding are discussed in Finding 2 of this report.

- The Asset Management Division (AMD) in the Office of Accounting is responsible for reporting on GASB 96 requirements. To accomplish these requirements, the AMD reviews all software purchases and maintenance contracts to determine which software meets the GASB 96 requirements and should be reported. As WMATA policy and best practices require, DM should have an MIS containing a technology asset inventory, which includes software characteristics data. An AMD representative stated to OIG that, although DM is responsible, DM's software inventory record could not be relied upon.

  The AMD representative further stated to the OIG that they used DM's software inventory record as a starting point, not as the official and final software, software license, and software contract inventory record. The AMD representative stated that AMD staff must perform independent exercises to identify, verify, and validate the software license and lease information. Further, the AMD representative stated that they discovered differences between DM's inventory and AMD's inventory count.

  An AMD representative also stated to OIG that because DM is responsible for managing WMATA's technology resources, AMD should be able to rely on DM's software inventory record for GASB 96 reporting. Instead, DM's inability to account for the resources it manages results in the duplicate organizational (WMATA) efforts described above.

  In response to OIG's follow-up questions, DM stated, "[d]iscussions have been initiated regarding DM potentially taking over the responsibility of managing software assets and providing the list to OAA [Office of Asset Management] to comply with GASB 96. This is still in the higher levels of discussion."

The three examples above demonstrate DM's need for a centralized MIS to manage software throughout its lifecycle. In response to OIG's follow-up questions, DM concurred with OIG's observation, stating, "[n]o, the current management information system for managing and tracking software assets does not include all software assets across the enterprise. The current decentralized process has no oversight and/or governance, allowing asset management functions and duties to be left to the department's/system owners' discretion."

Also, in response to OIG's follow-up questions, DM stated:

> The as-is state is a decentralized approach to ITAM in which DM leverages a combination of tools to manage information system software assets. ITAM toolset comprises Microsoft's SCCM, ServiceNow Asset Manager (AM), ServiceNow CMDB, and ForeScout. Combined, the tools provide WMATA with the capabilities needed to effectively manage its complex infrastructure assets, ensure operational reliability throughout their lifecycle, from acquisition to disposal, and support the delivery of critical transit services to the public.

OIG found that these tools offer **some** capability. For example, DM stated that these tools currently did not extend to Operational Technology (OT) digital assets and had not been integrated with all the inputs and supporting infrastructure installed to make these systems a complete enterprise-wide solution to software asset management.[6] Accordingly, by DM's own admission, these tools do not extend to the entire enterprise. Also, these tools are not adequately structured, integrated, and implemented to manage the administration of **All** enterprise software.

CAP Responses - DM has an outstanding Corrective Action Plan (CAP) for not having an ITAM. A software lifecycle and license management system is a subset of an ITAM System. DM has proposed several corrective actions over the years. On February 9, 2024, the Executive Vice President and Chief Digital Officer provided the WMATA Board of Directors with a memorandum addressing open CAPs. In pertinent part, one of those CAPs involved IT Asset Management. The memo states:

> DM is resetting the approach to address all asset management-related corrective actions to allow the implementation of an industry-specific program that applies best practices. The organizational project will transition software, hardware, capital, and sensitive assets into the ServiceNow module. Organizational policies, procedures, and management directives will govern the DM Asset Management program. The CAP was extended in January 2024 with a due date of 12/31/2025.

[6] Information Technology Laboratory, Computer Security Resource Center provides OT is "[p]rogrammable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms." https://csrc.nist.gov/glossary/term/operational_technology

Before DM issued this memorandum, DM had informed OIG that "Archer" would be the new inventory system.[7] In response to a follow-up question, DM stated "ServiceNow AM is the primary solution to which all other ITAM solutions integrate with and aggregate data." The memorandum states DM has halted previous corrective actions, including implementation of Archer. Regardless, currently, WMATA is without an automated system until the newly identified corrective actions are implemented.

Criteria/Requirement

Critical asset control requires an organization to identify its assets first, enabling effective management. *WMATA's Cybersecurity Policy Manual, Version 1.1,* dated August 9, 2022**,** section 3.4.8a-c provides, "Develop and document an inventory of system components within the enterprise CMDB. . . ."[8] The Policy provides the requirement to, at a minimum, have a system. The policy also provides instructions for what data and characteristics should be captured. Conceivably, the system and software-related data would assist DM and program management in managing software and software maintenance services contracts.

Impact/Effect

DM's lack of an enterprise-wide software management system to manage software throughout its lifecycle can have major consequences for WMATA, such as:

(1) *Audit and License Noncompliance* – Failure to follow existing policy makes it more challenging for WMATA to determine whether the software is being used in compliance with contract and license terms.

(2) *Overspending* - The lack of understanding of software utilization makes it difficult for an organization to optimize software usage.

(3) *Security Risks* - The lack of a complete or accurate inventory could result in critical security patches and updates not being applied, leaving systems vulnerable to cyber exploits and attacks.

(4) *Operational Inefficiency* - Manual tracking systems are time-consuming, leading to inaccuracies and straining communication resources.

[7] Archer is a software solution that assists organizations to identify, assess, and monitor risks across the entire enterprise.

[8] A Configuration Management Database (CMDB) is - A database to store information about hardware and software assets (commonly referred to as Configuration Items [CI]), used to break down configuration items into logical layers. This database acts as a data warehouse for WMATA and also stores information regarding the relationships among its assets. The CMDB provides a means of understanding the organization's critical assets and their relationships, such as information systems, upstream sources or dependencies of assets, and the downstream targets of assets. (*WMATA's Cybersecurity Policy Manual, Version 1.1*)

(5) *Lack of Visibility* - WMATA's lack of full visibility into software assets makes it more difficult to identify cost-saving opportunities and plan for future needs.

An MIS can assist WMATA in mitigating these consequences.

Recommendation

OIG recommends the GM/CEO:

1. Implement an MIS that accurately and completely maintains software inventories and software data characteristics necessary to manage software through its lifecycle.

Finding 2: Lack of Software Licensing Optimization and Utilization Management

Synopsis

DM had not implemented a software lifecycle management infrastructure (people and process) capable of readily measuring software license optimization characteristics, utilization characteristics, and software lifecycle management KPIs. Key changes in DM's leadership, historical DM and OT management fragmentation, and changes in strategic vision have hindered implementation or requisite infrastructure. Consequently, WMATA cannot readily plan the software life cycle or readily make software utilization and optimization decisions.

Condition

Software and Software Maintenance Contract Management (process) - DM utilized COTRs to manage the software, software license, and software maintenance services contracts. However, DM had not formally outlined the required processes to manage software and software maintenance service contracts. DM's response to the OIG *Audit of WMATA's End-of-Service Life Operating System Software*, Corrective Action Plan, ID 625, dated December 9, 2023, outlined the process DM utilizes to manage software. DM's response stated the following:

> DM manages Software License which is tracked by Procurement, Finance, and the DM Software and System teams. In addition, the DM Finance team tracks Software Maintenance Contracts to ensure maintenance contracts are up to date. All Software is required to be approved by the DM Cybersecurity (DMCS) team before installation. The DMCS team has tools in place that successfully monitor, alarm, and track software usage. [9]

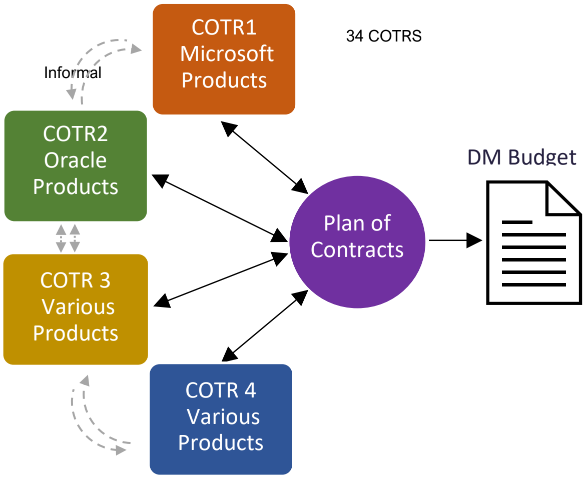
OIG asked DM who was responsible for managing enterprise software licenses and software optimization and utilization. DM responded with the name of one COTR and stated the person was responsible for software licenses. However, in another response, DM offered a conflicting response and stated, "[h]e is not responsible for the entire enterprise, but specifically for Digital Modernization Systems and Software." Also, DM stated, ". . . the current process [to manage software] does not encompass all software within the enterprise." DM's responses highlight that DM has not yet centralized the enterprise-wide administration of software license management. Further, DM had not established one person who ultimately had the responsibility and accountability for software license management.

[9] This section contains a direct quotation from a memorandum issued by management in response to OIG's report.

The COTR identified by DM informed OIG of several other COTRs who are also responsible for managing software and software maintenance service contracts. Further inquiry revealed that 34 COTRs were assigned to manage software and software service maintenance contracts for DM. None of these COTRs reported to a central software administrator.

DM clustered software and software maintenance services contract administration into logical and distinct groups and assigned a COTR to administer and manage the respective contracts within each group (*refer to Diagram 1*).

Diagram 1. Contractual Administration of Software Licenses



OIG spoke with three current and one former COTR who managed Microsoft, Oracle, or IBM product groups. These three product groups represent critical enterprise software and software maintenance service groups. The COTRs stated they only managed and reported on each software contract's contractual obligations. The three current COTRs stated they transmitted software and software maintenance contractual details, including costs, to the DM Office of Finance for budgetary purposes. This responsibility could entail coordinating with program and business owners to purchase additional licenses and, in some cases, removing licenses. However, these duties did not include, as a matter of policy or standard operating procedures (SOP), the development of KPIs, reporting, or tracking utilization and optimization. When these duties were performed, the duties were conducted randomly or on an ad-hoc basis.

This information was used to develop the "Plan of Contracts," which is vital in developing DM's annual budget.[10] However, this process is not a standard for managing the lifecycle of software and software maintenance contracts. At best, the "Plan of Contract" planning and development process would be a subset and part of a more extensive software management and administration program.[11]

The current software license management structure and processes are fragmented. This fragmentation hinders DM's ability to coordinate, communicate, and integrate the people, processes, and technologies required to manage software lifecycle and optimization.

Software Contract COTR Duties (people) - COTRs are responsible in part for managing licenses. The three current COTRs stated that the software contract COTR duty is a part-time assignment with full-time responsibilities. These COTRs stated these duties were not formal. They also stated that "software lifecycle management" is a discipline within itself and that the duties associated with managing the software lifecycle should be performed by full-time, trained, and experienced staff.

Even though *WMATA's Cybersecurity Policy Manual Version 1.1* provides guidance on what software attributes and characteristics should be captured at a minimum, the COTRs stated they had yet to be trained in tracking or managing software throughout its useful life or what attributes and characteristics should be tracked. OIG observed that COTRs used end-user computing methods like Excel to track software lifecycle attributes. DM had not conducted security and data integrity assessments of these end-user systems. Also, OIG found that the data characteristics gathered by each COTR varied. These conditions promote data integrity and quality issues, integration challenges, and reporting inconsistencies. Further, OIG found that when a new COTR was assigned to monitor a major software cluster of contracts, no training was provided on how to monitor, what to monitor, and other aspects of the "software asset management discipline."

OIG found that the COTRs had software contractual administration responsibilities. However, they lacked (1) the technical ability or responsibility to monitor the software utilization and

[10] The Plan of Contracts assists DM managers in understanding recurring and anticipated software and software maintenance costs at the yearly and multi-year levels.

[11] COBIT 5 provides a set of internationally accepted principles/guidelines that management can leverage to develop a well-rounded IT asset management program, including software license management. The general principles center on (1) policy development, (2) risk management, (3) resource management, (4) compliance/legal requirements, (5) monitoring and reporting, and (6) continuous improvement.

operation, (2) an automated means to monitor and track optimization and utilization, and (3) the capability to produce reports on crucial software lifecycle characteristics.

In response to an earlier OIG observation, DM, in an *Audit & Compliance, Corrective Action Plan (CAP) Extension Request*, dated December 8, 2023, CAP ID No. 625, stated that DMCS [DM Cybersecurity] can "…monitor, alarm, and track software usage." While that may be true, DMCS is a separate unit within DM and has no direct or formal reporting relationship with the COTRs. The COTRs are not responsible for coordinating or sharing information with other COTRs or DMCS. The software license contractual administration and software utilization/operational monitoring are decentralized, separate, and distinct functions. DM has not identified a communication approach between both groups. Finally, DMCS does not have visibility and scanning capability into all enterprise systems, as DM's response may imply.

Ultimately, DM validated OIG's observations in a follow-up response to OIG, which stated, "No, the current process does not encompass all software within the enterprise. The process is currently decentralized. DM groups are in the process of collecting an inventory of all software within the enterprise to create a baseline for all future dated ITAM project works."

Quality Control/Quality Assurance (process) - OIG inquired whether DM conducts software license audits as a quality control/quality assurance mechanism.[12] In a written response, DM stated, "[w]e do not conduct software license audits internally as we comply with the vendor's external audits." The OIG understood this to mean that DM relies on the vendor to validate how many licenses may be in use. This approach is more reactive than proactive. While DM informed OIG that it had conducted at least one inventory assessment of Oracle licenses, software optimization monitoring is a continual process and is required to align resource utilization with funding. This requirement is also found in *WMATA's Cybersecurity Policy Manual, Version 1.1,* dated August 9, 2022, section 3.4.8.a. This section requires DM to track software and hardware data characteristics to enable them to establish accountability and optimization of software and hardware inventories.

Criteria/Requirements

COBIT 5 2019, section BAI09.05, Manage Assets, Build, Acquire, and Implement, provides that an organization should "[m]anage software licenses so that the optimal number of licenses is

[12] Software license audits are a means an organization can use to determine whether (1) software meets business goals and needs, (2) software ownership and usage comply with license agreements, (3) software ownership and usage follow internal policies and procedures, and (4) software utilization is optimized. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/is-audit-basics-auditing-software-licenses?gad_source=1&gclid=Cj0KCQjwxeyxBhC7ARIsAC7dS3-JKxee6E9kHfv37PE6cdXLDtupEXDtAP3kFlsmszjeC3ssXC40XQYaAkNaEALw_wcB

maintained to support business requirements and the number of licenses owned is sufficient to cover the installed software in use."[13]

Additionally, COBIT 5 2019 section APO07.03 provides an organization should "[m]aintain the skills and competencies of personnel. Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles based on their education, training and/or experience, and verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals."

WMATA's Cybersecurity Policy Manual, Version 1.1, dated August 9, 2022, section 3.4.8.a.(v)(1)(a) & (b) provides, at a minimum, that data should be captured at a level of granularity to manage tracking and reporting on hardware, software, and firmware.

COBIT 5 and *WMATA's Cybersecurity Policy Manual, Version 1.1* require WMATA to implement the requisite infrastructure to ensure that (1) the optimal number of software licenses are acquired, maintained, and deployed, (2) suitable staff are retained and trained on how to manage software license administration, and (3) data characteristics collected by each COTR are consistent and reliable.

Causes

DM has experienced several critical changes in leadership and organizational structure, which affected its strategic direction/vision and operational continuity. Also, IT and OT management are still developing processes to communicate the information required to manage IT resources. Currently, the required structures have not been fully implemented.

Further, DM management and staff have agreed on the need for an ITAM program and pledged to implement it. However, DM has yet to formally implement a complete software management program that defines the people requirements (background, skills, and training), operational processes (policies and standard operating procedures), and technological solutions required to report on software assets lifecycle management, utilization, and optimization.

[13] COBIT 5: Is "[a] complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business and related IT goals. Formerly known as Control Objectives for Information and related Technology (COBIT)..." Found at https://www.isaca.org/resources/glossary#glossl

Impact/Effect

The following example illustrates a consequence of not implementing the appropriate infrastructure to manage software optimization and utilization.

According to DM, for the period August 1, 2023, to July 31, 2024, WMATA purchased approximately 20,460[14] Microsoft E3 and E5 license subscriptions (*refer to Table 2*). WMATA has approximately 12,675 employees. However, only 8,100 E3 or E5 licenses have been issued. Potentially, WMATA has 12,360 excess licenses. OIG could not attribute unit pricing or cost to the potential 12,360 excess licenses because DM could not provide OIG with a detailed breakdown of the E3 and E5 categories for the excess licenses.[15]

Table 2. Microsoft 365 Enterprise Licensing Agreements for E3 and E5 Licenses

Version No.	Licenses Purchased	Total Cost	Licenses Issued	Excess Licenses
E3	12,355	$2,670,326	7,750	4,605
E5	8,105	$1,822,592	350	7,755
Totals	**20,460**	**$4,492,918**	**8,100**	**12,360**

WMATA has purchased 12,355 enterprise version 3 (E3) licenses for $2.6 million and 8,105 enterprise version 5 (E5) licenses for $1.8 million. Of the 12,335 licenses purchased for version E3, only 7,750 have been issued; of the 8,105 licenses purchased for version E5, only 350 have been issued. When OIG asked the COTR responsible for managing the Microsoft contracts why there were so many E3 and E5 licenses, the COTR could not provide an explanation. OIG contacted DM a second time to confirm the breakdown numbers for each category, but DM was still unable to validate or confirm the purchases, issuance, or excess numbers of E3 and E5 licenses.

Also, there is no defined requirement to purchase E5 licenses instead of E3 or to upgrade from E3 to E5 licenses. E5 licenses offer more enhanced security functions than E3 and other functionality enhancements. OIG asked DM representatives why DM had not upgraded from E3 to E5, and DM did not provide a response.

[14] DM provided this number of E3 and E5 licenses purchased.

[15] According to DM, there are four E3 and three E5 categories, with each category having a different unit price.

Recommendations

OIG recommends the GM/CEO:

2. Develop and implement the requisite infrastructure of people and processes, according to best practices, to manage software license optimization and utilization.

3. Develop and implement a program to provide initial and refresher training to those responsible for managing software licensing. This program should cover essential areas, including (1) policy standards, (2) software and software contract administration requirements, and (3) best practices encompassing key aspects of software management such as data recording, communication, coordination, monitoring, and reporting.

Finding 3: Lack of Internal Controls Over IT Purchases Made with a Purchase Card

Synopsis

Software and IT equipment can be purchased with a purchase card without approval or authorization from DM, which is a violation of WMATA policies. DM has not implemented adequate controls to prevent or detect software and IT hardware purchases made with a purchase card. These conditions increase WMATA's exposure to software incompatibility, cybersecurity threats, and other vulnerabilities.

Condition

DM informed OIG the WMATA IT Hardware and Software Fulfillment Center (ITHSFC) should authorize and/or procure all IT hardware and software purchases. However, the Office of Procurement and Materials (Procurement) informed OIG that digital assets, such as software, IT hardware, and IT maintenance services, can be procured with a purchase card without DM's approval.

Table 3 shows software, hardware, and IT maintenance services procured using a purchase card for FY 2019 - FY 2023. These purchases totaled 200 transactions and approximately $371,254 over five years. While the monetary value may be low and, in some cases, immaterial, the lack of accountability could lead to software incompatibility or a potential security breach.

Table 3. Software/Hardware P-Card Transactions (Excluding DM and OIG cardholders)

Year	5045 Computers and Computer Peripheral Equipment and Software	5734 Computer Software Stores	5817 Digital Goods – Applications (Excludes Games)	7372 Computer Programming, Data Processing, and Integrated Systems Design Services	7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)	Total Amount	Transactions Per Year
2019	$45,275	$7,710	-	$4,294	$6,835	$64,114	41
2020	$41,840	$26,636	-	$25,965	-	$94,440	27
2021	$38,486	$9,401	-	$23,783	$1,154	$72,823	40
2022	$33,163	$21,952	$499	$21,364	$13,319	$90,297	53
2023	$16,313	$6,250	-	$16,557	$10,460	$49,580	39
Grand Total	**$175,076**	**$71,948**	**$499**	**$91,963**	**$31,768**	**$371,254**	**200**

OIG reviewed 17 of 39 purchase card transactions for FY 2023 that had Merchant Category Codes (MCC) representing IT-related classifications, such as the following:

- 5045 Computers and Computer Peripheral Equipment and Software
- 5734 Computer Software Stores
- 5817 Digital Goods – Applications (Excludes Games)
- 7372 Computer Programming, Data Processing, and Integrated Systems Design Services
- 7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)

Of the 17 transactions the OIG examined, OIG determined that one of the purchases was for software, and the remaining 16 were computer hardware, subscription services, peripheral equipment, and maintenance services (refer to Appendix B). The one software purchase was for one license and totaled $1,863. While some purchases may be miscoded to IT-related MCC's, because IT purchases can be made utilizing the purchase card, OIG's testing demonstrated the likelihood that IT-related purchase card transactions can occur without DM's knowledge and scrutiny and remain undetected.

Criteria/Requirement

Policy Instructions (P/Is) state that DM is responsible for approving all IT-related purchases. In part, P/I *15.20/4 Procurement of Administration IT Hardware and Software,* section 5.00 provides*:*

5.01 IT has the sole authority to approve the purchase of all IT hardware and software within the scope of this policy. The procedures used to procure IT hardware and software are in the fulfillment of requests for IT hardware and software SOP).[16]

5.02 IT has the sole authority to submit purchase requisitions for IT hardware and software within the scope of this policy.

P/I *8.11/6 Purchase Card Policy,* section 5.15, Prohibited Use of Card provides:

> (a) Unauthorized use of purchase cards occurs when a purchase is made or is used in violation of this policy. Metro is liable for unauthorized use of purchase cards unless reported and disputed with the financial institution. The purchase card shall not be used for: (11) IT equipment, systems, accessories, and services (i.e.). (xiii) software (network application and operating system).

[16] All Policies Instructions have not been updated to reflect IT's designation as DM.

Cause

DM has developed P/Is and SOPs for its own staff when making IT purchases utilizing purchase cards. However, DM had not implemented internal controls, quality controls, or quality assurance programs to prevent or detect purchase card procurements of IT-related equipment made by departments outside of DM. While Procurement and Audit & Compliance perform quality assurance reviews of purchase card purchases, these reviews are conducted post purchase card procurement.

Impact/Effect

Purchase card holders are not restricted from making purchases under IT-related MCC codes. Consequently, DM would not notice these purchases as they were not submitted for approval. Allowing unapproved software or IT hardware into WMATA's network and IT environment could pose potential security, legal, and compliance issues. These issues could increase WMATA's exposure to legal ramifications, cybersecurity threats, and other vulnerabilities.

Recommendations

OIG recommends the GM/CEO:

4. Develop and implement a robust quality assurance system to strengthen the existing process for monitoring and reviewing purchase card transactions specifically related to IT and IT-related procurements.
5. Collaborate with the purchase card issuer to implement and enhance alerts and controls to detect and prevent unauthorized IT and IT-related procurements.

Recommendation Summary

OIG recommends the GM/CEO implement the following recommendations to address the findings identified above and to strengthen the program and operations:

1. Implement an MIS that accurately and completely maintains software inventories and software data characteristics necessary to manage software through its lifecycle.
2. Develop and implement the requisite infrastructure of people and processes, according to best practices, to manage software license optimization and utilization.
3. Develop and implement a program to provide initial and refresher training to those responsible for managing software licensing. This program should cover essential areas, including (1) policy standards, (2) software and software contract administration requirements, and (3) best practices encompassing key aspects of software management such as data recording, communication, coordination, monitoring, and reporting.
4. Develop and implement a robust quality assurance system to strengthen the existing process for monitoring and reviewing purchase card transactions specifically related to IT and IT-related procurements.
5. Collaborate with the purchase card issuer to implement and enhance alerts and controls to detect and prevent unauthorized IT and IT-related procurements.

Summary of Management's Response

WMATA's Executive Vice President (EVP)/Chief Digital Officer (CDO) provided written comments to the report on June 3, 2024 (Appendix C). The EVP/CDO concurred with all the findings and recommendations. The EVP/CDO has initiated corrective measures for the recommendations made in this report. OIG considers management's comments responsive to the recommendations, and the actions taken or planned should correct the deficiencies identified in the report. OIG will follow up during the Corrective Action Plan process to ensure action is taken on the recommendations.

Scope

The scope of the audit included a review of current enterprise-wide software and associated licenses. The review included credit card transactions for FY 2023.

Methodology

To achieve the audit objective, OIG's audit methodology is provided in the following bullets.

- Reviewed and documented the organizational infrastructure responsible for the management and administration of the software license management.
- Reviewed relevant laws, regulations, policies, and procedures, as well as best practices and guidance, such as WMATA Policy Instructions, Accounting Policies and Procedures, and Standard Operating Procedures.
- Reviewed prior audits conducted by other OIG, Audit and Compliance, General Accountability Office, Federal Transit Administration, and other organizations.
- Reviewed relevant management recommendations, comments, and corrective actions.
- Conducted interviews with responsible management and staff.
- Conducted walkthroughs of relevant processes, operations, and practices to become familiar with administrative, operational, and management processes.
- Identified and documented relevant internal controls over software asset management.
- Identified a 5-year universe of purchase cards coded to IT-related MCC codes. Sampled IT-related procurements made in FY2023.

Generally Accepted Government Auditing Standards (GAGAS) Statement

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

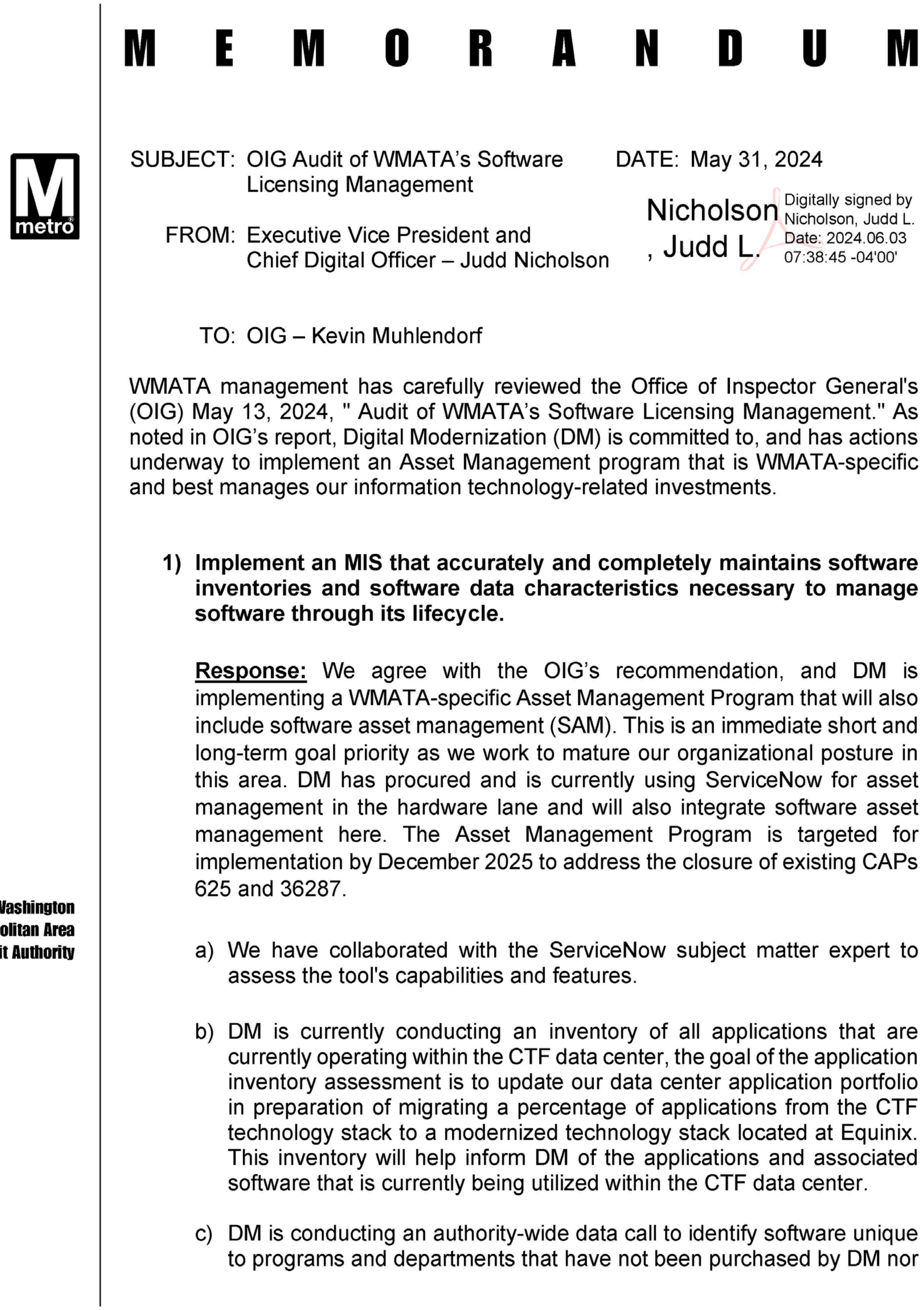
Appendix B: Table - IT-Related Purchase Card Transactions

Table 3. IT-Related Purchase Card Transactions (FY 2023)

No.	Transaction ID	Transaction Date	Merchant Name	Merchant Category Code (MCC)	Billing Amount
1	1552774262	7/31/2023	IN *INTEGRATED SECURITY T	7372 Computer Programming, Data Processing, and Integrated Systems Design Services	$1,005.00
2	1493189879	1/25/2023	SP TOTALELEMENT	5734 Computer Software Stores	$1,119.30
3	1545995714	7/11/2023	SP FALCON TECH ONLIN	5045 Computers and Computer Peripheral Equipment and Software	$1,193.67
4	1491391339	1/19/2023	SHOW ME CABLES	5045 Computers and Computer Peripheral Equipment and Software	$1,355.69
5	1560298544	8/28/2023	SP SWEEPSCRUB.COM	5734 Computer Software Stores	$1,659.55
6	1488473022	1/6/2023	SQ *Z IT SOLUTIONS	7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)	$1,680.00
7	**1525006361**	**5/6/2023**	**MICROSURVEY**	**5045 Computers and Computer Peripheral Equipment and Software**	**$1,863.00**
8	1545285076	7/7/2023	NCC GROUP SOFTWARE RESILI	7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)	$2,215.00
9	1546358810	7/12/2023	TEAM ONE REPAIR INC	5045 Computers and Computer Peripheral Equipment and Software	$2,250.00
10	1525567030	5/9/2023	SP PRIMELEC	5734 Computer Software Stores	$2,427.32
11	1488473023	1/6/2023	SQ *Z IT SOLUTIONS	7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)	$2,500.00
12	1516162702	4/11/2023	IN *INTEGRATED SECURITY T	7372 Computer Programming, Data Processing, and Integrated Systems Design Services	$2,700.00
13	1542829982	6/28/2023	SQ *Z IT SOLUTIONS	7379 Computer Maintenance, Repair and Services (Not Elsewhere Classified)	$3,280.00
14	1527345750	5/12/2023	CARAHSOFT TECHNOLOGY CORP	5045 Computers and Computer Peripheral Equipment and Software	$3,360.00
15	1520613290	4/25/2023	IN *DEWESOFT LLC	5045 Computers and Computer Peripheral Equipment and Software	$3,605.00
16	1516162703	4/11/2023	IN *INTEGRATED SECURITY T	7372 Computer Programming, Data Processing, and Integrated Systems Design Services	$4,812.50
17	1496473282	2/3/2023	IN *INTEGRATED SECURITY T	7372 Computer Programming, Data Processing, and Integrated Systems Design Services	$4,932.50
TOTAL					**$41,958.53**

**Red highlight indicates software purchase*

Management's Response



MEMORANDUM

SUBJECT: OIG Audit of WMATA's Software Licensing Management

DATE: May 31, 2024

FROM: Executive Vice President and Chief Digital Officer – Judd Nicholson

Nicholson , Judd L.

Digitally signed by Nicholson, Judd L.
Date: 2024.06.03
07:38:45 -04'00'

TO: OIG – Kevin Muhlendorf

Washington
Metropolitan Area
Transit Authority

WMATA management has carefully reviewed the Office of Inspector General's (OIG) May 13, 2024, " Audit of WMATA's Software Licensing Management." As noted in OIG's report, Digital Modernization (DM) is committed to, and has actions underway to implement an Asset Management program that is WMATA-specific and best manages our information technology-related investments.

1) **Implement an MIS that accurately and completely maintains software inventories and software data characteristics necessary to manage software through its lifecycle.**

   Response: We agree with the OIG's recommendation, and DM is implementing a WMATA-specific Asset Management Program that will also include software asset management (SAM). This is an immediate short and long-term goal priority as we work to mature our organizational posture in this area. DM has procured and is currently using ServiceNow for asset management in the hardware lane and will also integrate software asset management here. The Asset Management Program is targeted for implementation by December 2025 to address the closure of existing CAPs 625 and 36287.

   a) We have collaborated with the ServiceNow subject matter expert to assess the tool's capabilities and features.

   b) DM is currently conducting an inventory of all applications that are currently operating within the CTF data center, the goal of the application inventory assessment is to update our data center application portfolio in preparation of migrating a percentage of applications from the CTF technology stack to a modernized technology stack located at Equinix. This inventory will help inform DM of the applications and associated software that is currently being utilized within the CTF data center.

   c) DM is conducting an authority-wide data call to identify software unique to programs and departments that have not been purchased by DM nor are part of the suite of enterprise tools that DM provides.

d) Using existing scanning tools to identify software deployed on WMATA devices and the WMATA's network, DM will attempt to identify software in use that is not hosted in DM-managed data centers or servers.

e) DM's senior leadership, in cooperation with PRMT, is preparing a memorandum for Authority-wide distribution regarding the purchase of software. The memorandum will specify the required review of DM before acquisition to ensure purchases are not duplicative. This memorandum will be distributed before 6/30/25.

f) DM is currently exploring a best practice approach to eliminate the current gaps of recapturing software licenses for staff/contractors at the point of offboarding.

g) DM is currently defining the required attributes necessary for effective inventory lifecycle management via a proposed Asset Management Task Force in concert with the ask for CAP-36404 Mission Critical Systems.

h) The above actions align with DM's revised approach to software acquisition to reduce cost, waste, and redundancy in software and licensing management.

2) **Develop and implement the requisite infrastructure of people and processes, according to best practices, to manage software license optimization and utilization.**

Response: We agree with the OIG's recommendation, and DM will be reconstituting and chartering its Asset Management Task Force to drive the implementation of an Asset Management program. The task force will provide recommendations for strategic planning, policy development, and execution of best practices to optimize asset performance and value.

a) As stated in response to recommendation one, the actions denoted previously support and require the institution of best practices and program governance for an effective SAM program. These actions will be foundational in the organizational development of our policies, standard operating procedures (SOP), processes, and work instructions. Core staff have been identified as integral to the success of the SAM program's management.

b) DM will be developing an Asset Management Governance model and framework. The governance model will seek to address the following elements: **1)** compliance, **2)** cost optimization, **3)** risk management, **4)** asset lifecycle management, **5)** vendor management, **6)** alignment with business objectives, and **7)** continuous process improvement.

3) **Develop and implement a program to provide initial and refresher training to those responsible for managing software licensing. This program should cover essential areas, including (1) policy standards, (2) software and software contract administration requirements, and (3) best practices encompassing key aspects of software management such as data recording, communication, coordination, monitoring, and reporting.**

Response: We concur with the OIG's recommendation, and DM will take the following actions to align with the implementation of ServiceNow.

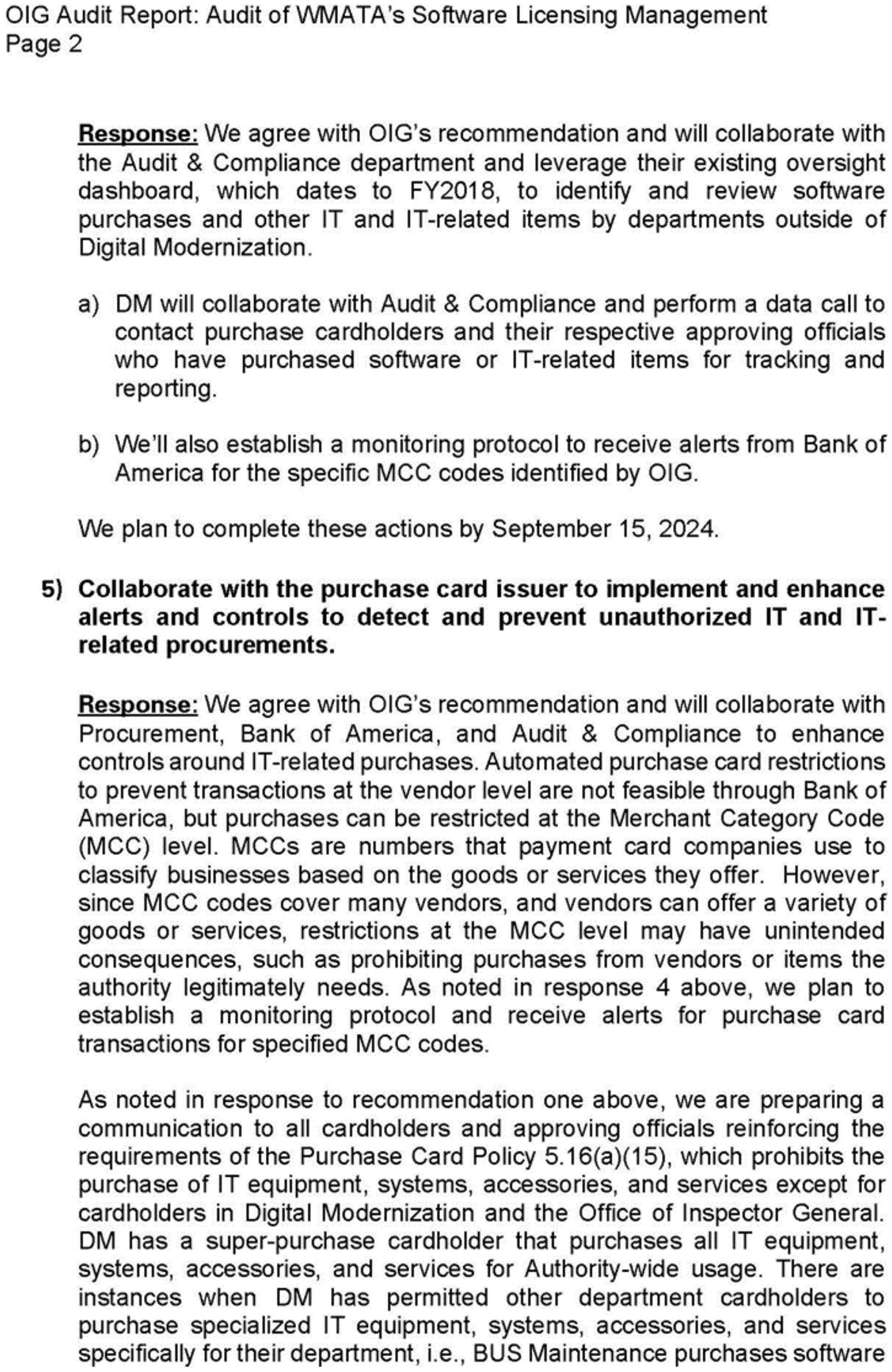
a) By identifying ServiceNow as the asset management tool of choice for DM, we will develop a training plan to support the requests the OIG requires in this finding. The training plan will be developed following the tool's implementation in December 2025.

b) DM will develop an agency-wide policy instruction that will govern how DM directs the ongoing management of Software Asset Management and a Standard Operating Procedure that will direct how DM will execute the necessary functions to manage the SAM efforts internally. This document will detail the roles and responsibilities within the DM organization, adapting to the recent organizational and structural changes. It will incorporate the Asset Management Governance Model that was previously mentioned. These governance activities will be aligned with the OIG's asks.

c) We will investigate training opportunities in partnership with Talent Management and Procurement.

d) DM will discern the feasibility of annual training for our stakeholders responsible for managing licensing within WMATA.

4) **Develop and implement a robust quality assurance system to strengthen the existing process for monitoring and reviewing purchase card transactions specifically related to IT and IT-related procurements.**



<u>**Response:**</u> We agree with OIG's recommendation and will collaborate with the Audit & Compliance department and leverage their existing oversight dashboard, which dates to FY2018, to identify and review software purchases and other IT and IT-related items by departments outside of Digital Modernization.

a) DM will collaborate with Audit & Compliance and perform a data call to contact purchase cardholders and their respective approving officials who have purchased software or IT-related items for tracking and reporting.

b) We'll also establish a monitoring protocol to receive alerts from Bank of America for the specific MCC codes identified by OIG.

We plan to complete these actions by September 15, 2024.

5) Collaborate with the purchase card issuer to implement and enhance alerts and controls to detect and prevent unauthorized IT and IT-related procurements.

<u>**Response:**</u> We agree with OIG's recommendation and will collaborate with Procurement, Bank of America, and Audit & Compliance to enhance controls around IT-related purchases. Automated purchase card restrictions to prevent transactions at the vendor level are not feasible through Bank of America, but purchases can be restricted at the Merchant Category Code (MCC) level. MCCs are numbers that payment card companies use to classify businesses based on the goods or services they offer. However, since MCC codes cover many vendors, and vendors can offer a variety of goods or services, restrictions at the MCC level may have unintended consequences, such as prohibiting purchases from vendors or items the authority legitimately needs. As noted in response 4 above, we plan to establish a monitoring protocol and receive alerts for purchase card transactions for specified MCC codes.

As noted in response to recommendation one above, we are preparing a communication to all cardholders and approving officials reinforcing the requirements of the Purchase Card Policy 5.16(a)(15), which prohibits the purchase of IT equipment, systems, accessories, and services except for cardholders in Digital Modernization and the Office of Inspector General. DM has a super-purchase cardholder that purchases all IT equipment, systems, accessories, and services for Authority-wide usage. There are instances when DM has permitted other department cardholders to purchase specialized IT equipment, systems, accessories, and services specifically for their department, i.e., BUS Maintenance purchases software

OIG Audit Report: Audit of WMATA's Software Licensing Management
Page 2

to diagnose the buses, and the vendor is responsible for the maintenance. DM will reexamine this practice in consultation with PRMT.

Attachment

cc: Senior Executive Team
VP & Chief Risk and Audit Officer - Elizabeth Sullivan

Report Fraud, Waste, or Abuse

Please Contact:

Email:	hotline@wmataoig.gov
Website:	wmataoig.gov/hotline-form/
Telephone:	1-888-234-2374
Facsimile:	1-800-867-0649
Address:	WMATA Office of Inspector General Hotline Program 500 L’Enfant Plaza SW, Suite 800 Washington D.C., 20024