



Results in Brief

OIG 22-01
August 24, 2021

Audit of WMATA's Mission Critical Legacy Systems

Why We Did This

Review

The Department of Information Technology (IT) provides information technology and telecommunication support services to support WMATA's strategic goals and operations.

The Metro – IT Strategic Plan, FY 2019 to 2024, dated July 2018 (Plan) provides strategic direction for IT. The Plan focuses on defining WMATA's over-arching goals and establishes the technology direction for the enterprise. The Plan provides the primary goal for IT is to ensure that information assets and resources are acquired, managed, and monitored in a manner consistent with the information needs of the enterprise in compliance with statutory and regulatory requirements.

WMATA identified 420 systems and has categorized these systems based on mission criticality and need for continuity of service.

The audit objective was to determine whether WMATA developed plans for modernizing or replacing legacy systems and the adequacy of the modernization plans.

What We Found

Washington Metropolitan Area Transit Authority (WMATA) had not developed or has incomplete modernization plans for six mission critical systems OIG sampled. These systems include [REDACTED]

[REDACTED] IT management stated this condition was inhibited by unexpected events (e.g., COVID 19 and the Jackson Graham Building (JGB) fire) coupled with a reactive replacement process and resource challenges. IT management also stated they are in the process of, but had not completed, developing a comprehensive system modernization program.

The absence of modernization plans could impact WMATA's ability to effectively and efficiently operate and meet system and mission requirements. The absence of plans: (1) makes system integration and scalability more difficult; (2) contributes to the potential for system crashes; (3) increases the possibility for data breaches or loss; (4) may adversely impact system performance; and (5) increases WMATA's exposure to loss of IT product technical support. Effective modernization plans provide a proactive and planned approach to managing WMATA's aging IT infrastructure. Without this approach, WMATA could (1) become dependent on costly maintenance contractors, (2) be forced to rely on temporary and short-term fixes, and (3) lose support services for IT products that are not timely updated or replaced.

Management's Response

WMATA's Executive Vice President and Chief of Internal Business Operations (EVP/CIBO) provided written comments, dated August 23, 2021 (Appendix B). The EVP/CIBO fully concurred with the finding and recommendations to be completed by December 31, 2023. OIG considers management's comments responsive to the recommendations and the actions taken or planned should correct the deficiencies identified in the report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS 2

BACKGROUND 3

AUDIT OBJECTIVE AND RESULTS 6

 Finding – Absent or Incomplete Modernization Plans for Mission Critical Systems.....6

SUMMARY OF MANAGEMENT’S RESPONSE..... 10

APPENDICES

- A. Objective, Scope, and Methodology
- B. Management’s Response
- C. List of Mission Critical Systems

ABBREVIATIONS AND ACRONYMS

ABBREVIATION	DESCRIPTION
EVP-IBOP	Executive Vice President of Internal Business Operations
JGB	Jackson Graham Building
PLM	Project Lifecycle Management
SAM	Software Asset Management

BACKGROUND

A member of WMATA's management team expressed concerns with WMATA's efforts to address aging IT systems. Management inquired whether plans had been developed to modernize those systems. OIG conducted this audit in response to that inquiry.

A legacy system is sometimes defined as an IT system that is aging, outdated, or obsolete.¹ Gartner defines a legacy application or system as:

“An information system that may be based on outdated technologies, but is critical to day-to-day operations. Replacing legacy applications and systems with systems based on new and different technologies is one of the information systems (IS) professional's most significant challenges. As enterprises upgrade or change their technologies, they must ensure compatibility with old systems and data formats that are still in use.”²

The IT Department management had not defined the term “legacy system.” IT management acknowledges that WMATA has aged applications and systems. IT management further stated that, even though those systems are aged, they are not obsolete and are fully operational as well as fulfill WMATA requirements. Those systems will remain operational until associated infrastructure issues are addressed.

A mission critical system is a system that is vital to enterprise operations. WMATA has 420 systems ranked according to mission³ criticality and availability. WMATA has classified 21 of 420 systems as mission critical systems (see Appendix C). WMATA spends an estimated \$28 million annually to maintain the 420 systems.

A 2019 GAO report concluded that federal agencies have historically had difficulties in acquiring, developing, and managing their IT investments.⁴ In addition, federal agencies have struggled with appropriately planning and budgeting for the modernization of their legacy systems. Agencies also had issues with upgrading their infrastructure and investing in high-quality cost-effective technology. The GAO report outlines best practices when planning the management of legacy systems. These best practices, if adopted, could benefit WMATA.

The *Metro - IT Strategic Plan, FY 2019 to 2024*, dated July 2018 focuses on high-level goals and sets a broad technology direction for the enterprise. The Plan's primary goal is to ensure that information assets and resources are acquired, managed, and monitored in a manner consistent with statutory and regulatory requirements. However, a strategic plan is not a modernization plan as outlined in the GAO report.

¹ The Modernizing Government Technology (MGT) Act defines a legacy IT system as a system that is outdated or obsolete. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G (2017).

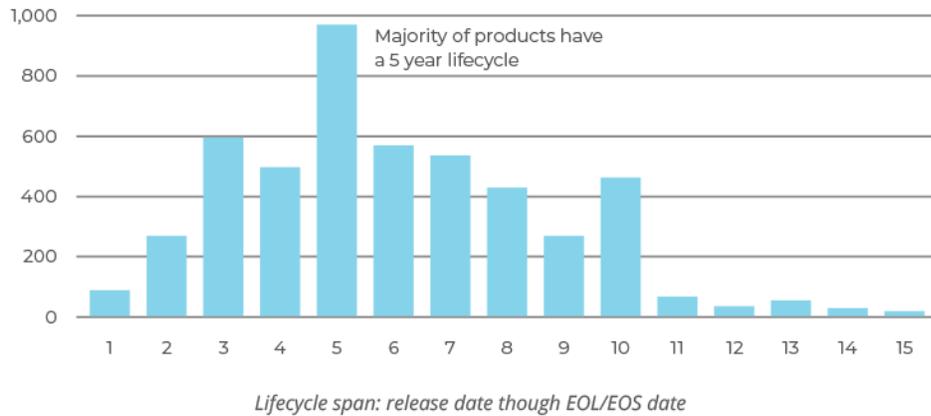
² <https://www.gartner.com/en/information-technology/glossary/legacy-application-or-system>

³ This ranking is based on WMATA's IT COOP and how IT assets are categorized by the incident response processes and severity (A = High, B = Medium, C = Low).

⁴ GAO-19-471 report entitled, *Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, issued in June 2019.

A 2018 Flexera Report⁵ provides that an IT application or system normal useful life is five years (see Diagram 1). However, the manufacturer/supplier may have their own recommendations for keeping the application or system current, and these conditions should be included in strategic planning considerations.

Diagram 1 - IT Application or System Life Span



The life span of a system can be extended by application or system enhancements, modifications, and new software releases. Several of WMATA aged systems have been enhanced and upgraded to extend the service life and improve functionality.

Business Units

The IT Department provides IT support to all WMATA Business Units operations. The IT Department provides information technology and telecommunication services to support WMATA's strategic goals including safety, customer service, transparency, and decision support.

The Office of IT Software Service and Infrastructure is responsible for planning and administering WMATA's transit, business applications, and systems. These services include IT project management and operational maintenance, development, configuration, implementation, upgrades of WMATA applications and lifecycle of systems.

The Office of Enterprise Architecture develops the IT strategic plan and facilitates transformation of business vision and strategy. This office provides an overarching architectural perspective and strategic roadmap to meet enterprise goals. This office acquires a complete understanding of business processes, information flows, and collaborating applications and technology infrastructure.

The Department of Strategy, Planning, and Program Management manages capital funds for IT projects. The Department of the Chief Financial Officer provides budget services for IT projects.

⁵ https://resources.flexera.com/web/pdf/Research-DP-Manufacturer-Product-EOL-EOS-Report-2018.pdf?elqTrackId=39ea27808bfa4bf0b3fc810d2b34492b&elqaid=3991&elqat=2&_ga=2.12461172.1384321781.1542126736-1286143296.1542126736

Prior Audit Coverage

The OIG report entitled, *Audit of WMATA's Software Asset Management (SAM) Program*, dated June 19, 2019, concluded that WMATA's IT Department had not implemented a comprehensive SAM program capable of managing software assets across the enterprise. A SAM program would allow WMATA to fully manage software from implementation to retirement which would support modernization planning. The IT Department did not have a comprehensive SAM program because it needed to centralize financial control of IT assets, better align IT resources, and develop baseline program policies. During this audit, OIG found that this condition still existed. The IT Department's management plans to fully implement the recommendations by FY 2022.

AUDIT OBJECTIVE AND RESULTS

Audit Objective

The audit objective was to determine whether WMATA has developed plans for modernizing or replacing legacy systems and the adequacy of the modernization plans.

Audit Results

Absent or Incomplete Modernization Plans for Mission Critical Systems

WMATA had not developed modernization plans for three of six of the mission critical systems OIG sampled and for the remaining three systems, modernization plans were incomplete (see Table 1). These systems include [REDACTED]

[REDACTED] All of the systems without plans are over ten years old, could require costly maintenance contracts, and may be incompatible with more modern systems.

To provide a road map for modernization, WMATA should develop modernization plans well in advance of system retirement/replacement. For example, WMATA took seven years to develop and implement MetroTime (the replacement of the PeopleSoft Human Capital Management suite) due to project management issues.

Table 1 - Sample Listing of Mission Critical Systems⁶

No.	System or Platform Name	Maintenance Cost (Annually)	Implementation Date	System Type	Criticality	Modernization Plans (Yes/No)
1	[REDACTED]	[REDACTED]	August 2008	[REDACTED]	High	No
2	[REDACTED]	[REDACTED]	May 2006	[REDACTED]	Medium	No
3	[REDACTED]	[REDACTED]	May 2005	[REDACTED]	Medium	No
4	[REDACTED]	[REDACTED]	July 2010	[REDACTED]	Medium	Yes
5	[REDACTED]	[REDACTED]	July 2004	[REDACTED]	Low	Yes
6	[REDACTED]	[REDACTED]	April 2013	[REDACTED]	High	Yes

* This system is internally maintained.

** An Enterprise Resource Plan assessment is in process.

*** This solution is being replaced with [REDACTED]

⁶The tables were developed based on a methodology used in the GAO-19-471 report titled, *Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, issued in June of 2019. OIG selected a judgmental sample of 6 of 21 systems, which WMATA had provided as critical rankings of low, medium, or high.

Incomplete Modernization Plans

While WMATA had developed elements of modernization plans, none of the plans were complete (refer to Table 2).

Table 2 – Documentation of Key Elements of Modernization Plans

System	Includes milestones to complete the modernization	Describes work necessary to modernize system	Summarized planned disposition of legacy system
[REDACTED]	Partial	Yes	Yes
[REDACTED]	Partial	No	Yes
[REDACTED]	Partial	No	Partial

Yes – Agency included element in modernization plan.
 Partial – Agency partially included element in the modernization plan.
 No – Agency did not include element in the modernization plan.

What Is Required

IT Project Lifecycle Management (PLM) Process - The PLM provides a project management framework for IT management and stakeholders to follow. The PLM requires that the organization monitor the IT solutions and identify and resolve changes and problems to ensure the solution meets ongoing organizational and functional needs.

A GAO report found, based on a review of government and industry best practices,⁷ agencies should document modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

CoBIT 5, section BAI03.10, entitled “Maintain Solutions” (IT assets or systems) provides a set of best practices for organizations to follow.⁸ Those best practices are as follows:

- Manage all programs in alignment with enterprise strategy and in a coordinated way;
- Realize business benefits and reduce the risk of unexpected delays, costs and value erosion by improving communications and involvement of business and end users;
- Develop and execute a plan for the maintenance of solutions and infrastructure components; and
- Conduct periodic reviews against business needs and operational requirements such as patch management, upgrade strategies (or modernizing), risk, vulnerabilities assessment, and security requirements.

⁷ *Information Technology - Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (June 11, 2019).

⁸ *The Control Objectives of Information Technology (CoBIT) 5th edition, Process Reference Guide*.

Why This Occurred

IT management provided several explanations on the issues that affected IT's ability to prepare and implement modernization plans. Those issues included:

- *Unexpected Events* - The IT Department intended to develop an Enterprise Resource Plan for IT asset replacement. However, COVID-19 impacts and the JGB fire hampered their efforts and plans.
- *Reactive versus Proactive Planning Approach* - IT Department officials indicated that strategic planning and modernization/retirement processes have been more reactive than proactive. For example, instead of proactively replacing the Peoplesoft suite of systems,⁹ the manufacturer's software retirement caused WMATA to seek other solutions. Regarding the Advanced Information Management System, no formal communication has taken place to address the system and IT infrastructure challenges to modernization. The IT Department and business owners intuitively know the challenges, but no modernization plan has been developed.
- *Resource Challenges* - IT Department management stated that IT is currently restructuring the organization to address resource allocation issues pertaining to staffing critical functions.
- *WMATA's IT Department Had Not Developed a Comprehensive System Modernization Program* - WMATA was in the process of, but had not completed, the development of a comprehensive system modernization program. Such a program would address: (1) development of modernization plans, (2) defining "legacy systems" or "aging IT systems and IT infrastructure," (3) development of corporate governance over system modernization or replacement, and (4) implementation of a centralized Management Information System.

Why This Is Important

The absence of or incomplete modernization plans could impact WMATA's ability to effectively and efficiently operate and accomplish its mission. Operationally, WMATA could experience a greater frequency of system crashes, data breaches and/or data losses, while also having lower performance, lower efficiency, and a greater number of technical limitations for improvement. Modernization plans provide a proactive and planned approach to managing WMATA's aging IT infrastructure. Without this approach, WMATA could (1) become dependent on costly maintenance contractors, (2) be forced to rely on temporary and short-term fixes, and (3) lose support services for IT products that are not timely updated or replaced.

In addition, a legacy system may still meet the needs for which it was originally designed yet not allow for growth or interaction with newer systems. Instead of offering WMATA the latest capabilities and services, such as cloud-based computing and better data integration, a legacy system may keep WMATA from achieving the benefits of new software and platforms.

⁹ A packaged business software system that allows an enterprise to automate and integrate its business processes, share common data and practices across the entire enterprise, and produce and access information in a real-time environment.

Recommendations

We recommend the General Manager/Chief Executive Officer (GM/CEO):

1. Develop and implement a comprehensive modernization/replacement program for all mission critical legacy systems that includes, at a minimum:
 - (a) defining mission critical legacy systems;
 - (b) prioritizing modernization or replacement plans by evaluating mission critical legacy systems risks, interfaces, costs, and other business needs;
 - (c) developing a comprehensive strategic plan for modernization and/or replacement of all mission critical legacy systems;
 - (d) developing modernization or replacement plans for individual mission critical legacy systems with the assistance of business owners; and
 - (e) finalizing management roles and organizational structure over WMATA's mission critical legacy system modernization or replacement processes. (EVP-IBOP)
2. Develop and implement a centralized Management Information System, solution, or tool to facilitate modernizing IT assets throughout their lifecycle. (EVP-IBOP)
3. Coordinate with the capital and budget departments to determine a strategy and funding for a (1) centralized Management Information System and (2) comprehensive modernization and replacement program. (EVP-IBOP, EVP-SPPM, EVP-CFO)

SUMMARY OF MANAGEMENT'S RESPONSE

WMATA's Executive Vice President and Chief of Internal Business Operations (EVP/CIBO) provided written comments, dated August 23, 2021 (Appendix B). The EVP/CIBO fully concurred with the finding and recommendations to be completed by December 31, 2023. OIG considers management's comments responsive to the recommendations and the actions taken or planned should correct the deficiencies identified in the report.

Further, OIG appreciated the additional information and clarifications to the report provided in Management's Response on pages 6 and 7. OIG agrees with responses numbered 1 - 5 and provided additional references to the report below for clarification, as necessary. OIG disagreed with WMATA's response to number 6 on the adequacy of current plans as none of the mission critical systems sampled had complete modernization plans.

OIG's comments to Management's Response are as follows:

1. OIG's comments to Management's Response - additional information and clarifications, number 1, response page 6: OIG agrees technology investments are scattered within and outside of IT. Management's Response clarified the extra-IT technology and systems outside IT will be remediated via the authority of the newly created centralized governance board.
2. OIG's comments to Management's Response - additional information and clarifications, number 2, response page 6: OIG agrees a balanced evaluation and assessment are needed to determine and identify legacy systems. We further agree that old systems may not always equate to obsolete; nor does long-life equate to increased maintenance costs. In the report, OIG cited outdated software and incompatibility with more modern systems as legacy factors. Further, OIG concluded that WMATA "could" rather than "will" become dependent of costly maintenance contractors.
3. OIG's comments to Management's Response - additional information and clarifications, number 3, response page 6: OIG agrees resource optimization challenges may have decelerated IT's momentum. The report referred to IT resource challenges and unexpected events, which hampered IT efforts and plans.
4. OIG's comments to Management's Response - additional information and clarifications, number 4, response page 6: OIG agrees that IT needs an enhanced IT asset management tool and as stated plans to migrate to an IT Asset Management (ITAM) system of record.
5. OIG's comments to Management's Response - additional information and clarifications, number 5, response page 6: OIG agrees that WMATA IT should take a proactive planning approach to modernizing its systems.

SUMMARY OF MANAGEMENT'S RESPONSE (continued)

6. OIG's comments to Management's Response - additional information and clarifications, number 5, response pages 6 and 7: OIG disagrees that the audit did not capture the current mission critical system plan(s). OIG specifically requested formal modernization plans for the six systems sampled. The report concluded none of the systems sampled had complete modernization plans. The report cites as criteria three key elements of a modernization plan: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether WMATA has developed plans for modernizing or replacing legacy systems and the adequacy of the modernization plans.

Scope

The audit included a review of mission critical systems and the attributes of those systems.

Methodology

To achieve our audit objective, OIG:

- (1) Conducted interviews with WMATA management and personnel who were responsible for the strategic planning, administering, and maintaining WMATA's mission critical systems and solutions.
- (2) Requested, gathered, and reviewed relevant documentation such as inventories and modernization plans, in addition to the IT PLM process.
- (3) Incorporated WMATA, federal government, and IT industry best practices, standards, guidance, and criteria (including GAO and OIG reports) in developing the report findings and recommendations.
- (4) Reviewed relevant internal controls related to WMATA's mission critical systems.
- (5) Selected 21 systems deemed mission critical by WMATA, and judgmentally selected three other critical systems with medium and low designations.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

MANAGEMENT'S RESPONSE

M E M O R A N D U M



SUBJECT: Office of the Inspector General (OIG) DATE: August 23, 2021
Audit of WMATA's Mission Critical
Legacy Systems

FROM: IBOP – John T. Kuo [Redacted]

THRU: GM/CEO – Paul J. Wiedefeld [Signature]

TO: OIG – Geoffrey Cherrington

WMATA's Executive Vice President and Chief of Internal Business Operations (CIBO) has prepared the following in response to the Office of Inspector General's (OIG) Audit of WMATA's Mission Critical Legacy Systems.

WMATA's CIBO has reviewed the audit report and held preliminary discussions regarding OIG's recommendations with the offices of Information Technology (IT). This memorandum details the initial plans to address referenced areas and improve the process to modernize or replace Mission Critical Legacy Systems, in line with the OIG's recommendations.

WMATA Management concurs with the findings and recommendations related to absence or incomplete modernization plans for Mission Critical Systems made in this report. Metro-IT is cognizant of the challenges and therefore, has already initiated significant mitigation actions (also recommended by Deloitte) including but not limited to the following:

- 1. Establishing a Digital Investment Governance Board (authorized by GM and CEO, and implementation is underway), and a part of Enterprise IT Governance Program that will begin influencing and directing the optimization of Enterprise Information Systems, modernization of mission critical systems, legacy systems and also adaptation of new technology and innovative solutions for future ready technology footprint at WMATA. The key value proposition is to promote clear Line of Sight from technology strategy and investment and oversee how technology is protected, planned, budgeted, and managed across WMATA.
2. Establishing a cohesive IT Asset Management Program that caters to both Software Asset Management (SAM) and Hardware Asset Management (HAM) in a unified manner (ITAM) to address and mitigate the procedural and operational challenges and optimize ongoing maintenance, support, updates, upgrades, renewals, license management etc. throughout the lifecycle of IT assets. RSA Archer is the current SAM solution, and a FY23

Washington
Metropolitan Area
Transit Authority

Office of the Inspector General (OIG)
Audit of WMATA's Mission Critical Legacy Systems
Page 2 of 7

project is proposed to enhance ServiceNow to be the enabling platform for ITAM.

Note: A separate but similar OIG audit of "End-of-Service Life Operating System Software" has been conducted and CAP 454 is in-effect to address those findings by 6/30/2022. For simplicity, the application software and operating system software actions will be separated in terms of reporting, but will leverage a common program, system, and discipline.

3. Establishing a key Design Unit (DU) with primary focus on design and development of an updated Enterprise Technology Optimization and Modernization Strategy and Plan. The end outcome is to have a planned and proactive approach to manage WMATA's aging IT Infrastructure evaluation against refreshed current- and future-state architectures, functionality, business value, technical fit and total cost of ownership etc. and leverage the recommendations for effective change management and technology migration strategy and implementation pathway.
4. Establishing another key Design Unit (DU) and an enabler for Enterprise Architecture and Modernization Roadmap for ensuring that all IT investment decisions are planned, strategically driven, standards-based, and non-duplicative. The end-outcome is to assist WMATA in reducing IT costs and enable effective business transformation.

WMATA Management also proposes that planful and persistent programmatic funding for, and commitment to, intelligent intra-IT and intra-authority technology investment for the above initiatives is fundamental to expected practice maturity, mitigate challenges and adverse impact triggered by reactive replacement processes and resource mobilization. Collectively, these initiatives (identified and planned) - upon relevant funding - address corrective actions that need to be taken to correct the deficiencies identified in the report.

WMATA Management agrees to complete all the recommendations by December 31, 2023.

OIG Recommendations and Management Response

1. Develop and implement a comprehensive modernization/replacement program for all mission critical legacy systems that includes, at a minimum:
 - (a) defining mission critical legacy systems;
 - (b) prioritizing modernization or replacement plans by evaluating mission critical legacy systems risks, interfaces, costs and other business needs;

Office of the Inspector General (OIG)
Audit of WMATA's Mission Critical Legacy Systems
Page 3 of 7

- (c) developing a comprehensive strategic plan for modernization and/or replacement of all mission critical legacy systems;
- (d) developing modernization or replacement plans for individual mission critical legacy systems with the assistance of business owners; and
- (e) finalizing management roles and organizational structure over WMATA's mission critical legacy system modernization or replacement processes.

Response:

ITSS, in collaboration with ITIO and ITEA will design, develop, and implement a comprehensive Technology Systems Modernization Strategy and Plan for all mission critical systems with following components, at minimum. This action will be complete by June 30, 2022.

- (a) defining mission critical legacy systems;

Response:

Recently ITCS has developed and presented an application risk rating, which may or may not align directly with OIGs also new critical application designation. It would be advantageous to ensure that all risk and criticality assignments are harmonized and used authority wide. Once agreed, IT/ITSS shall update the inventory of IT applications, define mission critical systems, including legacy systems, and segment the applications under various levels of criticality. This action will be complete by December 2021.

- (b) prioritizing modernization or replacement plans by evaluating mission critical legacy systems risks, interfaces, costs, and other business needs.

Response:

IT/ITSS shall prioritize individual modernization plans, retirement/replacement plans, update/upgrade plans, etc. for all mission critical systems (identified in (a) above) after due diligence based review and assessment factoring system risks, key interface ongoing costs, total costs of ownership, recurring costs, business needs etc. This action will be complete by June 30, 2022.

- (c) developing a comprehensive strategic plan for modernization and/or replacement of all mission critical legacy systems;

Office of the Inspector General (OIG)
Audit of WMATA's Mission Critical Legacy Systems
Page 4 of 7

Response:

The Digital Investment Governance board has been established by the GM (attached) and will begin influencing - and directing as necessary - a harmonized investment plan for technology across the authority. The success of this board is fundamentally contingent on the development of a holistic technology plan and fully integrated investment plan with IT/ITSS. IT shall develop a comprehensive strategic plan (near-term, short-term, and long-term) for modernization, retirement/replacement, etc. for all mission critical systems (identified in (a) above) and sign-off by stakeholders. This action will be complete by June 30, 2022.

(d) developing modernization or replacement plans for individual mission critical legacy systems with the assistance of business owners; and

Response:

IT/ITSS shall develop modernization plan, retirement/replacement plan etc. for individual mission critical system and sign-off by respective stakeholders. This action will be complete by August 31, 2022.

(e) finalizing management roles and organizational structure over WMATA's mission critical legacy system modernization or replacement processes.

Response:

IT/ITSS shall design and develop governance artifacts, including Standard Operating procedure, process flows, Roles and Responsibilities (RACI) chart and organizational structure to manage WMATA's mission critical and/or legacy system modernization, retirement/replacement plan. This action shall require approval and communication from EVP-IBOP and will be complete by June 30, 2022.

2. Develop and implement a centralized Management Information System, solution, or tool to facilitate modernizing IT assets throughout their lifecycle.

Response:

IT has implemented a software asset management solution hosted in RSA Archer; OIG was provided with access to this system to conduct this audit. The solution is being augmented and enhanced to provide additional value apart from its initial incarnation/iteration as an application inventory and software licensing management system. Later, as a FY2023 project, IT

Office of the Inspector General (OIG)
 Audit of WMATA's Mission Critical Legacy Systems
 Page 5 of 7

plans to migrate to ServiceNow as the final ITAM system of record.

In that project, IT/ITSS, in collaboration with IT/ITIO and IT/ITEA will complete the requirement specifications, proposed solution design, solution architecture landscape, develop, test and implement a centralized Management Information System solution to facilitate management and monitoring of modernization, and retirement/replacement of IT Assets throughout their lifecycle. This action shall require approval and communication from EVP-IBOP and will be complete by December 2022.

Note: This action also has dependencies related to completion of the following initiatives for an informed decision making related to modernization, retirement/replacement needs. EVP-IBOP and SVP and CIO shall collaborate to drive completion of these dependencies:

- Establishing a holistic Software and Hardware Governance Framework and enforce compliance with a cohesive IT Asset Management Program (expected to be completed by December 2022)
- Establishing a Digital Investment Governance Board within the framework of Enterprise IT Governance Program (expected to be completed by December 2021)
- Establishing a definitive Enterprise Technology Optimization and Modernization Strategy and Plan aligned with Enterprise Architecture and Modernization Roadmap (expected to be completed by December 2023)

3. Coordinate with the capital and budget departments to determine a strategy and funding for a (1) centralized Management Information System and (2) comprehensive modernization and replacement program.

Response:

IT/ITSS, in collaboration with EVP-IBOP, EVP-SPPM and EVP-CFO shall determine a strategy and funding for the following:

- (1) **Centralized Management Information System Solution.** Please refer response to 2. above. This action shall be completed and sign-off by EVP-IBOP, EVP-SPPM and EVP-CFO by December 2021.
- (2) **Comprehensive Modernization and Replacement Program.** Please refer response to 1. above. This action shall be completed and sign-off by EVP-IBOP, EVP-SPPM and EVP-CFO by December 2021.

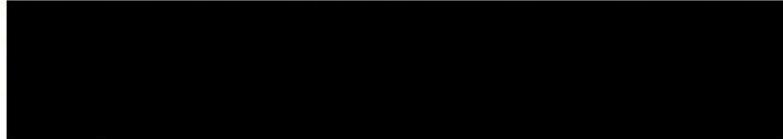
Office of the Inspector General (OIG)
Audit of WMATA's Mission Critical Legacy Systems
Page 6 of 7

The following paragraphs provide additional information and clarifications considered relevant to the findings in the report:

1. Historically, the technology investments are scattered across WMATA (within and outside of IT). The corrective action items outlined cover the systems known and supported by IT. The Risks associated with extra-IT technology and systems (outside of IT-discipline) will be remediated through the recently created centralized enterprise technology governance board, with a consolidated directive at the Authority Level. The board has been designated by the GM and had its inaugural meeting on August 20, 2021.
2. Technology solutions encompasses an integrated system of multiple components, and the technology roadmap, end of life and end of support defines the economic life of a technology solution. Old may not always equate to obsolete nor does the long-life equate to increased maintenance costs. A balanced evaluation and assessment are needed to carve of the segmentation of legacy applications and take mitigation actions accordingly.
3. Resource optimization challenges due to shift in priorities, accentuated with the pandemic response, and funding limitations decelerated the momentum across the technology investment portfolio.
4. An enhanced IT Asset Management tool is needed to support higher-level management functions, such as proactive monitoring, automated asset interrogation, and capacity planning. ServiceNow has been selected by ITSS for use as the enterprise Software and Hardware Asset Management and SACM tool. Service Now is a leader in SAM and ITAM systems, and WMATA already subscribes to the SAM module, so the HAM module will need to be implemented to facilitate and support this planned transformative capabilities maturation.
5. With the Digital technology Governance Board and Enterprise IT Governance framework, WMATA-IT intends to take a forward leap towards proactive planning approach that covers timely triggers, alerts, notifications, periodical reviews, proactive monitoring etc.
6. Related to the sample listing of mission critical systems, IT would suggest that OIGs report did not fully capture the current plan for each:

a. 

Office of the Inspector General (OIG)
Audit of WMATA's Mission Critical Legacy Systems
Page 7 of 7

- b. 
- c. 
- d. 
- e. 
- f. 

LIST OF MISSION CRITICAL SYSTEMS

No.	System Name	WMATA Business User	Criticality	PII	Business Function
1.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
2.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
3.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
4.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
5.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
6.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
7.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
8.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
9.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
10.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
11.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
12.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
13.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
14.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
15.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
16.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
17.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
18.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
19.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
20.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
21.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
22.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
23.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
24.	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

*In addition to the 21 systems deemed highly critical by WMATA, the OIG judgmentally selected three other critical systems with medium and low designations.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: hotline@wmataoig.gov

Telephone: 1-888-234-2374

Address: WMATA
Office of Inspector General
Hotline Program
500 L'Enfant Plaza SW, Suite 800
Washington, DC 20024