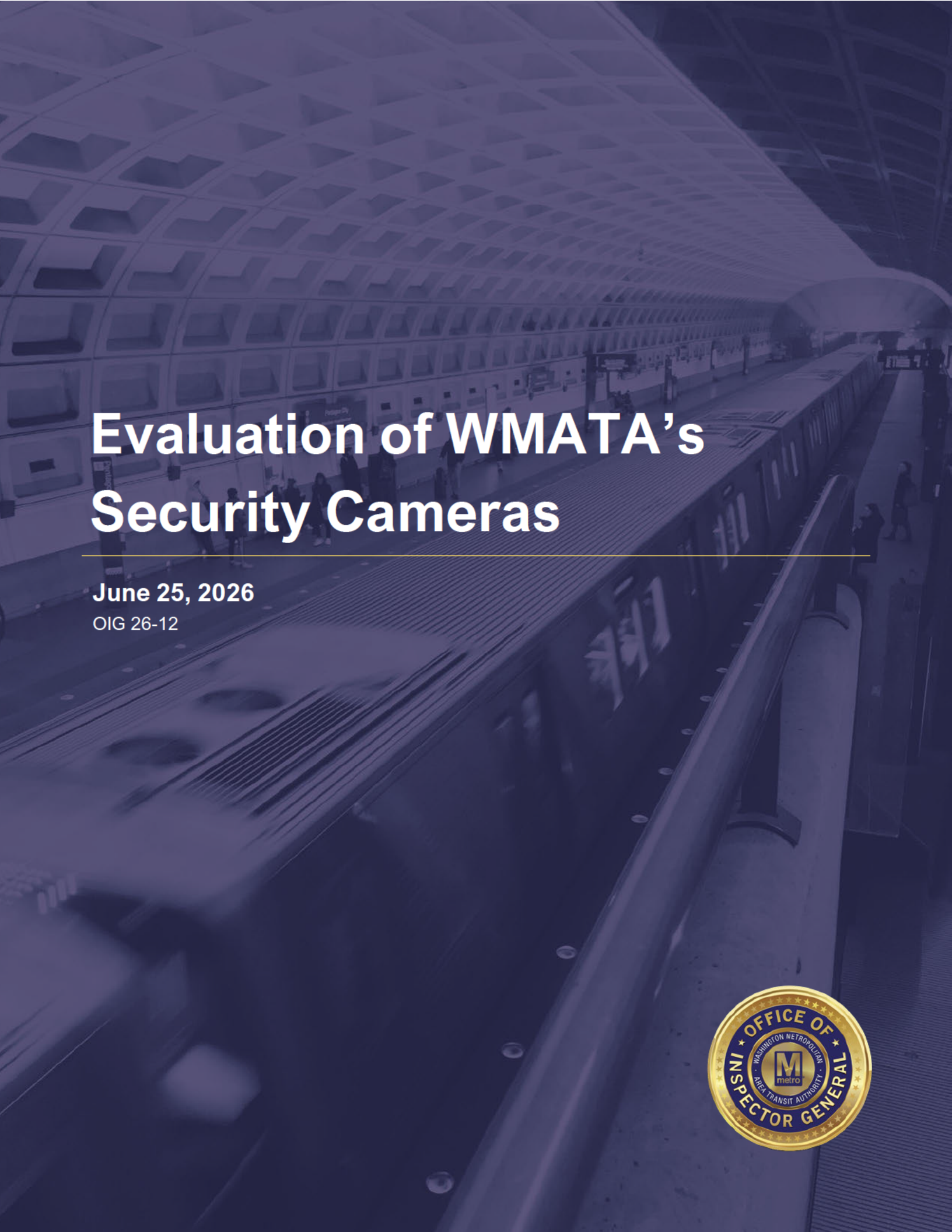

Evaluation of WMATA's Security Cameras

June 25, 2026

OIG 26-12

Results in Brief

Evaluation of WMATA's Security Cameras

Evaluation Objective

The evaluation objective was to assess the functionality and operational effectiveness of security cameras installed across the Washington Metropolitan Area Transit Authority (WMATA). Specifically, the Office of Inspector General (OIG) sought to determine if WMATA's cameras are functioning and being maintained to ensure safety and security throughout the WMATA system.

Why We Did the Evaluation

- Malfunctioning cameras may impact incident response capabilities, limit the availability of critical video evidence to support criminal and administrative investigations, and introduce potential safety, operational, legal, and reputational risks for WMATA.
- This evaluation was included in OIG's Annual Audit and Evaluation Plan for Fiscal Year 2025.
- The Infrastructure Investment and Jobs Act (IIJA) requires OIG to assess the effective use of funding for significant capital improvement projects.

Recommendations

OIG made six recommendations. By addressing these recommendations, WMATA can strengthen oversight, ensure comprehensive video availability, and mitigate safety and operational risks as they transition to a new video management system.

What OIG Found

OIG's review of over 5,700 cameras found that security cameras were generally working as intended. Most cameras were operational, and staff were generally performing preventive maintenance on schedule. However, we identified vulnerabilities that could impede WMATA's ability to respond to incidents and maintain comprehensive video coverage. OIG found the following:

1. Limitations in mSET technology and buses with incompatible camera systems impact real-time monitoring of WMATA's bus fleet.
2. Gaps exist in access and monitoring controls over the mSET application.
3. Gaps exist in the preventive maintenance and inspection records for fixed facilities.

Table of Contents

The Washington Metropolitan Area Transit Authority (WMATA) has over 30,000 cameras installed across its railcars, buses, MetroAccess vehicles, and facilities. WMATA's security cameras serve as both a visible deterrent to crime and a critical tool for real-time incident response, investigative support, and operational oversight. Reliable video coverage supports WMATA's commitment to safety and security, helps protect passengers and employees, and provides essential evidence for criminal, civil, and administrative matters. Overall, WMATA's camera systems are functioning effectively. For cameras installed in facilities, on railcars, and on MetroAccess vehicles, OIG observed limited instances where cameras were not working correctly or had obstructed views. Specifically, over 97 percent of the cameras we sampled at facilities and on railcars, and 96 percent in MetroAccess vehicles, were operating effectively.

Current Camera Systems

WMATA's security cameras operate on multiple video management systems (VMS): Verint, mSET, Genetec, FleetWise, and Lytx DriveCam (*see* **Table 1**). WMATA's Office of Infrastructure manages cameras installed at facilities (including railyards, bus garages, stations, and other facilities) through Verint. The Office of Operations manages cameras installed on railcars, buses, and MetroAccess vehicles through Genetec, mSET, FleetWise, and Lytx DriveCam.

The general collection of these video camera systems is known as the Camera Network System (CNS).[1] According to Policy/Instruction 11.6/1, Camera/Video Access, Distribution and Retention, WMATA's Metro Integrated Communication and Command Center (MICC) oversees access, distribution, and retention of video from CNS. MICC also uses CNS to monitor live and historical videos across the rail and bus networks, including stations and facilities.

Table 1: WMATA's Current Camera System Landscape

System	Installation Location/Type	Department Alignment	Description
Verint	Fixed facilities	Infrastructure	Hosted on WMATA's internal network • Real Time Video Access • Historic Video Access

[1] *Lytx DriveCam cameras installed in Metro Access vehicles are not considered part of the CNS, as Metro Access vehicles are operated and maintained by third-party contractors: WeDriveU and Challenger.*

mSET	Buses	Operations	Third-party application • Real Time Video Access • Historic Video Access
Genetec	6000-series railcars	Operations	The new Enterprise Video System (EVS) on WMATA's internal network • Real Time Video Access • Historic Video Access
FleetWise	7000-series railcars	Operations	Onboard Video Recorder • Historic Video Access
Lytx DriveCam	Buses and MetroAccess Vehicles	Operations	Used primarily to monitor operator behavior • Real Time Access • Historic Video Access

New Enterprise Video System (EVS) Project

In November 2024, WMATA launched the EVS project to strengthen system performance. The EVS project is a multi-year and multi-phased modernization initiative to bring all but the Lytx DriveCam camera system under a single application: Genetec. Currently, only phase one has been approved, and the project is ongoing. During the first phase, WMATA upgraded and transitioned the cameras installed on all 6000-series railcars to Genetec.[2] In addition, WMATA plans to upgrade 10 buses and integrate cameras at four stations over to Genetec. They will also complete the installation of the new Genetec video core server. Under phase two, WMATA will transition the 7000-series railcars to Genetec.[3] WMATA anticipates completion of phase two by fiscal year 2029. [redacted]. WMATA has developed a plan to implement this functionality; however, full coverage will not be achieved until implementation is complete.

[2] *Transition of 6000-series railcar cameras was completed on December 9, 2025.*

[3] *WMATA anticipates phase two to start in the first quarter of fiscal year 2027.*

Evaluation Methodology

To assess the functionality and operational effectiveness of the security cameras installed across WMATA, OIG reviewed live and historical video footage from cameras across the network as well as maintenance records and other relevant documents. OIG obtained the entire population of cameras and sorted them into five categories based on installation location: Facilities/Stations, 7000-Series, 6000-Series, Buses, and MetroAccess Vehicles.[4,5] OIG then selected a random sample of over 5,700 cameras, accounting for approximately 19 percent of the total population.

OIG established the following criteria to evaluate each camera within our sample:

Table 2: Evaluation Criteria for Cameras

Criteria	Definition
Is the camera on?	The camera is enabled and shows an active connection to the system.
Is an error code visible?	The system displays an error code for the camera.
Is the view obstructed?	An object, such as a structure, debris, or foliage, is blocking the camera's view.
Is the view in focus?	The camera video or image is clear.

OIG then reviewed maintenance records for cameras we identified as having an error code, being obstructed, or being out of focus. OIG established the following criteria to evaluate WMATA's maintenance practices for cameras:

Table 3: Evaluation Criteria for Maintenance

Criteria	Definition
Do inspection/maintenance process and procedures exist?	Written procedures that outline maintenance practices as they relate to cameras.
What is the inspection/maintenance schedule?	What are the maintenance intervals used to conduct preventive inspections?
Were any issues, including those observed by OIG, identified and documented on inspection/maintenance records?	Issue is identified, documented, and reported (included in a status report or work order).

[redacted] *These railcars will be phased out with the introduction of the 8000-series railcars currently in production.*

[5] *WMATA plans for camera systems installed on 8000-series railcars, currently in production, to be compatible with EVS (i.e., Genetec).*

What was the status of the issue?	Has the issue OIG observed been addressed or scheduled for correction?

Funding Sources for the Security Cameras

In November 2021, Congress and the President enacted the Infrastructure Investment and Jobs Act (IIJA). Section 30019(d)(2)(E)(iii) of IIJA requires WMATA OIG to issue a report, two years and five years after the enactment of the IIJA, that includes, among other things, an assessment of the effective use of funding to address major Capital Improvement Program (CIP) projects.

The security improvements, which include security cameras, are funded by CIP 0145, CIP 0007, and CIP 0386. CIP 0145 provides funding for improvements to WMATA's life safety and security system and associated state of good repair (SOGR) maintenance for those related systems. CIP 0007 provides funding for replacing CCTV cameras on board buses to maintain SOGR. CIP 0386 provides Metro with an integrated video surveillance and operations system. The purpose of the project, in part, is to bring all security camera systems under a single application to include bus, rail, and facilities.[6] See **Appendix B** for a detailed breakdown of cost information.

[6] *Cameras in Metro Access vehicles are not included in the project.*

Finding 1: Limitations in mSET Technology and Buses with Incompatible Camera Systems Impact Real-Time Monitoring of WMATA's Bus Fleet

OIG identified issues affecting WMATA's ability to monitor its bus fleet in real time due to limitations within the mSET video system and the presence of buses equipped with incompatible camera technology. These issues restrict WMATA's operational visibility while buses are in service and may reduce the agency's ability to respond promptly to safety- or security-related incidents.

Camera Systems on Buses

WMATA has between six and twelve cameras installed throughout each bus, which primarily operate on the mSET system.[7] Each bus is equipped with a digital video recorder (DVR) to store historical video footage that WMATA can download via MetroNet Wi-Fi when the bus returns to a WMATA facility. Additionally, WMATA should be able to access the cameras directly via a 4G LTE cellular network when buses are in service. However, some buses are equipped with older DVR systems that are not compatible with mSET and therefore cannot be accessed remotely. In these cases, WMATA personnel must be physically present on the bus to download video footage directly from those DVRs.

Real-Time Monitoring Limitations

OIG sampled 516 mSET cameras across 76 buses to evaluate their functionality by reviewing real-time video feeds. Of the 516 cameras sampled, OIG was unable to view real-time videos from 494, which accounts for 96% of the total. Moreover, 86 cameras, representing 17% of those cameras across 13 buses, had DVRs that were incompatible with mSET.

WMATA personnel reported that the connectivity issue began in July 2025 after an mSET software update and that management has yet to identify the root cause of these problems.[8] Therefore, WMATA has been relying on the Lytx DriveCam cameras, installed on buses to monitor bus operator behavior, for real-time video. However, Lytx DriveCam cameras only provide a single internal viewing angle from the front of the bus. In contrast, mSET cameras, when operating as intended, provide WMATA with multiple real-time views throughout the bus.

---

[7] *WMATA buses are also equipped with Lytx DriveCam cameras installed at the front of the bus. Those cameras are primarily intended for monitoring bus operator behavior.*

[8] *At the time of this evaluation, WMATA was actively engaged with the vendor to resolve the connectivity issue.*

Since OIG could not assess the cameras on mSET in real time, we reviewed 201 recordings from the DVRs to verify that the cameras on the mSET system were functioning. We determined that 200 of those cameras were functioning properly and clear of obstructions. However, not having real-time views from those cameras may negatively impact incident response and operational oversight.

Recommendation

OIG recommends that the GM/CEO:

1. Develop and implement a plan to prioritize and address deficiencies in real-time video access for cameras on the mSET system and cameras with incompatible DVR systems. This plan should include defined timelines and milestones for implementation.

   Management Response

   WMATA concurs with this finding and recommendation. The issue was not related to the mSET software update. Joint analysis by the Video and Service Delivery and Operation (SD&O) teams determined that the service disruption resulted from bandwidth constraints on APN circuits supporting real-time video access from the bus fleet. These constraints reduced throughput and caused intermittent retrieval failures.

   In coordination with AT&T, the teams addressed the backhaul limitations. On April 14, 2026, AT&T upgraded the affected circuits from 10 Mbps to 2 Gbps. Following the upgrade, system performance stabilized, and all real-time video access issues were resolved by mid-April 2026. Over the next 90 days, WMATA will implement proactive monitoring of APN circuit utilization to detect bandwidth saturation early and establish a formal cross-team escalation protocol between Video and Digital Modernization. This approach will accelerate issue identification and resolution, strengthening operational resilience, and improving detection of network-related risks.

   WMATA will also conduct an inventory-based assessment of buses equipped with incompatible DVR systems and develop a prioritized upgrade and replacement plan. The plan will include defined milestones, timelines, and regular status reporting to ensure accountability, prioritize upgrades based on operational risk, and maintain visibility into progress and potential delays.

Accountable Organizations: Digital Modernization (lead), Metro Integrated Command and Communications Center (MICC) Video Operations, in coordination with SD&O

Success Measures: Sustained real-time video availability; early detection of network saturation; completion of DVR upgrade plan

Risk if Delayed: Degradation of real-time video access impacting operational visibility and incident response

The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

Finding 2: Gaps Exist in Access and Monitoring Controls Over mSET

According to management, any bus that is in operation should appear as active in mSET and be available for real-time and historical video viewing. During functionality testing of the bus fleet cameras in October 2025, OIG identified 17 buses that were unavailable for viewing in mSET. Thirteen of these buses had incompatible DVR systems, so they were rightfully excluded from mSET (*see* **Finding 1**). However, according to management, the remaining four buses (B4711, B4761, B4772, and B4783) were in operation and should have appeared as active in mSET. For example, Bus B4711 was reported as out of service in mSET but has been in operation since June 2025. Similarly, management confirmed that buses B4761, B4772, and B4783 were also in service and should have appeared as active in mSET.

Bus Fleet personnel were unable to determine the reason these buses did not appear as active in mSET, suggesting they might have been unintentionally deactivated or deleted. Bus Fleet personnel cited two reasons for their inability to determine a root cause. First, many WMATA employees have administrative-level access to mSET, which allows them to make changes within the system. Second, [redacted]

By limiting administrative access rights to personnel with a defined operational need, WMATA can reduce its exposure to mSET issues caused by intentional or erroneous system changes. Further, implementing activity logging capabilities within mSET would allow WMATA to effectively monitor, track, audit, and manage the system. Without proper controls, the mSET system is susceptible to undetected actions that may affect visibility into video footage or incident response, potentially introducing safety, security, and operational risks.

Recommendations

OIG recommends that the GM/CEO:

2. Review and update all mSET access levels and limit administrative access levels based on operational need.

Management Response

WMATA concurs with this finding and recommendation. Management will identify and remove unnecessary or excessive administrative privileges, particularly for users whose roles do not require elevated access. Access levels will be standardized and documented to ensure consistency, accountability, and compliance with internal security control requirements. Supervisory approvals and periodic access reviews will be implemented to strengthen governance and mitigate the risk of unauthorized access or misuse. Within the first 90 days, management will establish a recurring review process to ensure MSET access remains current and appropriate in response to personnel changes, including role changes, transfers, and separations. These actions are designed to strengthen internal controls and enhance overall system security.

Accountable Organization: Digital Modernization, Metro Integrated Command and Communications Center (MICC) Video Operations

Success Measures: All access roles reviewed and validated; administrative access limited to essential personnel

Risk if Delayed: Increased exposure to unauthorized access or misuse of sensitive data

The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

3. Implement activity tracking and access logging capabilities for mSET to record and monitor user access and actions. If full logging is not feasible, document the rationale and implement compensating controls, such as periodic access reviews, system monitoring, or audit trails, that provide equivalent oversight.

Management Response

WMATA concurs with this recommendation. Within the first 90 days, management will assess existing logging functionality and other critical system activities within MSET.

Digital Modernization and Metro Integrated Command and Communications Center (MICC) Video Operations will coordinate with Luminator to evaluate and, where necessary, enhance audit logging capabilities, including the capture of user behavior and administrative actions. If comprehensive activity logging cannot be achieved due to system, technical, or resource constraints, management will formally document the limitation and associated risk. To address any resulting gaps, management will implement compensating controls to ensure effective oversight and strengthen internal controls. These controls will include periodic user access reviews, supervisory monitoring of administrative activities, system-generated reporting, segregation of duties, and manual audit procedures.

Once implemented, these measures will support:

- Review and retention of audit logs
- Ongoing monitoring of reports to identify unauthorized access, inappropriate activity, or potential security concerns
- Periodic validation that user access remains appropriate and aligned with operational responsibilities.

Accountable Organizations: Digital Modernization (lead), Metro Integrated Command and Communications Center (MICC) Video Operations, Luminator.

Success Measures: Effective logging or compensating controls in place; availability of audit records for review.

Risk if Not Achieved: Limited ability to detect or investigate inappropriate system activity.

The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

Finding 3: Gaps Exist in the Preventive Maintenance and Inspection Records for Fixed Facilities

OIG conducted a review of preventive maintenance (PM) records for each department to determine if maintenance was performed within scheduled timeframes and properly documented. PM and inspection practices for security cameras vary across WMATA departments. In general, maintenance activities were performed as scheduled and properly documented for Bus Fleet, Rail Fleet, and MetroAccess vehicles.[9] However, OIG noted that PM records for fixed facilities were incomplete.

PM inspections for cameras at fixed facilities are governed by two procedures: ESS-PMI_E17000, *Video Camera Inspection and Cleaning* _Rev.4.0_2024, and INFR-COSI-COMM-SOP-01-00, *Entering Camera Position Numbers into Maximo for Corrective Maintenance.* Collectively, these procedures outline processes for conducting security camera PM inspections at four-month intervals and, if required, initiating corrective maintenance for offline cameras. WMATA also actively monitors camera statuses by conducting a daily camera network scan. Cameras that do not appear as active are noted in an offline camera report.

According to management, WMATA performs and documents PM inspections for security cameras by installation location (e.g., Metro Center Station). The Communications and Signals department retains camera PM inspection results in a centralized repository within a Microsoft SharePoint folder. As part of testing, OIG sought to sample PM records for 155 cameras installed across 32 locations. However, PM records for 98 of the 155 cameras (63 percent) at 14 locations we selected for review were not available in the repository. Moreover, 17 cameras were not included on the PM inspection sheets for nine locations. As a result, OIG could not determine if PM activities were performed.

OIG followed up with the Communications and Signals department to determine the cause of the missing PM inspections. They reported that personnel had misunderstood the instructions for PM inspection records retention. As a result, PM inspection records were not uploaded to the SharePoint folder.[10] OIG also noted that ESS-PMI_E17000 and INFR-COSI-COMM-SOP-01-00 do not provide guidance on PM inspection records retention.

Comprehensive PM documentation is critical to ensure security cameras remain operational and available to support incident response, investigations, and claims. Incomplete records reduce

[9] *See Appendix C for the PM and inspections practices for Bus Fleet, Rail Fleet, and Metro Access.*
[10] *Communications and Signals is now working to ensure all PM records are uploaded in SharePoint.*

assurance that all cameras receive required maintenance and that corrective actions are properly documented. WMATA can strengthen controls over records management and retention by providing clear guidance in its procedures.

Recommendations

OIG recommends the GM/CEO:

4. Update procedures to include placing completed preventive maintenance inspection records in the centralized SharePoint repository.

   Management Response

   WMATA partially concurs with this recommendation. In accordance with our Maintenance Control Policy, Maximo serves as the Communications and Signaling centralized system of record for all preventive and corrective maintenance activities. As noted in the OIG report, Management will revise the **ESS PMI_E17000** document to clearly identify Maximo as the centralized system of record and ensure full alignment with our policy. For clarity, document **INFR-COSI-COMM-SOP-01-00** is a procedural guide that instructs maintenance personnel on how to correctly identify the specific camera or device that failed in Maximo. Its purpose is to ensure accuracy and traceability when a deficiency is discovered during a preventive maintenance inspection. Because this procedure supports corrective maintenance activities and Maximo already serves as the centralized repository, this document does not require revision to include PM inspection record retention.

   Additionally, Management will reinforce the requirement that all maintenance documentation be consistently and accurately entered into Maximo to guarantee complete and reliable records.

   Accountable Organization: Communications & Signaling (COSI)

   Success Measures: Clear documentation of system of record; consistent and accurate maintenance record entry.

   Risk if Misaligned: Data inconsistencies and reduced traceability

   The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

5. Ensure that preventive maintenance and inspection processes provide assurance that all cameras are included in preventive maintenance inspections for each location; records are completed and stored in the centralized repository, and corrective actions are documented.

Management Response

WMATA concurs with this recommendation. Management will collaborate with Engineering to revise the preventive maintenance template to include a comprehensive checklist of all cameras at each facility. Management will also reinforce expectations for accurate completion of inspection records, proper documentation within the centralized repository, and timely initiation of corrective maintenance for any offline or defective cameras.

Accountable Organizations: COSI, Engineering

Success Measures: 100% of cameras included in inspections; complete documentation; corrective actions tracked.

Risk if Delayed: Undetected equipment issues and gaps in maintenance records

The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

6. Conduct periodic compliance reviews to confirm that preventive maintenance activities are properly documented and accessible.

Management Response

WMATA concurs with this recommendation. Management will perform periodic reviews to confirm that preventive maintenance inspections are completed in accordance with requirements, and that records are accurately documented and maintained in the centralized repository. These reviews will also identify documentation gaps and address any inconsistencies.

Accountable Organization: COSI

Success Measures: Verified completion and accessibility of maintenance records; closure of identified gaps.

Risk if Not Sustained: Reduced auditability and potential non-compliance

The estimated completion date for this action is: November 30, 2026

OIG Comment

OIG considers management's comments to be responsive to the recommendation and the corrective actions taken should resolve the issue identified in the report. OIG will follow up on the planned actions during the corrective action phase.

Scope

The scope of the evaluation includes security cameras managed by the Offices of Infrastructure and Operations, including Communications and Signals, Bus, Rail, and MetroAccess. During the evaluation, OIG reviewed the cameras' live feed and historical video to assess camera functionality, clarity, and compliance with preventive maintenance and inspection schedules.

Methodology

To achieve the evaluation objective, OIG's evaluation methodology was as follows:

- Researched and reviewed information, including current procedures and practices, benchmarking, and best practice reviews.
- Gained an understanding of management's plans and programs for managing security cameras across WMATA's system.
- Conducted interviews and reviewed data and documents related to the management and maintenance of security cameras.
- Performed testing of camera functionality based on computer-generated selected samples, with a sample size of approximately 19 percent of security cameras across all applications.
- Performed alternative procedures for bus security cameras on the mSET system.
- Reviewed maintenance records for compliance with preventive maintenance schedules and corrective maintenance.
- Benchmarked and compared WMATA's practices to the following other transportation agencies: the Southeastern Pennsylvania Transportation Authority, the New York Metropolitan Transportation Authority, and the Los Angeles Metro.

Principles and Standards for Offices of Inspector General (Green Book) Statement
The evaluation was conducted in accordance with the *Principles and Standards for Offices of Inspector General,* dated July 2024, approved by the Association of Inspectors General.

In November 2021, Congress and the president enacted IIJA. Section 30019(d)(2)(E)(iii) of IIJA requires WMATA OIG to issue a report, two years and five years after the enactment of the IIJA, that includes, among other things, an assessment of the effective use of funding to address major capital improvement projects. The funds used for security and camera surveillance upgrades are part of OIG's assessment of the effective use of funding to address major capital improvement projects.

The security improvements include security cameras and are funded under CIPs 0386, 0145, and 0007. The programs are funded through a combination of federal, debt (dedicated revenue bonds),[11] non-federal, system performance,[12] and dedicated funds.[13] See **Table 4** for the CIPs and the associated projects.

Table 4: List of CIPs and Budgets

CIP	Budget
CIP 0386	$29.62 million (FYs 2025-2026)
CIP 0145	$54.35 million (FYs 2022-2026)
CIP 0007	$23.15 million (FYs 2022-2026)

CIP 0386, Enterprise Video Ops & Security Program, is a security camera-specific program to integrate the video surveillance and operations system, install new cameras, and update backend systems to support camera operations, and include the following projects.

Table 5: Projects Related to CIP0386

Project ID	Project Name
CIP 0386_01	Enterprise-Wide Video Systems
CIP 0386_02	6000-series - Cameras, Routers, Storage
CIP 0386_03	7000-series - Video
CIP 0386_04	Platform Monitors

According to WMATA documents CIP 0007, Bus CCTV Replacement Program was to replace Metrobus cameras on-board buses to maintain SOGR, on lifecycle buses. CIP 0145, Facility Security Equipment Program, is to upgrade the life safety and security systems for security improvements, including Public Announcement systems, intrusion and additional security measures, SOGR maintenance for those related systems, and monitoring and supporting

[11] *Dedicated revenue bonds are paid down by jurisdictional dedicated funds.*

[12] *System performance is a different type of non-federal funding provided by the jurisdictions via the Capital Funding Agreement (CFA).*

[13] *Funds received through VA, MD, and DC.*

WMATA's legacy system during the transition to the Genetec. The projects included in the CIP are listed below.

Table 6: List of Projects Under CIP 0145

Project ID	Project Name
CIP 0145	Facility Security Equipment Program
CIP 0145_01	Bus Security
CIP 0145_02	Electronic Security Systems
CIP 0145_03	Security Systems - Non-Grant
CIP 0145_04	CCTV, 7 Stations (DHS)
CIP 0145_05	CCTV, 7 Stations SUP Funding
CIP 0145_06	Bus Authentication (DHS)
CIP 0145_07	CCTV, 8 Stations (DHS)
CIP 0145_08	NoMa Station CCTV Upgrade
CIP 0145_09	ESS Parking Garages
CIP 0145_10	Intercom Upgrade - 3 Locations
CIP 0145_11	Dulles Yard CCTV Improvements
CIP 0145_12	Tunnel Camera Demonstration
CIP 0145_13	End Platform Cameras
CIP 0145_14	ESS SOGR - Elec Labor Services

Tables 7-9 provide a detailed breakdown of funding sources and unaudited expenditures through November 30, 2025, for each CIP.

Table 7: CIP 0386 Expenditures through FY 2025

CIP #	Dedicated Funding	Federal Funding	Non-Federal Debt	Non-Federal System Performance	Total
CIP 0386					
2023			$1,636.09		$1,636.09
2024			$23,511.85	$473.95	$23,985.80
2025			$16,112.75	$44,918.51	$61,031.26
CIP 0386_01					
2023			$15,225.30		$15,225.30
2024				$10,021.49	$10,021.49
2025				$58,909.60	$58,909.60
CIP 0386_02					
2023			$86,871.09		$86,871.09
2024		$2,850,660.32	$3,577,985.24	$124,357.67	$6,553,003.23
2025			$6,258,911.53	$1,595,985.45	$7,854,896.98
CIP 0386_03					
2024			$181,530.63		$181,530.63
2025			$10,150.79		$10,150.79
CIP 0386_04					
2025				$410,239.18	$410,239.18
Total	**$ -**	**$2,850,660.32**	**$10,171,935.27**	**$2,244,905.85**	**$15,267,501.44**

Table 8: CIP 0007 Expenditures through FY 2025

CIP #	Dedicated Funding	Federal Funding	Non-Federal Debt	Non-Federal System Performance	Total
CIP 0007					
2022	$677,310.38				$677,310.38
2023					
2024	$338,008.00				$338,008.00
Total	**$1,015,318.38**				**$1,015,318.38**

Table 9: CIP 0145 Expenditures through FY 2025

CIP #	Dedicated Funding	Federal Funding	Non-Federal Debt	Non-Federal System Performance	Total
CIP 0145					
2022	$5,480,088.70			$469,043.82	$5,949,132.52
2023	$5,092,957.52		$10,594,005.93		$15,686,963.45
2024	$3,513,971.98		$2,903,262.74		$6,417,234.72
2025	$3,626,828.68		$149,068.30		$3,775,896.98
2026	$552,317.54				$552,317.54
CIP 0145_02					
2024	$222,954.00				$222,954.00
CIP 0145_03					
2023			$(3,968.63)		$(3,968.63)
2024	$3,968.63				$3,968.63
CIP 0145_04					
2023	$7,377.60				$7,377.60
CIP 0145_05					
2022	$5,052,549.80				$5,052,549.80
2023	$7,239,804.17				$7,239,804.17
2024	$418,055.75				$418,055.75
2025	$(1,045.06)				$(1,045.06)
CIP 0145_07					
2022				$62,351.29	$62,351.29
CIP 0145_08					
2022				$15,530.39	$15,530.39
2023	$1,925,133.95		$(79,121.30)		$1,846,012.65
2024	$1,220,688.80				$1,220,688.80
2025	$11,443.45				$11,443.45
CIP 0145_09					
2022				$6,968.76	$6,968.76
2023	$88,505.75		$298,312.40		$386,818.15
2024	$1,104,225.35		$136,122.95		$1,240,348.30
2025	$601,237.56		$5,165.10		$606,402.66

CIP #	Dedicated Funding	Federal Funding	Non-Federal Debt	Non-Federal System Performance	Total
CIP 0145_10					
2023	$92,482.55		$824,167.62		$916,650.17
2024	$1,601,671.51		$501,649.78		$2,103,321.29
2025	$801,060.34		$116,067.58		$917,127.92
CIP 0145_11					
2023	$792,503.61		$102,932.78		$895,436.39
2024	$930,857.48		$1,603.24		$932,460.72
CIP 0145_12					
2023	$570,703.39				$570,703.39
2024	$70,245.80				$70,245.80
CIP 0145_13					
2023	$304,704.98		$397,019.57		$701,724.55
2024	$3,169,398.26		$17,306.55		$3,186,704.81
2025	$28,373.69				$28,373.69
CIP 0145_14					
2023	$395,562.23		$(884,295.30)		$(488,733.07)
2024	$4,479,372.31		$16,360.86		$4,495,733.17
2025	$20,250.14				$20,250.14
Total	**$49,418,250.46**		**$15,095,660.17**	**$553,894.26**	**$65,067,804.89**

Bus Fleet

Procedures for the management and maintenance of security cameras for WMATA's bus fleet[14] is governed by BUSV-BMNT-SOP-1.27.07, *Bus Video Surveillance System Maintenance Program*, September 3, 2025. SOP-1.27.07 requires bi-annual PM inspections that consist of visual inspection of all cameras and DVRs, camera cleaning, and procedures to ensure cameras are functioning. PM for Bus Fleet cameras is performed by a contractor, and inspection results are documented on the PM inspection line card.

Rail Fleet

Rail Fleet does not have a PM policy or procedure specific to cameras. However, inspections of cameras are conducted by Rail Fleet personnel as part of daily and periodic railcar inspections. At the time of OIG's evaluation, daily and period inspection procedures were in draft form and awaiting implementation and distribution. Daily and 60-day periodic maintenance inspection procedures include visual inspection of security cameras for proper mounting, cleanliness, and clarity (unobstructed).

MetroAccess

MetroAccess does not have a preventative maintenance policy or procedure specific to cameras as DriveCam camera operation and maintenance is performed by a contractor. However, the contractor conducts daily and 30-day vehicle inspections which include verification that the camera is working, and that the camera lens is clear and properly aimed.

[14] *Installed under the Video Surveillance Preventive, Corrective, and Replacement Maintenance Services Contract and New Bus Warranty.*

Management's Response

M E M O R A N D U M

Washington Metropolitan Area Transit Authority

SUBJECT: Evaluation of WMATA's Security Cameras

DATE: June 8, 2026

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

Nicholson, Judd L.
Digitally signed by Nicholson, Judd L.
Date: 2026.06.10 12:47:34 -04'00'

Executive Vice President and Chief Infrastructure Officer – Theresa Impastato

Joseph Fowler
Digitally signed by Joseph Fowler
Date: 2026.06.08 16:41:50 -04'00'

Executive Vice President and Chief Operations Officer – Leroy Jones

Leroy M. Jones Jr.
Digitally signed by Leroy M. Jones Jr.
Date: 2026.06.11 09:32:01 -04'00'

TO: OIG – Michelle Zamarin

WMATA management has carefully reviewed the Office of Inspector General's (OIG) May 18, 2026, *Evaluation of WMATA's Security Cameras*. WMATA concurs with the findings and recommendations outlined in the report and is committed to timely corrective action to strengthen system reliability, data security, and maintenance oversight.

Immediate actions have been taken to address critical issues impacting real-time video access, and additional controls are being implemented to mitigate risk, improve accountability, and ensure sustained compliance across operations. We will provide periodic status updates on the implementation of these actions and remain committed to transparency and accountability in addressing the OIG's recommendations. Executive leadership will oversee progress to ensure timely completion and sustained compliance with operational and security standards

Finding 1 - Limitations in mSET Technology and Buses with Incompatible Camera Systems Impact Real-Time Monitoring of WMATA's Bus Fleet

Recommendation 1: Develop and implement a plan to prioritize and address deficiencies in real-time video access for cameras on the mSET system and cameras with incompatible DVR systems. This plan should include defined timelines and milestones for implementation.

Response: WMATA concurs with this finding and recommendation.

The issue was not related to the mSET software update. Joint analysis by the Video and Service Delivery and Operation (SD&O) teams determined that the service disruption resulted from bandwidth constraints on APN circuits supporting real-time

video access from the bus fleet. These constraints reduced throughput and caused intermittent retrieval failures.

In coordination with AT&T, the teams addressed the backhaul limitations. On April 14, 2026, AT&T upgraded the affected circuits from 10 Mbps to 2 Gbps. Following the upgrade, system performance stabilized, and all real-time video access issues were resolved by mid-April 2026. Over the next 90 days, WMATA will implement proactive monitoring of APN circuit utilization to detect bandwidth saturation early and establish a formal cross-team escalation protocol between Video and Digital Modernization. This approach will accelerate issue identification and resolution, strengthening operational resilience, and improving detection of network-related risks.

WMATA will also conduct an inventory-based assessment of buses equipped with incompatible DVR systems and develop a prioritized upgrade and replacement plan. The plan will include defined milestones, timelines, and regular status reporting to ensure accountability, prioritize upgrades based on operational risk, and maintain visibility into progress and potential delays.

Accountable Organizations: Digital Modernization (lead), Metro Integrated Command and Communications Center (MICC) Video Operations, in coordination with SD&O

Success Measures: Sustained real-time video availability; early detection of network saturation; completion of DVR upgrade plan

Risk if Delayed: Degradation of real-time video access impacting operational visibility and incident response

The estimated completion date for this action is: November 30, 2026

Finding 2 - Digital Modernization Cyber Security (DMCS) Has Not Fully Implemented Comprehensive Enterprise-Wide Automated Security Solutions to Protect Vulnerable Data

Recommendation 2: Review and update all mSET access levels and limit administrative access levels based on operational need

Response: WMATA concurs with this recommendation.

Management will identify and remove unnecessary or excessive administrative privileges, particularly for users whose roles do not require elevated access. Access levels will be standardized and documented to ensure consistency, accountability, and compliance with internal security control requirements. Supervisory approvals and

periodic access reviews will be implemented to strengthen governance and mitigate the risk of unauthorized access or misuse. Within the first 90 days, management will establish a recurring review process to ensure MSET access remains current and appropriate in response to personnel changes, including role changes, transfers, and separations. These actions are designed to strengthen internal controls and enhance overall system security.

Accountable Organization: Digital Modernization, Metro Integrated Command and Communications Center (MICC) Video Operations

Success Measures: All access roles reviewed and validated; administrative access limited to essential personnel

Risk if Delayed: Increased exposure to unauthorized access or misuse of sensitive data

The estimated completion date for this action is: November 30, 2026

Recommendation 3: Implement activity tracking and access logging capabilities for mSET to record and monitor user access and actions. If full logging is not feasible, document the rationale and implement compensating controls, such as periodic access reviews, system monitoring, or audit trails, that provide equivalent oversight.

Response: WMATA concurs with this recommendation.

Within the first 90 days, management will assess existing logging functionality and other critical system activities within MSET. Digital Modernization and Metro Integrated Command and Communications Center (MICC) Video Operations will coordinate with Luminator to evaluate and, where necessary, enhance audit logging capabilities, including the capture of user behavior and administrative actions.
If comprehensive activity logging cannot be achieved due to system, technical, or resource constraints, management will formally document the limitation and associated risk. To address any resulting gaps, management will implement compensating controls to ensure effective oversight and strengthen internal controls. These controls will include periodic user access reviews, supervisory monitoring of administrative activities, system-generated reporting, segregation of duties, and manual audit procedures.
Once implemented, these measures will support:

- Review and retention of audit logs
- Ongoing monitoring of reports to identify unauthorized access, inappropriate activity, or potential security concerns
- Periodic validation that user access remains appropriate and aligned with operational responsibilities.

Accountable Organizations: Digital Modernization (lead), Metro Integrated Command and Communications Center (MICC) Video Operations, Luminator.

Success Measures: Effective logging or compensating controls in place; availability of audit records for review.

Risk if Not Achieved: Limited ability to detect or investigate inappropriate system activity.

The estimated completion date for this action is: November 30, 2026

Finding 3 – Gaps Exist in the Preventive Maintenance and Inspection Records for Fixed Facilities

Recommendation 4: Update procedures to include placing completed preventive maintenance inspection records in the centralized SharePoint repository.

Response: WMATA partially concurs with this recommendation.

In accordance with our Maintenance Control Policy, Maximo serves as the Communications and Signaling centralized system of record for all preventive and corrective maintenance activities. As noted in the OIG report, Management will revise the **ESS PMI_E17000** document to clearly identify Maximo as the centralized system of record and ensure full alignment with our policy. For clarity, document **INFR-COSI-COMM-SOP-01-00** is a procedural guide that instructs maintenance personnel on how to correctly identify the specific camera or device that failed in Maximo. Its purpose is to ensure accuracy and traceability when a deficiency is discovered during a preventive maintenance inspection. Because this procedure supports corrective maintenance activities and Maximo already serves as the centralized repository, this document does not require revision to include PM inspection record retention.

Additionally, Management will reinforce the requirement that all maintenance documentation be consistently and accurately entered into Maximo to guarantee complete and reliable records.

Accountable Organization: Communications & Signaling (COSI)

Success Measures: Clear documentation of system of record; consistent and accurate maintenance record entry.

Risk if Misaligned: Data inconsistencies and reduced traceability

The estimated completion date for this action is: November 30, 2026

Recommendation 5: Ensure that preventive maintenance and inspection processes provide assurance that all cameras are included in preventive maintenance inspections for each location; records are completed and stored in the centralized repository, and corrective actions are documented.

Response: WMATA concurs with this recommendation.

Management will collaborate with Engineering to revise the preventive maintenance template to include a comprehensive checklist of all cameras at each facility. Management will also reinforce expectations for accurate completion of inspection records, proper documentation within the centralized repository, and timely initiation of corrective maintenance for any offline or defective cameras.

Accountable Organizations: COSI, Engineering

Success Measures: 100% of cameras included in inspections; complete documentation; corrective actions tracked.

Risk if Delayed: Undetected equipment issues and gaps in maintenance records

The estimated completion date for this action is: November 30, 2026

Recommendation 6: Conduct periodic compliance reviews to confirm that preventive maintenance activities are properly documented and accessible.

Response: WMATA concurs with this recommendation.

Management will perform periodic reviews to confirm that preventive maintenance inspections are completed in accordance with requirements, and that records are accurately documented and maintained in the centralized repository. These reviews will also identify documentation gaps and address any inconsistencies.

Accountable Organization: COSI

Success Measures: Verified completion and accessibility of maintenance records; closure of identified gaps.

Risk if Not Sustained: Reduced auditability and potential non-compliance

The estimated completion date for this action is: November 30, 2026

cc: Senior Executive Team
SVP & Chief Risk and Audit Officer – Elizabeth Sullivan

To 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