OFFICE OF THE
INSPECTOR GENERAL
DISTRICT OF COLUMBIA GOVERNMENT

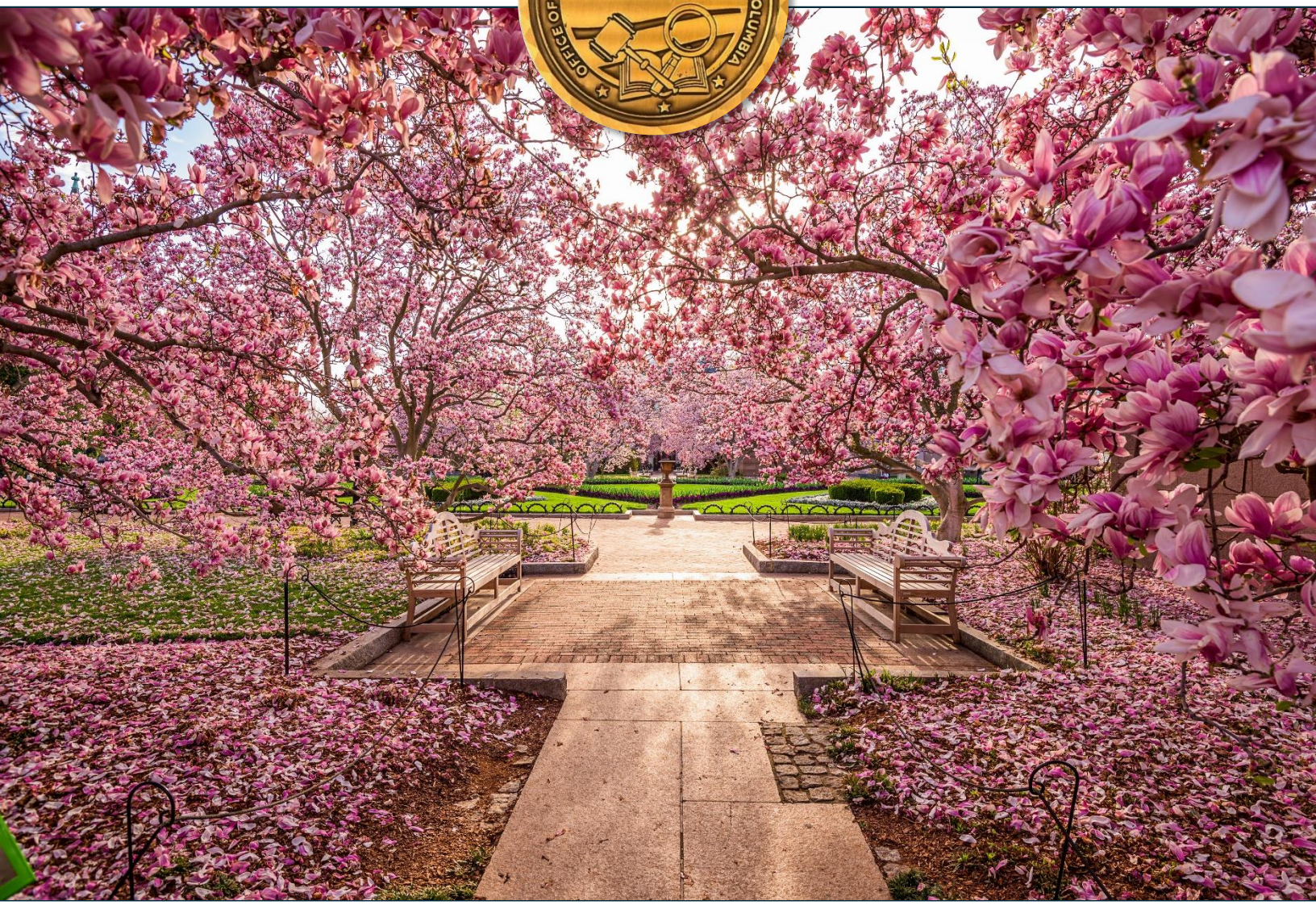
AUDIT REPORT

District of Columbia Government

Management Recommendations
Fiscal Year 2025

OIG No. 25-1-01MA(a)

January 30, 2026



DANIEL W. LUCAS
INSPECTOR GENERAL

OUR MISSION

We independently audit, inspect, and investigate matters pertaining to the District of Columbia government in order to:

- prevent and detect corruption, mismanagement, waste, fraud, and abuse;
- promote economy, efficiency, effectiveness, and accountability;
- inform stakeholders about issues relating to District programs and operations; and
- recommend and track the implementation of corrective actions.

OUR VISION

We strive to be a world-class Office of the Inspector General that is customer focused and sets the standard for oversight excellence!

OUR VALUES

Accountability: We recognize that our duty extends beyond oversight; it encompasses responsibility. By holding ourselves accountable, we ensure that every action we take contributes to the greater good of the District.

Continuous Improvement: We view challenges not as obstacles, but as opportunities for growth. Our commitment to continuous improvement drives us to evolve, adapt, and enhance our practices.

Excellence: Mediocrity has no place in our lexicon. We strive for excellence in every facet of our work.

Integrity: Our integrity is non-negotiable. We act with honesty, transparency, and unwavering ethics. Upholding the public's trust demands nothing less.

Professionalism: As stewards of oversight, we maintain the utmost professionalism. Our interactions, decisions, and conduct exemplify the dignity of our role.

Transparency: Sunlight is our ally. Transparency illuminates our processes, decisions, and outcomes. By sharing information openly, we empower stakeholders, promote understanding, and reinforce our commitment to accountability.

MEMORANDUM

To: The Honorable Muriel Bowser
Mayor of the District of Columbia

The Honorable Phil Mendelson
Chairman, Council of the District of Columbia

From: Daniel W. Lucas
Inspector General

Date: January 30, 2026

Subject: **District of Columbia Government Management Recommendations**
OIG No. 25-1-01MA(a)

This memorandum transmits the final report *District of Columbia Government Management Recommendations* for fiscal year 2025. CliftonLarsonAllen LLP (CLA) provided this report to the Office of the Inspector General as part of the annual audit of the District of Columbia's general-purpose financial statements for fiscal year 2025.

On January 23, 2026, CLA issued nineteen recommendations to improve the effectiveness of operational and programmatic internal controls. When addressed, these improvements can increase assurances that District agencies run their operations efficiently and effectively, report reliable operational information, and comply with applicable laws and regulations.

Should you have questions or concerns, please contact me or Dr. Slemo Warigon, Assistant Inspector General for Audits, at (202) 792-5684.

DISTRICT OF COLUMBIA GOVERNMENT

MANAGEMENT RECOMMENDATIONS

YEAR ENDED SEPTEMBER 30, 2025

CPAs | CONSULTANTS | WEALTH ADVISORS

CLAconnect.com

DISTRICT OF COLUMBIA GOVERNMENT
MANAGEMENT RECOMMENDATIONS
TABLE OF CONTENTS
YEAR ENDED SEPTEMBER 30, 2025

CliftonLarsonAllen LLP
CLAconnect.com

To the Mayor, Members of the Council of the District of Columbia,
Inspector General of the District of Columbia, and
Chief Financial Officer of the District of Columbia

In planning and performing our audit of the financial statements of Government of the District of Columbia (the District) as of and for the year ended September 30, 2025, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards* as promulgated by the Government Accountability Office (GAO), we considered the entity's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we do not express an opinion on the effectiveness of the entity's internal control.

However, during our audit we became aware of deficiencies in internal control other than significant deficiencies and material weaknesses and other matters that are opportunities to strengthen your internal control and improve the efficiency of your operations. Our comments and suggestions regarding those matters are summarized below. We previously provided a written communication dated January 23, 2026, on the entity's internal control, that report contains a material weakness in the entity's internal control. This letter does not affect our report on the financial statements dated January 23, 2026, nor our internal control communication dated January 23, 2026.

We will review the status of these comments during our next audit engagement. We have already discussed many of these comments and suggestions with various entity personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

Management's written response to findings have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we do not provide any assurance on the responses.

This communication is intended solely for the information and use of management, others within the organization, the Mayor and Members of the Council of the District of Columbia, the Inspector General of the District of Columbia, and the Chief Financial Officer of the District of Columbia and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
January 23, 2026

CURRENT YEAR FINDINGS AND RECOMMENDATIONS

2025-001 – Office of the Deputy Mayor for Planning and Economic Development (DMPED) – Missing Documentation on a Sole Source Procurement

During our testing of controls over the procurement award process, including controls over the sole source procurements award process, we identified one instance in which the Office of the Deputy Mayor for Planning and Economic Development (DMPED) procured professional services pertaining to the Industrial Revenue Bond Program under sole source procurement in the amount of $609,548.

We received a copy of the Determination and Findings Form (D&F), purchase requisition, and purchase order. We noted the D&F Form did not include a description of the market survey conducted or a statement of reasons why a market survey was not performed.

Section 1.2.2.F of the District of Columbia Office of Contracting and Procurement (OCP) Procurement Procedures Manual requires that the D&F Form for sole source procurements include:

> "A description of the market survey conducted and the results, including a list of the potential sources contacted by the contracting officer or which expressed, in writing, an interest in the procurement (if no market survey was done, a statement of the reasons why a market survey was not conducted."

The omission appears to be due to inadequate review or oversight during the preparation and approval of the D&F Form, resulting in non-compliance with documentation requirements.

Noncompliance with District procurement regulations and statute (27 DCMR § 1700; D.C. Official Code § 2 354.04), exposing the District to legal, oversight, and financial reporting risks.

The D&F Form sets forth the justification for sole source procurements. Failure to include the required market survey information in the D&F Form reduces transparency and may limit assurance that the sole source procurement was properly justified. This could increase the risk of non-compliance with procurement regulations and undermine public confidence in the integrity of the procurement process.

Recommendation

We recommend that the DMPED, in coordination with OCP, strengthen controls over the preparation and review of D&F Forms to ensure compliance with Section 1.2.2.F of the Procurement Procedures Manual, including:

- Implement a checklist or automated validation step to confirm inclusion of market survey details or justification for its omission before approval.
- Provide refresher training to procurement staff on documentation requirements for sole source procurements.

Management Response

Management concurs with the finding. The finding is in accordance with 27 DCMR. However, a supplemental D&F may be prepared and posted in accordance with Title 27 DCMR § 1700.2 and D.C. Code § 2–354.04.

2025-002 – Department of Motor Vehicles (DMV) – Inappropriate Use of an Emergency Procurement Provision

During our testing of controls over the procurement award process, including controls over the emergency awards process, we identified one instance in which the Department of Motor Vehicles (DMV) procured traffic violation ticket processing services under emergency procurements in the amount of $5,156,650.

We received a copy of the Determination and Findings Form (D&F) purchase requisition, and purchase order. We noted, the contract had a period of performance from January 29, 2025 to May 29, 2025 (120 days). The same vendor provided identical services under a prior emergency contract with a period of performance from October 1, 2024 to January 28, 2025. There was no development time required for the goods or services to justify exceeding the 90-day limit applicable to emergency procurements.

27 DCMR § 1702.7: “Emergency procurement procedures shall not be used for contracts exceeding ninety (90) days; provided that if the development time for the goods or services exceeds ninety (90) days, the contract shall not exceed one hundred twenty (120) days.”

Procurement Practices Reform Act (PPRA) § 405(d), codified at D.C. Official Code § 2-354.05(d): “Emergency procurement procedures shall not be used for contracts exceeding 90 days; provided, that if the development time for the good or service exceeds 90 days, the contract shall not exceed 120 days.”

Procurement Practices Reform Act (PPRA) § 202(a)(1), codified at D.C. Official Code § 2-352.02(a)(1) and (d): “Before the award of a multiyear contract or a contract in excess of $1 million during a 12-month period, the Mayor or executive independent agency or instrumentality shall submit the proposed contract to the Council for review and approval… [and] no proposed multiyear contract and no proposed contract in excess of $1 million for a 12-month period shall be awarded until after the Council has reviewed and approved the proposed contract[.]”

Planning gap and reliance on emergency method for ongoing, routine services: DMV used consecutive emergency contracts to cover sustained operational needs instead of initiating a timely competitive procurement.

Misinterpretation of the “development time” exception: Staff appear to have applied the 120-day allowance without a qualifying development need for the service.

Insufficient pre-award compliance review: The approval process did not identify and prevent an emergency contract duration inconsistent with statutory limits. Controls did not prevent award/ execution before District Council approval for a contract exceeding $1 million.

Noncompliance with District procurement regulations and statute (27 DCMR § 1702.7; D.C. Official Code §§ 2-354.05(d) and 2-352.02(a)(1), (d)), exposing the District to legal, oversight, and financial reporting risks.

Reduced competition and transparency, which may result in unfavorable pricing or value for money compared to a properly competed award.

Precedent for improper use of emergency procedures, undermining public confidence in the integrity of the procurement process.

Recommendation

We recommend that DMV, in coordination with OCP, strengthen controls over the emergency procurement process, including:

- Cease use of emergency procedures for routine, ongoing services and initiate a full and open competitive procurement (e.g., issuing an RFP) for traffic ticket processing services prior to the expiration of any temporary or bridge arrangements.

- Strengthen pre-award compliance checks by instituting a mandatory duration-limit validation aligned to 27 DCMR § 1702.7 and PPRA § 405(d), with documented review by procurement/legal prior to approval of any emergency procurement.

- Clarify and train staff on the narrow "development time" exception, including examples of what does/does not qualify, and require affirmative documentation in the emergency procurement when invoking the 120-day allowance.

- Implement a tracking dashboard for emergency procurements that flags cumulative durations and back-to-back emergency awards for the same requirement, triggering leadership review.

- Use competitively awarded bridge or short-term vehicles (where applicable) instead of emergency procedures when the need is foreseeable but the competitive award is pending.

- Establish an automated hold in the procurement system that prevents award/execution until District Council approval is recorded. Ensure the contract file contains evidence of submission and approval under § 2-352.02.

Management Response

Management does not concur with this finding and believes the matter is better suited for policy review and clarification, as opposed to a control deficiency requiring corrective action.

2025-003 – Department of Human Services (DHS) – Missing Documentation Related to a Certificate of Clean Hands

During our testing over procurement, we tested controls over the procurement award process, including compliance with the Procurement Procedures Manual, issued by the Office of Contracting and Procurement (OCP). OCP procured, on behalf of the Department of Human Services (DHS), maintenance and support services for existing software in the amount of $236,946 without obtaining a Certificate of Clean Hands from the vendor.

We received a copy of the purchase requisition, purchase order, and receipt noting that for this contract, OCP did not obtain a Certificate of Clean Hands from the vendor to evidence District tax compliance prior to award. The Certificate of Clean Hands issued by District's Office of Tax and Revenue is the District's standard mechanism to verify vendors are compliant with District tax filing and payment requirements when seeking District contracts.

Additionally, we noted that that the transaction was improperly entered into the Procurement Automated Support System (PASS) as a 'sole source' procurement rather than as an 'exempt from competition' procurement.

Pursuant to 27 DCMR § 2204, contracting officers are required to make an affirmative determination of responsibility prior to award, which includes obtaining a Certificate of Clean Hands for contracts exceeding $100,000. Clean Hands confirms that a prospective contractor has complied with District tax filing requirements and have paid taxes due to the District or are compliance with an approved payment agreement with OTR and DOES.

The Procurement Procedures Manual, Section 2.3.2 D stipulates that the contract specialist is responsible for obtaining evidence of the applicant's compliance with District laws and regulations by obtaining a Certificate of Clean Hands from the Office of Tax and Revenue, among other forms and verifications.

OCP's system controls did not require upload/verification of a current Certificate of Clean Hands before award. Staff may have been unaware that a Certificate of Clean Hands verification is the standard method to document tax compliance and support eligibility for District contracts, or relied on other documents that do not satisfy the Certificate of Clean Hands requirement.

Staff selected the wrong procurement method in PASS, classifying the action as 'sole source' instead of the appropriate 'competition exemption' for software maintenance/support.

Awarding a contract without a Certificate of Clean Hands risks noncompliance with the District's Clean Hands mandate and the Procurement Procedures Manual. The District may contract with a vendor that is not current on District taxes or filings, which can lead to payment holds, offsets, administrative burden to cure after award, and reputational impacts undermining public confidence in the integrity of the procurement process.

Misclassification of procurements may result in improper or unnecessary forms, verifications and posting artifacts while omitting the exemption justification that Procurement Practices Reform Act requires, creating file inconsistency with the governing method.

Recommendation

We recommend that OCP strengthen controls over the emergency procurement process, including:

- Reinforcing established pre-award documentation applicable, and ensuring PASS procurement method classifications are accurate prior to award and purchase order issuance. Conduct spot checks to confirm evidence is retained.

- Provide short, role-based training on the Certificate of Clean Hands mandate, how to request/verify certificates, and when the requirement applies, as well as the importance of properly classifying procurement activities within PASS.

Management Response

Management concurs with the finding and will implement the recommended corrective actions.

2025-004 – Office of the Chief Technology Officer (OCTO) – Account Management Lifecycle

We identified several items related to account management including:

- Dormant or inactive accounts that have not been used in over 6 months and were not disabled: 483 Peoplesoft

- 2,047 separated users with active accounts in Peoplesoft

OCTO Identification and Authentication Policy: The Districts agencies must manage information system identifiers by: Disabling the identifier after 6 months of inactivity.

OCTO Personnel Security Policy: District agencies must, upon an individual's separation from the District workforce: Disable user's information system access on the employee's last workday.

Without disabling inactive and separated users' account access to District systems and applications, DC is at risk of allowing excessive or unauthorized access to information systems and data.

DC Manages several thousand internal and external facing applications which makes it difficult to maintain fidelity over account management across the entire portfolio as personnel changes such as transfers and separations take place.

Recommendation

We recommend OCTO work with Agency IT and system owners to implement improved account management controls and processes including for the control of inactive accounts and removal of access for separated users.

Management Response

Management concurs with finding. The OCTO Directory Services team is currently implementing a new Identity Management platform designed to automate user provisioning and deprovisioning in alignment with established policy. The solution is in the testing phase and is scheduled to go live in December 2025.

2025-005 – Office of the Chief Technology Officer (OCTO) - Configuration Baseline Implementation and Enforcement

In review of the configuration management capabilities in place for OCTO supported systems we noted 30,000 devices were tracked and monitored for configuration standards; however, OCTO was only able to implement configurations and push updates to server platforms. Other devices such as end user systems were the responsibility of the system owner/Agency IT. Additionally, we noted 56,000 critical and high severity compliance findings present on the network as reported by the scanning tool currently in place. We were informed the tracking of configuration and remediation process was primarily focused on security patches and configuration updates for servers only.

OCTO Configuration Management Policy:

> All District agencies must:
>
> 4.4.1. Establish and document configuration settings for information technology applications and technologies deployed within their information system in accordance with Center for Internet Security (CIS) benchmarks for servers and network devices as part of configuration files that reflect the most restrictive mode consistent with operational requirements.
>
> 4.4.2. Implement the configuration settings.

Without consistently implementing and enforcing baseline standards on end user devices, the District is at risk of operating potentially vulnerable or insecure systems increasing the possibility of unauthorized access to or modification/destruction of data.

Policy and baseline standards are set and monitored via automated capabilities by OCTO, however, the responsibility for implementation and enforcement of the standards are the responsibility of each specific agency. OCTO was performing configuration updates for server systems.

Recommendation

We recommend OCTO work with District officials and agency IT support to further implement existing capabilities for monitoring the technical environment for configuration weaknesses and security vulnerabilities including on district workstations.

Management Response

Management concurs with finding. Multiple OCTO teams are actively working across their respective platforms (servers and workstations) to implement compliance standards aligned with CIS benchmarks. In addition, the OCTO Endpoint Management team is collaborating with a partner to deploy third-party patching solutions that address non-security critical and high-priority patches across all endpoints.

2025-006 – Office of the Chief Technology Officer (OCTO) - Enforcement of Risk Management Framework Policy

While OCTO Policies have been established utilizing the NIST Standards and Guidelines such as Special Publication 800-53 and 800-37 (The Risk Management Framework), we noted that several key elements documented in these guides and policies have not been fully implemented throughout the DC government portfolio of systems and applications.

These processes include formal system categorization, formal documented risk assessments (outside of cyber risks), and continuous monitoring assessments evaluating the implementation of controls for DC systems.

OCTO Risk Assessment Policy:

> District's agencies must:
>
> 4.1.1. Categorize information and the system per applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. District's agencies must:
>
> 4.2.1. Conduct assessments of risks, including the likelihood and magnitude of the harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. OCTO Security Assessment and Authorization Policy: District agencies must ensure that risk monitoring is an integral part of the I continuous monitoring strategy that includes the following:
>
> 4.6.1. Controls effectiveness monitoring.
>
> 4.6.2. Compliance monitoring.
>
> 4.6.3. System change monitoring.

Without fully implementing and enforcing policy defined risk management functions, DC is at risk of operating systems and applications with unknown and unmanaged security weaknesses or vulnerabilities.

The District operates a significant portfolio of internal and external facing applications and there is not a standardized process in use at the agencies for documenting and managing systems risks and categorizations in accordance with policy.

Recommendation

We recommend OCTO work with Agency leadership and governance to ensure that risk management processes and controls are implemented to the level feasible throughout the portfolio of DC systems and applications to comply with documented OCTO policy.

Management Response

Management concurs with the finding. OCTO has been approved for funding under the State and Local Cybersecurity Grant Program (SLCGP), which will be utilized to implement the Risk Assessment policy and conduct initial assessments of DC agencies under the authority of the Mayor.

2025-007 – Office of the Chief Technology Officer (OCTO) – Unsupported Systems

We noted several unsupported operating systems in the District server inventory (845 systems at RHEL 7 or lower and Windows 2012 or 2008).

OCTO System and Services Acquisition Policy: The District agency must replace systems and/or components when support for the components is no longer available from the developer, vendor, or manufacturer.

Without updating or removing unsupported platforms, DC is at risk of allowing vulnerable systems to operate within their environment increasing the possibility of unauthorized access, destruction, or removal of sensitive data.

District agencies procured system platforms to support specific applications or services but did not plan for the ultimate upgrade or decommission of the platform hosting the application.

Recommendation

We recommend OCTO work with agencies and system owners to update or decommission systems and applications running on unsupported versions of operating systems.

Management Response

Management concurs with this finding. OCTO Security already performs the task of identifying End-of-Life (EOL) machines on the network and coordinates with agencies *to* update or decommission these systems. The EOL list is compiled, presented, and shared with CIOs, and we provide migration support when needed. This information is tracked and reported weekly through our established process.

2025-008 – Office of the Chief Technology Officer (OCTO) – Formal Contingency or Disaster Recovery Plans

We noted that OCTO performed an exercise testing the recovery capability of their network, however, we have not received evidence of a formal network Contingency/Disaster Recovery plan that complies with OCTO policy including documenting essential mission functions, recovery time and point objectives, and is reviewed and approved by senior management.

OCTO Contingency Planning Policy: All District agencies must:

Requirement: 4.1.1. Develop a contingency plan for the information system that:

- Identifies essential missions, business functions, and appropriate contingency requirements.
- Provides recovery objectives, restoration priorities, and metrics.
- Addresses contingency roles, responsibilities, and outlines the assigned individuals with contact information.
- Addresses the maintenance of essential missions and business-critical functions during an information system disruption, compromise, or failure.

- Addresses full information system restoration without deterioration of security safeguards originally implemented.

- Is reviewed by Agency ISOs and approved by senior management.

Without formal, documented contingency and recovery plans, OCTO is at risk of being unprepared for real-world system outages or disruption events or not being able to recover systems and applications within stated objective timeframes.

OCTO has established resiliency controls and recovery capabilities for network infrastructure but not yet formally documented plans describing all elements and recovery objectives as required by policy.

Recommendation

We recommend that OCTO document a formal Contingency and Recovery plan for their systems and networks to comply with policy.

Management Response

Management concurs with the finding, however developing and maintaining Contingency and Recover Plan for every application is not feasible. We think that we need a Contingency and Recover Plan for all Critical and important OCTO applications and the Datacenters.

2025-009 – Office of the Chief Financial Officer (OCFO) – **Account Management Lifecycle**

We identified several items related to account management including:

- Dormant/inactive accounts that have not been used in over 6 months and were not disabled: 434 DIFS, and 30 OCFO AD

OCTO Identification and Authentication Policy, Section 4.5.5: The Districts agencies must manage information system identifiers by: Disabling the identifier after 6 months of inactivity.

OCTO Personnel Security Policy, Section 4.3.1: District agencies must, upon an individual's separation from the District workforce: Disable user's information system access on the employee's last workday.

Without disabling inactive and separated users account access to District systems and applications, DC is at risk of allowing excessive or unauthorized access to information systems and data.

After the transition to DIFS the primary focus was on ensuring individuals across DC government were provisioned with appropriate access. OCFO had not yet established a formal policy requiring the review and disablement of accounts after a period of inactivity. Additionally, the legacy mainframe system had a technical control to accomplish this process while the new application does not yet have that functionality.

Recommendation

We recommend OCFO establish a formal policy for account inactivity and implement review procedures to ensure that individuals with privileges above standard employees in their applications have their accounts removed after a designated period of inactivity.

Management Response

Management concurs with the finding. During the FY 26 annual security review, user access will be reviewed to determine that dormant users (180 days or greater) will be inactivated in the DIFS system. Further, we will review to ensure terminated users are also inactivated in the system.

The DIFS Security Access Policy will be reviewed and updated to include a dormant user policy. Further, procedures will be implemented to ensure terminated employees are inactivated in a timely manner.

2025-010 – Department of General Services (DGS) – Unidentified Leases

During our testing of lease additions and modifications, we noted multiple instances in which lease transactions executed in FY2024 were not recorded until FY2025:

- Lessor: one (1) lease abatement executed September 26, 2024, was recorded in FY2025, resulting in a $53,412,051 overstatement of lessor activity in FY2025.

- Lessee: 9 lease agreements executed between October 1, 2023, and September 24, 2024, were recorded in FY2025, resulting in a $14,014,278 overstatement of lessee activity in FY2025. 2 lease amendments executed on between February 11, 2024, and September 23, 2024, were recorded in FY2025, resulting in a $47,811,517 overstatement of lessee activity in FY2025.

Accounting principles generally accepted in the United States (GAAP) requires a lessee to recognize a lease liability and right-to-use asset at the commencement of the lease term; and a lessor to recognizes a lease receivable and deferred inflow of resources at commencement. Amendments that change consideration or terms (e.g., abatements) are lease modifications (or terminations, if the right-of-use decreases) and require remeasurement in the period of the amendment rather than deferral to a later fiscal year. Recording leases in a later fiscal year than commencement results in period misstatements.

Lease documents from the Department of General Services (DGS) did not reach the Office of the Chief Financial Officer timely, and no automated linkage existed between execution dates and the lease accounting database. Insufficient controls and reconciliations between the lease repository/contract management system and EZ Lease allowed FY2024 events to be booked in FY2025.

In the aggregate, FY2025 lessee activity was overstated by $62,213,804 and lessor activity was overstated by $53,412,051 due to a misstatement of FY2024 balances and activity were understated and lease note disclosures were potentially misstated due to cutoff errors relative to GAAP recognition requirements.

Recommendation

We recommend that DGS program management, in coordination with the Office of the Chief Financial Officer:

- Strengthen year-end cutoff controls by implementing a year-end lease cutoff checklist requiring (a) written confirmations from agencies executed through fiscal year-end, and (b) reconciliations of EZLease to the GL before close, with management sign-off.

- Automate intake-to-GL workflow. Configure the EZLease (or DIFS/related modules) to require key dates (execution/commencement, modification date) and block posting into a subsequent fiscal year when commencement is in a prior year; enable alerts for unrecorded executed leases.

- Update the District's lease accounting policy to:

    - Require recognition at commencement for lessee/lessor leases and timely remeasurement for modifications/abatements.

    - Define documentation deadlines (e.g., within 10 business days of execution/commencement) and roles for agencies forwarding executed agreements to OFOS.

    - Provide annual training to agency controllers and contract administrators on lease requirements and cut-off expectations.

Management Response

Management concurs with finding. Lessor condition – One DGS/AM0 lease amendment (Total recorded in FY25 $53.4M) We concur that there was a time lag in the flow of information and related documents from DGS Portfolio Management Division to the OCFO Accounting department. This has caused a delayed recording of accounting effect of lease amendment. To remediate this issue going forward

(a) DGS Portfolio Management Division will ensure lease related documents and reports are submitted to DGS Accounting within 5-10 business days of document execution date.

(b) On a quarterly basis and a month before the fiscal year closes DGS Accounting will send email reminders requesting for active lease report, new lease report and amendment reports. All reports will require PMD management certification for accuracy and completeness.

Lessee condition – 5 (not 9) DGS/AM0 new leases (Total $12.6M): 2 DGS/ AM0 Amendments (Total $47.8M) We concur that there was a time lag in the flow of information and related documents from DGS Portfolio Management Division to the OCFO Accounting department. This has caused a delay in recording the accounting effect of new leases and amendments in the year the documents were executed. To remediate this issue going forward

(a) DGS Portfolio Management Division will ensure lease related documents and reports are submitted to DGS Accounting within 5-10 business days of document execution date.

(b) On a quarterly basis and a month before the fiscal year closes DGS Accounting will send email reminders requesting for active lease report, new lease report and amendment reports. All reports will require PMD management certification for accuracy and completeness.

DISTRICT OF COLUMBIA GOVERNMENT
MANAGEMENT RECOMMENDATIONS
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATION
YEAR ENDED SEPTEMBER 30, 2025

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

The following chart outlines the status of the two prior year management recommendations that were not fully implemented as of September 30, 2025.

Management Recommendations

Finding Number	**Recommendations**	**Status**
2018-03	**Office of the Chief Technology Officer (OCTO)** - Implement a Risk Management Framework to Comply with National Institute of Standards and Technology (IST) Publication 800-37	This finding is repeated as finding number 2025-006.
2024-02	**Office of the Chief Financial Officer (OCFO)** - We recommend OCFO to follow their procedures and implement controls to help prevent/deter fraudulent access to their systems.	OCFO has implemented three out of four corrective actions.

[This page is intentionally blank.]

REPORT WASTE, FRAUD, ABUSE, AND MISMANAGEMENT

(202) 724-TIPS (8477) and (800) 521-1639

https://oig.dc.gov

oig@dc.gov

STAY UP TO DATE

instagram.com/OIGDC

x.com/OIGDC

facebook.com/OIGDC

Sign-up for email/text updates from OIG