OFFICE OF THE
INSPECTOR GENERAL
DISTRICT OF COLUMBIA GOVERNMENT

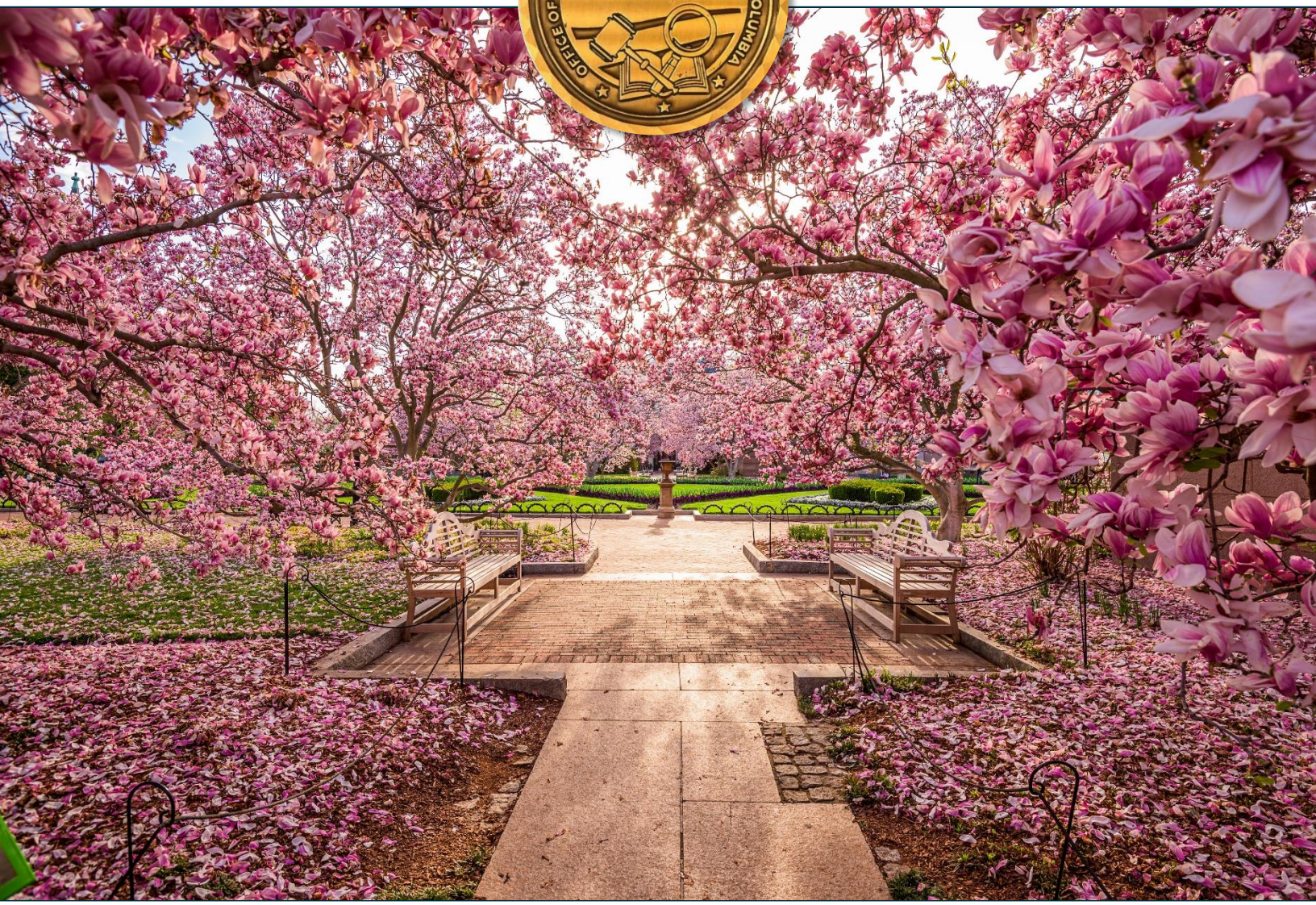
AUDIT REPORT

Office of Lottery and Gaming

Management Recommendations
Fiscal Year 2025

OIG No. 25-1-09DC(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: **Office of Lottery and Gaming Management Recommendations**
OIG No. 25-1-09DC(a)

This memorandum transmits the final report *Office of Lottery and Gaming 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 2, 2026, CLA issued a management letter noting nine control deficiencies discovered during the audit. While there were not significant deficiencies or material weaknesses, CLA provided nine recommendations to enhance the fund's internal controls and improve operational efficiency.

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

CliftonLarsonAllen LLP
CLAconnect.com

Management
Office of Lottery and Gaming
Washington, D.C.

In planning and performing our audit of the financial statements of the Office of Lottery and Gaming (the Lottery) as of and for the year ended September 30, 2025, in accordance with auditing standards generally accepted in the United States of America, 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 these matters are summarized below. This letter does not affect our report on the financial statements dated January 2, 2026, nor our internal control communication dated January 2, 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 responses to the above deficiencies 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 of the Office of Lottery and Gaming, and others within the District of Columbia Government, 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 2, 2026

CURRENT YEAR FINDINGS AND RECOMMENDATIONS

2025-001: Backup Restore Testing

No tests were performed for the restore capability of backup data within the period under review. This lack of periodic testing means that, in the event of a system outage or service disruption, there is a risk that data may not be readily recoverable, potentially impacting the continuity of operations.

The OCTO Contingency Planning Policy requires all District agencies to conduct backups of user-level information on a daily, weekly, or monthly basis, consistent with established recovery time and recovery point objectives. Backup data must be retained for up to four weeks and safeguarded to ensure its confidentiality, integrity, and availability at designated storage locations. These requirements are intended to support timely and reliable data recovery in the event of system disruptions or failures.

Without periodic testing to confirm that backup data can be successfully restored, OLG faces an increased risk that critical information may not be readily available when needed. In the event of an actual system outage or service disruption, the inability to restore data promptly could hinder operations and delay recovery efforts, potentially impacting business continuity.

The primary cause of this issue was resource constraints during the review period, which prevented the performance of a dedicated backup restoration exercise. As a result, management was unable to validate the effectiveness of existing backup procedures through testing, despite the presence of established backup processes.

Recommendation:
We recommend that DC Lottery implement procedures for periodically testing the restore capability of their system and application backup data.

Management Response:
Management concurs. By February 28, 2026, OLG will implement and document a standardized backup restore testing process, including scope, results, and retained evidence.

2025-002: Disaster Recovery Testing

There was no evidence of a formal test or exercise of the ICS Disaster Recovery Plan during the period. Although management indicated that an exercise was performed, no formal documentation, such as lessons learned or an after-action report, was maintained. This absence of documentation could hinder the organization's ability to fully recover systems and applications within the required recovery timeframes in the event of a disruption.

The OCTO Contingency Planning Policy requires all District agencies to coordinate contingency plan testing with relevant District departments and responsible groups. Agencies must test their information system contingency plans at least annually using appropriate methodologies, such as tabletop exercises, to evaluate the effectiveness of the plans and organizational readiness to execute them. Copies of test reports documenting the results of these exercises must be provided to District agencies to support oversight and accountability.

Without regularly testing contingency and disaster recovery plans and maintaining formal documentation—such as after-action reports or lessons learned—OLG is at risk of being unable to fully recover systems and applications during a real-world disruption. This gap could result in delays or failures to meet established recovery timeframes, potentially impacting operations and service delivery.

Management indicated that a contingency exercise was conducted during the period; however, no formal documentation was maintained. Specifically, supporting materials such as an after-action report or documented lessons learned were not prepared, limiting the ability to demonstrate compliance with policy requirements or assess the effectiveness of the exercise.

Recommendation:
We recommend that DC Lottery management implement documented procedures for performing exercises of the Disaster Recovery capability and maintain documentation of the results.

Management Response:
Management concurs. By February 28, 2026, OLG will formalize disaster recovery testing documentation, including results, lessons learned, and corrective action tracking.

2025-003: Multi-Factor Authentication (MFA) for ICS

Multi-factor authentication is not enforced for remote access to the ICS application, which is accessed through domain-joined jump box servers. The lack of MFA increases the risk of account compromise and unauthorized access, removal, or destruction of sensitive data.

The OCTO Identification and Authentication Policy requires District agencies to enforce multi-factor authentication (MFA) for network access to information systems, including access by non-privileged accounts. This requirement is intended to strengthen authentication controls and reduce reliance on single-factor credentials when accessing District systems and applications.

Without implementing MFA for application access, OLG is exposed to an increased risk of account compromise and unauthorized access. This heightened risk could lead to the improper access, removal, or destruction of sensitive data, potentially affecting the confidentiality and integrity of information maintained within the system.

The underlying cause of this issue is that the ICS application is a legacy system that may not support MFA functionality. As a result, technical limitations may prevent the implementation of MFA without system upgrades, enhancements, or compensating controls.

Recommendation:
We recommend DC Lottery management implement Multi-Factor Authentication for access to the ICS application.

Management Response:
Management concurs. By August 31, 2026, OLG will enforce multi factor authentication for ICS administrative access in coordination with Elsym and Intralot, informed by penetration test results.

2025-004: ICS User Access Authorization Documentation

Evidence of access approval and authorization was not provided for two out of three ICS users sampled during the audit. Management indicated that these users had been in the system prior to the implementation of the current approval documentation process. The absence of documented access authorizations increases the risk of excessive or unauthorized access to application data, resources, and processes.

The OCTO Access Control Policy requires District agencies to formally define and document authorized users for each system, including group and role membership, access authorizations, and other relevant account attributes. The policy also requires that requests to create system accounts receive appropriate approval from organization-defined personnel or roles. In addition, agencies must review user accounts at least annually to ensure continued compliance with account management requirements.

Without properly documenting and maintaining system access authorizations, OLG is at risk of permitting excessive or unauthorized access to application data, resources, and processes. Inadequate access controls increase the likelihood that users may retain access beyond their job responsibilities, potentially compromising the confidentiality, integrity, or availability of system information.

The cause of this condition is that some sampled users were provisioned prior to the implementation of the current access request and approval process. As a result, formal access reviews or recertifications for these users were not performed or documented, limiting management's ability to verify the appropriateness of existing system access.

Recommendation:

We recommend that DC Lottery implement formal, documented procedures for the authorization and periodic review and approval of system users.

Management Response:

Management concurs. By February 28, 2026, OLG will implement documented ICS access approval and retention procedures pending tooling integration with external vendors.

2025-005: ICS Periodic User Access Review

There was no evidence of a periodic review or recertification of ICS user access. Management stated that user accounts are reviewed periodically as updates are made to the system, but no formal documentation was available. Without periodic and documented reviews, there is a risk that excessive, unneeded, or unauthorized privileges may persist on user accounts.

The OCTO Access Control Policy requires District agencies to review system user accounts at least annually to ensure compliance with established account management requirements. These reviews are intended to confirm that access remains appropriate based on users' roles and responsibilities and that accounts are properly managed throughout their lifecycle.

Without performing and documenting periodic access reviews and recertifications, OLG is at risk of allowing excessive, unnecessary, or unauthorized privileges to persist on user accounts. Such conditions increase the likelihood of inappropriate access to system resources and data, potentially compromising security and internal controls.

Management indicated that user accounts are reviewed periodically as system updates occur; however, formal documentation of these reviews was not provided. As a result, there is limited evidence to demonstrate that access reviews are performed consistently or in accordance with policy requirements.

Recommendation:
We recommend that DC Lottery implement formal, documented procedures for the authorization and periodic review and approval of system users.

Management Response:
Management concurs. By September 30, 2026, OLG will execute and document periodic (quarterly bi-annual) ICS access reviews using JIRA workflows and vendor supported reporting, and remediate identified exceptions.

2025-006: Inactive Accounts Not Disabled

Inactive accounts were found in the ICS application that had not been disabled. The presence of such accounts increases the risk of excessive or unauthorized access to information systems and data, particularly if these accounts are not monitored or managed in accordance with policy.

The OCTO Identification and Authentication Policy requires District agencies to manage information system identifiers by disabling user accounts after six months of inactivity. This requirement helps ensure that access to systems is limited to active, authorized users and supports effective account lifecycle management.

Without disabling inactive user accounts in a timely manner, OLG is at risk of allowing excessive or unauthorized access to information systems and data. Dormant accounts may be more vulnerable to misuse or compromise, increasing the potential for unauthorized system access and data exposure.

The cause of this condition is that the ICS application is a legacy system that may not support automated mechanisms for disabling inactive accounts. As a result, account deactivation may rely on manual processes or system limitations that hinder consistent enforcement of policy requirements.

Recommendation:
We recommend that DC Lottery implement procedures for the identification and timely disablement of inactive accounts in accordance with OCTO policy.

Management Response:
Management concurs. By August 31, 2026, OLG will implement an ICS account lifecycle process covering provisioning and deprovisioning using JIRA workflows and vendor supported integrations.

2025-007: Unsupported Operating Systems

There were fifteen servers running the Windows 2012 operating system, which is no longer supported by the vendor. Operating unsupported platforms exposes the organization to increased risk of vulnerabilities, which could lead to unauthorized access, destruction, or removal of sensitive data.

The OCTO System and Services Acquisition Policy requires District agencies to replace systems or system components when vendor, developer, or manufacturer support is no longer available. This requirement is intended to ensure that District systems remain maintainable, secure, and capable of receiving necessary patches, updates, and technical support throughout their lifecycle.

Without updating or removing unsupported platforms, OLG is at increased risk of allowing vulnerable systems to continue operating within its environment. Unsupported systems may contain unpatched security weaknesses, increasing the likelihood of unauthorized access, data destruction, or the removal of sensitive information.

The underlying cause of this issue is that certain applications or services currently in use at OLG depend on outdated platforms. To date, formal measures have not been implemented to upgrade or decommission these systems, resulting in continued reliance on unsupported technologies.

Recommendation:
We recommend OLG IT work with system owners to update or decommission systems and applications running on unsupported versions of operating systems.

Management Response:
Management concurs. By April 31, 2026, OLG will complete licensing and staged upgrades of Windows server platforms or formally decommission unsupported systems to establish a supported baseline.

2025-008: IT Risk Assessment

There was no formal, documented IT risk assessment. While scans and other assessments are performed to identify cyber risks on network-connected endpoints, a broader, more formal overarching risk assessment was not performed. This gap increases the risk of operating systems and applications with unknown and unmanaged security weaknesses or vulnerabilities.

The OCTO Risk Assessment Policy requires District agencies to categorize information systems and the information they process in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Agencies must also conduct comprehensive risk assessments that consider both the likelihood and potential magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and data. In addition, the OCTO Security Assessment and Authorization Policy requires agencies to integrate risk monitoring into their continuous monitoring strategies, including control effectiveness monitoring, compliance monitoring, and system change monitoring.

Without fully implementing and enforcing policy-defined risk management and continuous monitoring functions, OLG is at risk of operating systems and applications with unknown or unmanaged security weaknesses or vulnerabilities. The absence of a formalized, comprehensive risk assessment framework limits management’s ability to proactively identify and address emerging risks, potentially exposing systems to security threats that go undetected.

While scans and other targeted assessments are performed to identify cybersecurity risks on network-connected endpoints, a broader and more formal enterprise-level risk assessment was not conducted. As a result, risk identification and management efforts remain fragmented, reducing visibility into systemic risks that could affect the security and reliability of OLG's information systems.

Recommendation:
We recommend that DC Lottery implement and document a formal process to assess and document IT and operational risks and their responses in accordance with defined OCTO policy.

Management Response:
Management concurs. By May 31, 2026, OLG will complete a third party risk assessment based on the stabilized environment and update the enterprise risk register accordingly.

2025-009: ICS Penetration Testing

No penetration test had been conducted for the ICS application. While scans and other assessments are performed to identify cyber risks, the absence of a specific penetration test means that code weaknesses and vulnerabilities may not have been identified or managed, increasing the risk to the organization.

The OCTO Risk Assessment Policy requires District agencies to monitor and scan for vulnerabilities across all District-owned systems, hosted applications, and network devices on at least an annual basis, as well as following system changes or upgrades. This requirement also includes identifying and reporting newly discovered vulnerabilities that could potentially affect system security, ensuring risks are addressed in a timely manner.

Without performing penetration testing on application environments, OLG is at risk of operating systems that contain code weaknesses and application-level vulnerabilities that have not been identified or properly managed. Such vulnerabilities may not be detected through standard scanning alone and could increase the likelihood of security incidents or system compromise.

While scans and other assessments are conducted to identify cybersecurity risks on network-connected endpoints, a more targeted penetration test of the ICS application was not performed. As a result, application-specific vulnerabilities may remain unaddressed, limiting OLG's ability to fully assess and mitigate risks within the application environment.

***Recommendation*:**
We recommend DC Lottery periodically perform enhanced security assessments such as penetration tests for key applications to ensure key security weaknesses are identified and remediated in a timely manner.

Management Response:
Management concurs. By June 30, 2026, OLG will complete a third party ICS focused penetration test and document prioritized remediation actions aligned to validated residual risk.

[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