VIRGINIA LOTTERY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2022

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Lottery as of and for the year ended June 30, 2022, and issued our report thereon, dated October 31, 2022. Our report is included in the Virginia Lottery's Annual Report that it anticipates releasing in December 2022.

Our audit of the Virginia Lottery for the year ended June 30, 2022, found:

- the financial statements are presented fairly, in all material respects;
- four internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- four instances of noncompliance or other matters required to be reported under Government Auditing Standards.

– TABLE OF CONTENTS –

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Ensure System Access Adheres to Principles of Least Privilege
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

The Virginia Lottery's (Lottery's) management needs to strengthen system access controls over its financial accounting and reporting system (system) to ensure individuals' access adheres to the principle of least privilege. During our review of a sample of 11 system users, we identified ten users with the ability to modify the system's workflow process. The Commonwealth's Information Security Standard, SEC 501 (Security Standard), requires an organization to employ the principle of least privilege when granting access to ensure users only have the minimum access that is necessary to accomplish their assigned tasks. The Security Standard also requires Lottery to segregate duties of individuals as necessary to prevent unauthorized activity (Security Standard sections: AC-5 Separation of Duties and AC-6 Least Privilege).

Workflows represent the automated parts of a business process that coordinates various human activities, system activities, or both, to achieve a particular system outcome. Workflow controls within Lottery's system also help to ensure system users uphold the principle of least privilege by not allowing a user to approve their own transactions or deviate from a prescribed procedure (i.e., requiring higher levels of management approval for transactions over a certain threshold). Lottery uses workflows as a mitigating control to manage risk that exists within certain system users' access profiles, hence, inappropriate access to modify workflows could allow a user to circumvent this system control.

Lottery upgraded its system during the fiscal year. During this transition, Lottery assigned users default roles which allow users to modify aspects of certain workflow processes. Lottery is working to limit the ability to modify workflow access to system administrators only. Lottery should continue to evaluate all assigned roles within each system user profile to ensure it adheres to the principle of least privilege.

Improve Virtual Private Network Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Lottery does not define certain controls and processes within its policies, procedures, and baseline configuration that manage its Virtual Private Network (VPN). As a result, Lottery did not implement some security controls for its VPN in accordance with the Security Standard, and industry best practices.

We identified and communicated five specific control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

Lottery should dedicate the necessary resources to implement the security controls for its VPN, that meet the requirements of the Security Standard and industry best practices. Implementing these controls will help maintain the confidentiality, integrity, and availability of Lottery's sensitive and mission-critical data.

Improve IT Asset Management Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Lottery does not define some of its requirements and procedures related to its information technology (IT) asset management, surplus, and disposal process. Additionally, Lottery does not consistently track all IT assets from purchase to surplus and disposal, causing discrepancies between its internal documentation and its external contractor's records. Lottery uses an external contractor to sanitize and destroy electronic devices that Lottery indicates are surplus. Lottery receives a certificate and list of devices from the external contractor as verification the contractor sanitized and destroyed the devices it received. Due to the inconsistent process, Lottery has three instances of discrepancies between its internal records and its external contractor's record of disposed devices for fiscal year 2022. We communicated the specific discrepancies to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires Lottery to review, approve, track, document, and verify media sanitization and disposal actions (Security Standard, section MP-6: Media Sanitization). Additionally, Lottery's Information Technology (IT) Asset Management Standard requires its system owners to verify that the disposal of hardware and software is in accordance with the Commonwealth's Removal of Commonwealth Data and Electronic Media Standard, SEC 514 (Media Standard).

Without policies and procedures that define all requirements and procedures staff must perform, Lottery cannot ensure its staff consistently follow the processes in accordance with the Security Standard and Media Standard and maintain the necessary documentation. Also, without tracking all IT devices throughout their lifecycle prior to disposal, Lottery is unable to reconcile its internal records with the external contractor's records to confirm the contractor destroyed the correct devices. IT assets designated for surplus or disposal may contain sensitive data that is exempt from public disclosure; therefore, having strong controls over the decommissioning and surplus of IT assets is critical. Lottery currently uses an IT asset management system to maintain records of physical workstations, servers, and virtual servers. However, due to system limitations with the IT asset management system, Lottery is unable to maintain records for additional IT devices, further hindering Lottery from consistently and effectively tracking its IT devices. Lottery is currently implementing a new IT asset management system that will allow the agency to track all IT assets across all departments during the device's lifecycle.

Lottery should update its policies and procedures to include requirements for all departments to track all IT assets throughout their lifecycle. Additionally, Lottery should ensure its policies and procedures include requirements outlined in the Security Standard and Media Standard and reflect its current IT asset management, surplus, and disposal processes. Lottery should implement a process to

reconcile its internal records with its external contractor's records to validate that all IT assets followed the appropriate process for surplus and disposal. Implementing these procedures will assist Lottery in consistently disposing IT assets across all departments, while ensuring it maintains an auditable record of IT asset surplus data removal documentation.

Improve Oversight of Third-Party IT Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Lottery does not have formal policies and procedures to maintain oversight over its third-party information technology service providers (providers) and as a result, does not consistently obtain and review independent audit assurance from its providers. Additionally, Lottery does not document its reviews and determination of possible compensating controls for deficiencies found in the providers' assurance reports. Providers are organizations that perform outsourced business functions on behalf of Lottery and the Commonwealth.

The Security Standard states that agency heads remain accountable for maintaining compliance with the Security Standard through documented agreements with the providers and oversight of services provided. Additionally, the Commonwealth's Hosted Environment Information Security Standard, SEC525 (Hosted Environment Security Standard), requires Lottery to perform an annual security audit or review the annual audit report conducted by an independent, third-party audit firm on an annual basis (Security Standard, section 1.1: Intent; Hosted Environment Security Standard, section SA-9-COV-3: External Information System Services).

Without an established process to consistently obtain and review independent audit assurance over the providers' internal controls, Lottery cannot validate that those providers have effective IT security controls to protect sensitive data. Lottery conducts reviews of independent audit assurance reports as part of a risk assessment or when evaluating new providers and verbally communicates the results of the evaluation but does not perform the reviews on a scheduled basis. The lack of a consistent and documented process is due to the absence of formal policies and procedures that address the requirements outlined in the Security Standard and Hosted Environment Security Standard.

Lottery should develop and implement a formal framework for gaining appropriate assurance over outsourced operations that affect its IT environment, sensitive data, or mission-critical processes. This process should include developing formal policies and procedures to obtain independent audit assurance for Lottery's evaluation. The evaluation will allow Lottery to determine whether providers' security controls comply with the requirements described in the Security Standard, Hosted Environment Security Standard, and documented contract agreement. Lottery can obtain assurance in several forms including, but not limited to, System and Organization Controls (SOC) reports, on-site reviews, or other independently verified assurance of the providers' internal control environment. Also, to maintain consistency and continuity, Lottery should document its evaluation of independent audit assurance reports, final decisions, and actions items resulting from the assurance report evaluation process.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 31, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Virginia Lottery Board
Virginia Lottery

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the governmental activities, the business-type activities, the major enterprise fund, and the remaining fund information of the **Virginia Lottery** as of and for the year ended June 30, 2022, and the related notes to the financial statements, which collectively comprise the Virginia Lottery's basic financial statements, and have issued our report thereon dated October 31, 2022.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Virginia Lottery'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 opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Virginia Lottery's internal control. Accordingly, we do not express an opinion on the effectiveness of the Virginia Lottery's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Ensure System Access Adheres to Principles of Least Privilege," "Improve Virtual Private Network Security," "Improve IT Asset Management Process," and "Improve Oversight of Third-Party IT Service Providers," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Virginia Lottery's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and**,** accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Ensure System Access Adheres to Principles of Least Privilege," "Improve Virtual Private Network Security," "Improve IT Asset Management Process," and "Improve Oversight of Third-Party IT Service Providers."

The Virginia Lottery's Response to the Findings

We discussed this report with management at an exit conference held on November 14, 2022. The Virginia Lottery's response to the findings and recommendations identified in our audit is described in the accompanying section titled "Virginia Lottery Response." The Virginia Lottery's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Finding

The Virginia Lottery has taken adequate corrective action with respect to the audit finding reported in the prior year.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

LDJ/vks

November 15, 2022

Ms. Staci A. Henshaw, CPA
The Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Re: Virginia Lottery Fiscal Year 2022 Internal Control Report

Dear Ms. Henshaw,

Thank you for the opportunity to respond to the annual audit of the Virginia Lottery for the year ended June 30, 2022. I appreciate the thorough work of your team and the APA's recommendations. Below please find the Lottery's response to the items included in your report.

Ensure System Access Adheres to Principles of Least Privilege
The Lottery does assign user access on the principles of least privilege. As noted, the system referenced was upgraded during the audit review period and these default role assignments were not identified as able to modify certain aspects of workflow processes. The Lottery is working to adjust system access and will complete this process in January 2023.

Improve Virtual Private Network Security
The Lottery has measures in place to ensure appropriate access to the Virtual Private Network. As part of the Lottery's Information Technology Systems Security Program, a formalized annual review of VPN access will be implemented. This measure, in conjunction with the ongoing measures including monthly configuration reviews, tiered approvals of access, and increased emphasis on document retention, will be completed and in place by January 2023.

Improve IT Asset Management Process
The Lottery does have legacy asset management procedures and acknowledges some paperwork errors in the documentation of the sampled surplus disposals. The Lottery will revise the current surplus policy to conform with the Commonwealth's Information Security Standard, SEC501, and will revise the procedure for system owners to verify that the disposal of hardware and software is in accordance with the Commonwealth's Removal of Commonwealth Data and Electronic Media Standard, SEC514. In addition, the Lottery is implementing the Inventory and Asset Management module of IVANTI Service Manager to track all Lottery owned hardware and software from procurement to disposal. This implementation will be complete by January 2023, and all inventories will be updated by April 2023.

Improve Oversight of Third-Party IT Service Providers

The Lottery has requirements for the primary vendor partners to provide System and Organization Control (SOC) reports annually, and the Lottery Director of Security and/or Information Security Manager reviews the reports annually. The Lottery will evaluate all third-party service providers and expand the contract requirements, as necessary. As of October 3, 2022, the Lottery has documented and implemented a formal process to document and maintain evidence of a more consistent oversight over third-party services providers. This process includes procedures to review SOC reports, communicate outcomes of the reviews, and to include final decisions and/or action items to the Lottery Security and Technology Architecture Review (STAR) committee. The outcomes of these reviews will be documented and maintained.

The Lottery remains diligently committed to continuous improvement, integrity, and effective accountability over all our business functions and regulatory responsibilities, including compliance with information security standards.

Sincerely,

Kelly Gee

VIRGINIA LOTTERY

For the year ended June 30, 2022

Kelly T. Gee
Executive Director

BOARD MEMBERS

Ferhan Hamid
Chair

Cynthia D. Lawrence
Vice-Chair

Vonda M. Collins

Orrin K. Gallop

Kimberly L. Martin

John Paul Powell

Scott A. Price