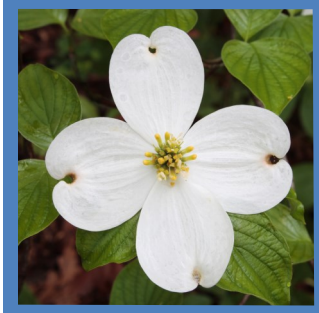

VIRGINIA LOTTERY

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2023

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 Virginia Lottery as of and for the year ended June 30, 2023, and issued our report thereon, dated November 17, 2023. Our report is included in Virginia Lottery's Annual Report that it anticipates releasing in December 2023.

Our audit of Virginia Lottery for the year ended June 30, 2023, found:

- the financial statements are presented fairly, in all material respects; and

- three internal control findings requiring management's attention that also represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and developing and appropriately implementing adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

– TABLE OF CONTENTS –

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

Virginia Lottery (Lottery) does not implement certain security controls for the database that supports its public website as required by its policies and the Commonwealth's Information Security Standard, SEC 501 (Security Standard), or recommended by industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmark). We communicated two control weaknesses to Lottery's management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Lottery's policy, which aligns with the Security Standard, requires Lottery to implement certain security controls to safeguard systems that contain or process sensitive data. By not meeting the minimum requirements in the Security Standard and industry best practices, Lottery cannot ensure the confidentiality, integrity, and availability of data within its system. Delays in implementing a new solution and lack of documentation caused the two weaknesses to exist.

Lottery should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with its policy, the Security Standard, and industry best practices. Implementing these controls will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Improve Procedures and Process for Oversight of Third-Party IT Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency

Lottery does not have certain elements in its policies and current process to consistently maintain oversight of its information technology (IT) third-party service providers (providers) in accordance with the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard).

Lottery has a Security Operation Control Report Review Process to outline requirements for Lottery's annual review of providers' independent audit assurance. Additionally, Lottery added provider acquisitions and renewals to its Security and Technical Architecture Review team's process to assess and approve the proposed provider and solution prior to procurement. However, the following weaknesses exist:

- Lottery does not document and maintain a complete and accurate list of its providers that perform business functions or processes on behalf of Lottery. Without an accurate list of all providers, Lottery is unable to validate that all providers are complying with contractual requirements and implement security controls to protect Lottery's sensitive data (Hosted

Environment Security Standard, Section: CA-3 and CA-3-COV Information System Connections).

- Lottery does not have formal policies and procedures that outline contractual agreement language requirements for providers based on the service procured. The Hosted Environment Security Standard requires Lottery to include specific requirements, descriptions, and criteria in the acquisition contract for the information system, system component, or information system service. The minimum requirements include security strength requirements, security assurance requirements, security-related documentation requirements, and requirements for protecting security-related documentation. Without formal policies and procedures to ensure the consistent application of contractual language requirements to provider agreements, Lottery's agreements may not include requirements to protect Lottery's sensitive data or perform a task. Also, Lottery is unable to compel the provider to give Lottery certain documentation that verifies compliance with Lottery's internal policies and the Hosted Environment Security Standard and implementation of specific security measures to protect Lottery's sensitive data (Hosted Environment Security Standard, Sections: 1.1 Intent, SA-4 Acquisitions).

- Lottery does not contractually require its providers to provide independent audit assurance reports on an annual basis. Additionally, Lottery does not conduct annual security audits or reviews of all providers' independent audit assurance reports. While Lottery conducts a review of a proposed provider's independent audit assurance report prior to approval and implementation, Lottery only conducts an annual review of independent audit assurance for two of its providers. Lottery's Security Operation Control Report Review Process requires, in accordance with the Hosted Environment Security Standard, for Lottery to perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis. Without conducting an annual review of the independent audit assurance report for all providers, Lottery is unable to verify if providers implemented the necessary security controls and processes, as required by the contract agreements and the Hosted Environment Security Standard, to protect Lottery's sensitive data. Additionally, Lottery is unable to review the list of complementary controls traditionally included in a provider's independent audit assurance report to determine whether Lottery needs to implement applicable security controls to mitigate potential risks (Hosted Environment Security Standard, Sections: 1.1 Intent, SA-9-COV-3 External Information System Services).

- Lottery does not have a process to confirm the exact location of sensitive data monthly after implementation. Lottery also does not contractually restrict the location of information processing, data, and information system services to locations within the continental United States. By not restricting its data to U.S. borders and confirming the location of its data monthly, Lottery increases the risk that its data may be offshored and not governed by Commonwealth and U.S. laws and regulations (Hosted Environment Security Standard, Sections: 1.1 Intent, SA-9-COV-1 External Information System Services).

- Lottery does not require its providers to provide vulnerability scan reports every 90 days. Lottery also does not have a process to review the vulnerability scan reports to verify providers are applying patching and mitigation efforts in a timely manner in accordance with its internal policies and the Hosted Environment Security Standard. By not obtaining and reviewing the vulnerability scan reports and enforcing remediation requirements, Lottery may be exposed to an increased risk of a successful cyberattack, exploit, and data breach in its providers' environments (Hosted Environment Security Standard, Sections: 1.1 Intent, SA-9-COV-3 External Information System Services).

- Lottery does not establish a data escrow policy or exit plan to address the data recovery process in case of system failure or facility issues and ensure providers return all copies of data to Lottery at the end of the contract. Without establishing a data escrow policy or other exit plan, Lottery is at risk of not having its data recovered as needed or ensuring the removal of data from the providers' systems at the end of the contract (Hosted Environment Security Standard, Section: SA-9-COV-2 External Information System Services).

Lottery's lack of formal policies and procedures that fully align with the Hosted Environment Security Standard, outlining all requirements for Lottery's acquisition and oversight of its providers led to the weaknesses noted above. Additionally, the absence of a complete and accurate provider list led to Lottery not ensuring it conducted its oversight process for all providers.

Lottery should improve policies and procedures to align with the Hosted Environment Security Standard and outline Lottery's requirements and process for consistently procuring and maintaining oversight of its providers on an ongoing basis. Lottery should also identify and document a list of its providers and implement a process for maintaining the list to ensure it is current. Additionally, Lottery should communicate required security controls to its providers through documented agreements, as appropriate. Furthermore, Lottery should request and evaluate the necessary security documentation from each provider to ensure the provider has effective operating controls to protect Lottery's sensitive data. Employing appropriate processes, methods, and techniques to monitor providers' security control compliance on an ongoing basis will help address the weaknesses listed above and ensure the confidentiality, integrity, and availability of Lottery's sensitive and mission-critical data.

Improve System Access Policies and Procedures for Critical Systems

Type: Internal Control and Compliance
Severity: Significant Deficiency

Lottery does not have properly documented policies and procedures reflective of the agency's controls for granting and monitoring access for all critical systems. Lottery incorporates the use of multiple information systems that support its traditional and online gaming operations, casino operations, and accounting and financial reporting functions. During our review of five critical information systems, we noted that Lottery did not have documented policies and procedures detailing the functionality of system user roles, including role combinations that violate segregation of duties principles for three of the five (60%) systems reviewed.

The Security Standard requires an agency to develop, document, and disseminate to all organization personnel, contractors, and service providers an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance (Security Standard, Section: AC-1 Access Control Policy and Procedures). The Security Standard further requires the agency to review the access control policy and procedures on an annual basis or more frequently to address environmental changes as needed. Further, agencies should structure policies to ensure system owners only grant access to users with documented job responsibilities that require those rights (Security Standard, Section: AC-6 Least Privilege). Lottery's current system access control framework centers around system workflows and vendor-provided support. While Lottery does have some procedures outlined, they do not individually address each unique system's permissions, and instead reference system access from a general perspective. Without system specific, detailed policies and procedures that depict all applicable user roles, the related capabilities of those roles, and annual monitoring processes, it is difficult for Lottery to ensure that it is appropriately applying segregation of duties and the principle of least privilege in each system.

Lottery should ensure that all critical systems have detailed policies and procedures for system access that, at a minimum, include defined user roles; defined authorizations to support segregation of duties and principles of least privilege; and defined monitoring processes including annual access reviews in accordance with the Security Standard to minimize the risk of inappropriate access for system users.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 17, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Virginia Lottery Board
Virginia Lottery

Tony Russell, Interim Director
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 **Virginia Lottery** as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise Virginia Lottery's basic financial statements, and have issued our report thereon dated November 17, 2023.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered 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 Virginia Lottery's internal control. Accordingly, we do not express an opinion on the effectiveness of 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 "Improve Database Security," "Improve Procedures and Process for Oversight of Third-Party IT Service Providers," and "Improve System Access Policies and Procedures for Critical Systems," 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 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 titled "Improve Database Security," "Improve Procedures and Process for Oversight of Third-Party IT Service Providers," and "Improve System Access Policies and Procedures for Critical Systems."

Virginia Lottery's Response to the Findings

We discussed this report with management at an exit conference held on November 21, 2023. Government Auditing Standards require the auditor to perform limited procedures on Virginia Lottery's response to the findings identified in our audit, which is included in the accompanying section titled "Virginia Lottery Response." Virginia Lottery's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Finding

Virginia Lottery has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

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.

AUDITOR OF PUBLIC ACCOUNTS

LDJ/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Ensure System Access Adheres to Principles of Least Privilege	Completed	2022
Improve Virtual Private Network Security	Completed	2022
Improve IT Asset Management Process	Completed	2022
Improve Oversight of Third-Party IT Service Providers	Completed	2022
Improve Database Security	Ongoing	2023
Improve Procedures and Process for Oversight of Third-Party IT Service Providers	Ongoing	2023
Improve System Access Policies and Procedures for Critical Systems	Ongoing	2023

GLENN YOUNGKIN, GOVERNOR | TONY R. RUSSELL, INTERIM DIRECTOR
Virginia Lottery | 600 E. Main St. | Richmond, VA 23219 | ph: 804.692.7100 | valottery.com

November 30, 2023

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

Re: Virginia Lottery Fiscal Year 2023 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, 2023. 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.

Improve Database Security
On September 13, 2023, the Lottery completed onboarding Bulletproof as the Managed Services Security Provider (MSSP) contracted to monitor our network and computer assets through their Security Operation Center (SOC).

One of the noted weaknesses was addressed through the implementation of the SOC; the other weakness identified has been majorly addressed, but will be fully addressed no later than May 1, 2024.

Improve Procedures and Process for Oversight of Third-Party IT Service Providers
The Lottery has longstanding contract requirements for primary vendor partners to provide System and Organization Control (SOC) reports annually, and procedures outlining the review and follow-up protocols for those primary providers. While the Lottery has worked to establish a complete and accurate list of service providers for which SOC reviews are needed and to establish additional contract requirements, this process was not complete at the time of the audit. The Lottery will continue to improve our procedures and documentation, and will prospectively implement practices to confirm the storage location of data, review Data Escrow policies or exit plans, and assure that vulnerability scanning and patch management programs are effective for sensitive and mission-critical data. These corrective actions will be in place no later than May 1, 2024.

Improve System Access Policies and Procedures for Critical Systems
The Lottery has an Information Security Program and Information Systems Security Policy that are updated annually, the most recent versions were updated October 12, 2023, and August 25, 2023, respectively. The policy sets out

requirements for Granting Access to Information Systems and other information systems requirements that employees review and acknowledge upon hiring and annually thereafter.

While the Lottery does acknowledge that formal documentation on specific procedures is an area for improvement, we do have processes in place for granting and monitoring access to these critical systems, and to ensure access does not violate segregation of duties principles. We will complete the documentation for each identified critical system, including documentation of critical user roles, no later than March 31, 2024.

The Virginia 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. An active Information Security program, including a Director-level program leader, a cyber liability insurance policy with ready access to legal and technology professional support, and a Security Operations Center are just a few significant examples of the Lottery's commitment to both supporting and maintaining information security policies, standards, and best practices.

Respectfully,

Tony R. Russell

Tony R. Russell