VIRGINIA LOTTERY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2016

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

Our audit of the Virginia Lottery for the year ended June 30, 2016, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention that, collectively, we consider to be a material weakness;
- internal control findings requiring management's attention that we consider to be significant deficiencies; and
- instances of noncompliance required to be reported under Government Auditing Standards.

We have audited the basic financial statements of the Virginia Lottery as of and for the year ended June 30, 2016, and issued our report thereon, dated October 10, 2016. Our report is included in the Virginia Lottery's Annual Report that it anticipates releasing in January 2017.

–TABLE OF CONTENTS–

STATUS OF PRIOR YEAR FINDINGS

Improve Capital Asset Management

In our last audit, we recommended that Lottery improve capital asset policies and procedures and implement additional procedures over physical inventory, asset classification, asset removal, asset identifiers and useful life. Lottery was not properly conducting physical inventories, and the capital assets policies and procedures over inventory did not specify unique inventory procedures for some departments. As a result, there were instances of misclassified capital assets, instances of assets not removed from the accounting system in a timely manner, and instances of assets in the system without a unique identifier. Without proper controls over capital assets, there is risk that the financial statements do not accurately reflect the true value of Lottery's capital assets.

We obtained a status update from Lottery on the corrective actions related to these weaknesses. As of our report date, some corrective actions were completed and some remain ongoing. Lottery began updating and implementing new procedures during fiscal year 2016 and plans to complete a physical inventory during 2017 and fully implement all corrective actions. We will review the implementation of management's corrective actions during our next audit.

Continue to Improve End User Controls

Lottery has made progress since the last audit and is currently working to remove unnecessary and elevated permissions without affecting Lottery's software and applications that are used to support business functions. We obtained a status update from Lottery on the corrective actions related to these findings. Lottery tested the removal of these permissions but had to delay the implementation due to incompatibility with Lottery applications. Lottery has since then removed permissions from certain accounts and created an alternate control for tracking elevated permissions. Lottery is taking a phased approach to resolving this weakness and planned to finish all corrective actions by September 2016. Sufficient time was not available to review the corrective action implementation before the issuance of this report; therefore, we will review their implementation during our next audit.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Application and Database Controls over the Dynamics AX Financial System

On February 1, 2016, the Virginia Lottery (Lottery) implemented a new enterprise resource planning system, Microsoft Dynamics AX (Dynamics), to serve as Lottery's general ledger, fixed asset, cash management, procurement and sourcing system. Effective the same date, Lottery was required to establish an interface from Dynamics to Cardinal, the Commonwealth's newly implemented financial management system.

Lottery met implementation deadlines for the new system and the new interface and both went operational by the required deadline. Upon completion of a post-implementation risk assessment of Dynamics, Lottery identified numerous risks and challenges impacting its control environment. Additionally, during our audit Lottery had difficulty generating auditable system reports relating to Dynamics system controls.

Many of the internal control weaknesses identified in this report are a result of the implementation of Dynamics. We identified and communicated these weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. An overview of the control deficiencies that illustrate Lottery's need to improve its internal controls over the Dynamics system is discussed below.

Improve Application Monitoring and Logging

Lottery does not adequately monitor and log access and activity to its financial reporting system, Dynamics, in accordance with the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard).

Lottery should dedicate the necessary resources to develop and implement the appropriate procedures and controls to ensure that adequate preventive, detective and corrective controls exist to address the weaknesses communicated in the FOIAE recommendation.

Prohibit Shared User Accounts and Passwords

Lottery allowed two user accounts to be shared for its financial reporting system, Dynamics. Additionally, these user accounts are not specific to an individual employee but are generically named user accounts.

Lottery's Information System Access Control Standard and Section AC-2 of the Security Standard prohibit the use of employee shared, generic, or guest accounts on information technology systems. Allowing employees to share user accounts and

passwords eliminates management's ability to identify which individual initiated system activity and hold them accountable.

Lottery should assign user accounts and passwords to individual employees to minimize security risks, increase accountability, and to ensure compliance with internal policies and the Security Standard.

Perform Reviews of Users Accounts and Privileges

Lottery did not perform and document a review of user accounts and privileges to the Dynamics application and database in accordance with internal policies and the Security Standard.

Lottery should dedicate the necessary resources to develop and implement the appropriate procedures and controls to address the weaknesses communicated in the FOIAE recommendation and to ensure compliance with internal policies and the Security Standard.

Assign System Access Based on Least Privilege

In initially setting up access to the Dynamics system, Lottery did not grant access based on the principle of least privilege. Additionally, Lottery did not have a process in place to determine if segregation of duties issues exist within Dynamics.

Lottery should dedicate the necessary resources to develop and implement the appropriate procedures and controls to identify segregation of duties issues within Dynamics. Additionally, Lottery should enforce the principle of least privilege when granting access to Dynamics in accordance with the Security Standard.

The Security Standard requires agencies to use specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Management is currently working to address these risks and challenges with the assistance of consultants. Lottery should continue to dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE that will align Lottery's operations with industry best practices and the Security Standard.

Improve IT Risk Management Controls

Lottery's new process to determine information technology (IT) risk is missing some fundamental components that are necessary to establish a complete information security posture that protects the confidentiality, integrity, and availability of mission critical and sensitive data.

Specifically, Lottery's new process to determine system sensitivity does not include classifications of data types, the identification and determination of potential damages, or have a requirement for an annual self-assessment process to evaluate and communicate to management any changes in data and risk.

The Security Standard requires agencies to identify mission critical and sensitive data in each of its systems and to classify this data based on sensitivity (for example: high, medium, or low). The Security Standard also requires agencies to determine the potential damages caused by a compromise by each data type. Lastly, the Security Standard requires agencies to perform and document an annual self-assessment where it evaluates the continued validity of each IT system's risk assessment and make any necessary recommendations for changes (*Security Standard sections: 4.2 IT System and Data Sensitivity Classification, RA-3 Risk Assessment, and 6.2 Risk Assessment*).

The absence of these components in Lottery's IT risk management controls introduces a risk that Lottery may not consider all the risk factors facing its systems, thereby not establishing adequate safeguards to protect mission critical and sensitive data. Additionally, not having a process to perform annual self-assessments to ensure system risk assessments are current does not give management the opportunity to accept changes in its environment.

The inconsistent data sensitivity classifications, inadequate documentation of potential damages, and lack of appropriate approvals occurred primarily due to an on-going change in Lottery's internal risk management and risk evaluation process. While the new methodology does have its merits, including increased stakeholder understanding, it does not encompass all of the related requirements and controls of the Security Standard.

Lottery should reevaluate and continue to develop the data classification and risk management methodology to ensure that it not only fosters stakeholder understanding, but also includes all of the required controls by the Security Standard, including a process for conducting annual self-assessments. Additionally, Lottery should complete and approve risk assessments for all sensitive and mission critical system according to the requirements in the Security Standard.

Improve System Patch Management

Lottery does not apply software patches to sensitive and mission critical systems in accordance with requirements defined in Lottery's policy. Lottery's Patch Management Standard requires the installation of patches and updates to servers and clients on a monthly basis.

Two systems were identified during the audit that were not patched according to Lottery's policy. The details of these weaknesses were communicated to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

Running out-of-date software increases the risk of a data breach or system unavailability, which could result in financial, legal, or reputational damages. Lottery has not patched these systems

according to its policy due to concerns that the patches may be incompatible in the environment and cause system unavailability. However, this concern should be remediated by Lottery's own policy to install patches in a test environment prior to implementation into a production environment.

Lottery should dedicate the necessary resources to update both systems to the newest and compatible software versions after following its formal testing and configuration management process. Lottery should also document any deviations and compensating controls to any patches found incompatible during testing. Lottery should apply patches according to its policy or update the policy to identify any systems that are patched according to different requirements.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 10, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, 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 **Virginia Lottery** as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise Virginia Lottery's basic financial statements, and have issued our report thereon dated October 10, 2016.

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 to determine the 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 Virginia Lottery's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Virginia Lottery's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the sections entitled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings," we identified certain deficiencies in internal control that we consider to be significant deficiencies and deficiencies that we consider to collectively be a material weakness.

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. We consider the combination of the deficiency entitled "Improve Application and Database Controls over the Dynamics AX Financial System," which is described in the section titled "Internal Control and Compliance Findings and Recommendations;" along with the deficiency entitled "Continue to Improve End User Controls," which is described in the section titled "Status of Prior Year Findings," to constitute a material weakness.

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. We consider the deficiencies entitled "Improve IT Risk Management Controls," and "Improve System Patch Management," which are described in the section titled "Internal Control and Compliance Findings and Recommendations;" along with the finding entitled "Improve Capital Asset Management," which is described in the section titled "Status of Prior Year Findings," 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 determination of financial statement amounts. 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 sections titled "Internal Control and Compliance Finding and Recommendations" and "Status of Prior Year Findings" in the findings entitled "Improve Capital Asset Management," "Continue to Improve End User Computer Controls," "Improve Application and Database Controls over the Dynamics AX Financial System," and "Improve IT Risk Management Controls."

The Virginia Lottery's Response to Findings

We discussed this report with management at an exit conference held on December 9, 2016. The Virginia Lottery's response to the findings identified in our audit is described in the accompanying section titled "Agency 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 Findings

The Virginia Lottery is taking corrective action with respect to the previously reported findings "Improve Capital Asset Management" and "Improve End User Computer Controls." Accordingly, we included these findings in the section entitled "Status of Prior Year Recommendations."

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 Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

AVC/clj

Terry McAuliffe, Governor | **Paula I. Otto,** Executive Director

Virginia Lottery | 600 East Main Street | Richmond, VA 23219 | ph: 804.692.7100 | fax: 804.692.7102 | valottery.com

January 11, 2017

Ms. Martha S. Mavredes, CPA
Auditor of Public Accounts
101 North 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

I appreciate the opportunity to respond to the issues included in the Auditor of Public Accounts Report on Audit for the year ending June 30, 2016. Your review confirmed several issues that the Lottery had identified and begun to improve, particularly related to the implementation of the new Enterprise Resource Planning (ERP) system in conjunction with the statewide conversion of the Commonwealth's accounting system. This new ERP provides enhanced system and process controls over transactions, supplementing the longstanding controls the Lottery has in place to ensure the integrity and accuracy of its systems and results. The implementation timeframe primarily was dictated by the Commonwealth's statewide accounting system conversion date of February 1, 2016, and while implementation of the new ERP was well planned and executed, there were aspects of the system that the Lottery identified as requiring additional work. Those are the issues included in this report, and we are happy to provide updates and clarifications.

The following are our responses to the issues contained in the internal control report:

Improve Capital Asset Management

The Lottery continues its commitment to the bi-annual physical inventory process, to be completed by June 30, 2017. The Lottery consistently takes a conservative approach to expensing capital assets, using a shorter useful life to ensure that remaining depreciation or amortization expense is not required when assets are taken out of service. Capital assets represent less than 3% of total assets for the Lottery, and consist mainly of gaming equipment deployed at Lottery retailer locations and information technology infrastructure hardware.

Continue to Improve End User Controls

Elevated permissions have been removed for all employees except for those requiring such access for business needs.

Improve Application and Database Controls over the Dynamics AX Financial System

As noted in the finding, the Lottery identified and started addressing issues with Dynamics AX, the new ERP system, prior to the audit. A new software solution to improve application monitoring and logging, provide reports for reviewing user accounts and privileges, and assist with ensuring access is in accordance with least privilege was identified and procured quickly after the ERP implementation, and then installed in November 2016.

Improve Application Monitoring and Logging

The installed software provides the necessary monitoring and logging capabilities.

Prohibit Shared User Accounts and passwords

Two new accounts were created so that the two accounts in question are no longer shared.

Perform Reviews of Users Accounts and Privileges

The Lottery does perform regular reviews of user accounts and privileges. A review of Dynamics AX access is scheduled for January 2017, less than one year after implementation.

Assign System Access Based on Least Privilege

The Lottery disagrees with this finding. Dynamics AX system user access was methodically granted using the principle of least privilege. The Lottery's System Administrator created new user roles to limit access even more than that provided by the default roles in the Dynamics AX system and worked with the implementation consultants from the accounting, consulting and technology firm Crowe Horwath, LLP in implementation of Dynamics AX, including controls and user roles. We recognized that useful user role security reporting tools were not available as part of the system and have already implemented a software solution as noted above. The individual accounts in question were either disabled or adjusted.

Improve IT Risk Management Controls

The Lottery continues its progress in updating sensitive system risk management controls (risk assessments) to use the new format, and we have worked with VITA and our Internal Audit team to develop a timeline for the risk assessments that will see this project to completion by June 2017.

With regard to the classification of data types, in September 2015 the Lottery developed a repository of information for its accessible databases to determine the purpose of the database and, if applicable, the type of sensitive information contained within. This enhances the Lottery's

ability to identify the potential impact of identified risks and thereby make better informed decisions for mitigation activities.

The Information Technology Security Committee will update the Lottery's Information Technology System Security Plan Standard by June 2017 to include the requirement for annual reviews of the risk assessments for each sensitive system.

Improve System Patch Management

The Lottery does not concur with this finding. Software patches for sensitive and mission critical systems are identified, tested and installed in a timely and appropriate manner. Factors including risk, timing, and other pertinent issues are thoughtfully evaluated when determining the course of testing and implementation.

We are in the process of updating our Patch Management Standard to explicitly commit these practices in writing within the policy. The details of our response were communicated to the Auditor of Public Accounts in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

In conclusion, the Lottery has operated successfully since the inception of sales in September 1988. During this time, systems development, implementation, maintenance, and delivery have been at the core of our operations. The integrity, reliability, and security of our systems is key to our success. Our financial statements fairly and accurately reflect these operations, and have been certified by the Auditor of Public Accounts annually as required by statute. The ERP system implemented provides enhanced controls over transactions and operations, enhanced from the previous manual control practices in place for which no deficiencies had been noted. My commitment to continuous improvement, integrity, and security of all Virginia Lottery operations does not waver. As another component of this commitment, the Lottery will contract with an independent resource to escalate addressing these system security concerns.

Sincerely,

Paula I. Otto

Paula I. Otto

c: Mr. Robert Howard, Chairman, Virginia Lottery Board
Mr. Fred Helm, Chairman, Virginia Lottery Board Audit Committee
Mr. Ferhan Hamid, Member, Virginia Lottery Board

VIRGINIA STATE LOTTERY DEPARTMENT

As of June 30, 2016

Paula I. Otto
Executive Director

BOARD MEMBERS

Robert M. Howard
Chairman

Fred P. Helm
Vice Chairman

Ferhan Hamid
Cynthia D. Lawrence
Scott A. Price