Audit Report

State Lottery and Gaming Control Agency

March 2018

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

March 8, 2018

Senator Craig J. Zucker, Co-Chair, Joint Audit Committee
Delegate C. William Frick, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the State Lottery and Gaming Control Agency (SLGCA) for the period beginning March 20, 2014 and ending January 2, 2017. SLGCA generates revenue primarily for the State's General Fund and the Education Trust Fund through various lottery games, as well as casino-operated video lottery terminals and table games. Approximately $1.1 billion of its revenue for fiscal year 2017 was credited to various State funds or agencies as prescribed by law.

Our audit disclosed certain control deficiencies regarding instant ticket games. For example, certain gaming contractor employees could perform critical transactions on the Lottery Gaming System, such as activate instant tickets, without independent supervisory review. In addition, SLGCA did not ensure that its vendor provided contractually required quality assurance reports related to ticket printing specifications and game prize structure.

We also noted several deficiencies relating to required monthly testing by SLGCA of video lottery terminals (VLTs) which are intended to help ensure that VLTs accurately process and report player activity. For example, SLGCA did not always document the results of the tests performed nor had it developed instructions for addressing discrepancies that on occasion were identified. For example, for one of ten monthly tests reviewed, SLGCA did not follow up and resolve discrepancies on five VLTs between the cash actually played by the tester and the cash reported to have been played by the VLTs.

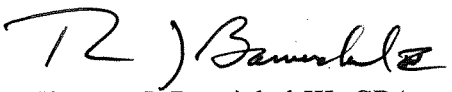
Our audit also disclosed deficiencies pertaining to the security of personally identifiable information and SLGCA's public website. For example, controls

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

over sensitive personally identifiable information, including social security numbers, maintained on SLGCA's mainframe computer were not sufficient.

SLGCA's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by SLGCA.

Respectfully submitted,



Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Background Information

Agency Responsibilities

The State Lottery and Gaming Control Agency (SLGCA) operations generate revenue for the State's General Fund, the Education Trust Fund, the Maryland Stadium Authority, and certain other governmental funds and agencies.

SLGCA administers and operates various lottery games. During fiscal year 2016, there were 4,843 lottery retail agents who sold instant tickets, and tickets for draw games and monitor games. Draw games include traditional games, such as Pick 3/Pick 4, and multi-state games, such as Mega Millions and Power Ball. Monitor games include Keno and Racetrax. SLGCA's responsibilities for the operation of these games require continuous oversight and marketing of lottery gaming operations as well as the development of new games. SLGCA has entered into an agreement with a gaming contractor to help fulfill these responsibilities, as well as to perform the daily operation and maintenance of the Lottery Gaming System used for administering these games.

SLGCA is also responsible for administering the video lottery terminal (VLT) program within the State's six authorized VLT facilities (casinos), including accounting for and distributing VLT revenue, managing the program's central system, and regulating and licensing operators. SLGCA has entered into an agreement with another contractor to assist SLGCA in meeting these responsibilities. Finally, SLGCA is responsible for regulating and creating standard rules for table games at the State's casinos. The State's first casino opened in Cecil County in September 2010 and its most recent casino opened in Prince George's County in December 2016. The four other casinos are located in Worcester, Anne Arundel, and Allegany Counties, and Baltimore City. As of June 2017, these six casinos operated 11,591 VLTs and 585 table games.

The State Lottery and Gaming Control Commission consists of seven members appointed by the Governor with the advice and consent of the State Senate. The Commission has oversight responsibilities for SLGCA's operations and, in conjunction with SLGCA, is responsible for regulating the operations of the State's VLTs and table games.

Financial Information

According to SLGCA's audited financial statements for the fiscal year ended June 30, 2017, gross revenue totaled approximately $3.4 billion, as detailed below.

Approximately $1.1 billion of this revenue was credited to various State funds or agencies as prescribed by law.

- $1.2 billion was disbursed for prize claims;
- $965 million was disbursed for agent and casino commissions and claims fees;
- $102 million was used to pay SLGCA's operating expenses;
- $484 million was credited to the State's General Fund;
- $451 million was credited to the Education Trust Fund;
- $40 million was transferred to the Maryland Stadium Authority; and
- $149 million was credited to other governmental funds and agencies.

SLGCA engages an independent accounting firm to perform an annual audit of its financial statements and monthly audits of special-purpose financial statements, and to provide assistance in technical matters. In the related audit reports for the fiscal years ended June 30, 2015, 2016, and 2017, the firm stated that SLGCA's financial statements presented fairly, in all material respects, its financial position, and the respective changes in its financial position and cash flows, for the years then ended in conformity with accounting principles generally accepted in the United States of America.

Status of Findings from Preceding Audit Reports

Our audit included a review to determine the status of the five findings contained in our preceding audit report dated April 14, 2015. We determined that SLGCA satisfactorily addressed these findings.

We also determined the status of the one finding in our performance audit report on Video Lottery Operation Licensees, Minority Business Participation dated October 19, 2016. That finding recommended that SLGCA establish amended minority participation goals for all categories (architectural and engineering, construction, operational procurements) in which VLT licensees have expenditures. We determined that SLGCA satisfactorily addressed that finding.

Findings and Recommendations

Instant Tickets

Background

As of June 30, 2017, the State Lottery and Gaming Control Agency (SLGCA) offered 74 different instant ticket games, also referred to as scratch-offs, with costs ranging from $1 to $30 per ticket. SLGCA contracted with a vendor to print and deliver instant tickets for each game in accordance with SLGCA's requirements regarding printing specifications, the game prize structure, the number of tickets required, and the required delivery schedule.

SLGCA has also entered into an agreement with a gaming contractor to operate and maintain the Lottery Gaming System. SLGCA's Lottery Gaming System provides certain automated operational, accounting, and control functions over instant tickets. For example, instant tickets must be activated on the System prior to being eligible for redemption for any winnings. Activation normally takes place at the lottery retail agent's (seller's) location. According to SLGCA records, net sales of instant tickets totaled approximately $676.8 million, with printing expenditures totaling $7.5 million in fiscal year 2017.

Finding 1
Controls over individual access to perform critical transactions on the Lottery Gaming System and for the payment of instant tickets printed were not sufficient. In addition, processes in place to ensure tickets met required specifications were not consistently performed.

Analysis

Individual access to perform critical transactions on the Lottery Gaming System and for the payment of instant tickets printed were not adequately controlled. In addition, processes in place to ensure tickets met required specifications were not consistently performed.

- Four gaming contractor employees had access to an administrator user account on the Lottery Gaming System that allowed them to perform critical transactions, such as activating instant tickets without independent supervisory review. While the contractor needed this access to occasionally process transactions as directed by SLGCA, SLGCA had no procedure to identify and review the transactions processed for propriety. Furthermore, all four gaming contractor employees shared the same administrator user account, which precluded individual accountability over transactions processed. The

State's Department of Information Technology's *Information Security Policy* generally prohibits multiple individuals from sharing the same account.

According to reports obtained from SLGCA, 107 transactions, primarily activations, were performed by individuals using this shared account during the period from March 31, 2014 through October 26, 2016. Our test of 30 of these transactions did not disclose any improper transactions.

- The employee responsible for processing and approving payments for instant tickets printed, did so without reviewing adequate documentation that the required quantity of tickets had been received. Specifically, this employee did not obtain the signed receiving report from an independent employee and, as a result, payments could be made for tickets that were not received.

- SLGCA did not always obtain and review quality assurance reports intended to monitor certain contractual requirements relating to ticket production. Specifically, SLGCA's contract with the vendor that printed instant tickets required the vendor to hire an independent accounting firm to conduct a review and issue a written report for each ticket production (for example, for a new game) indicating compliance with certain requirements, including whether the tickets were printed in accordance with the required specifications, and that the game prize structure was proper. However, at the time of our review, SLGCA had not obtained these reports for the period from December 2016 through February 2017. During that period, 13 reports should have been provided.

  In addition, SLGCA did not document its review of reports that were received prior to this period. Furthermore, reports prepared by the firm were provided to SLGCA by the vendor, rather than directly by the firm as required by the contract. Our review of 19 reports issued by the independent accounting firm during calendar year 2016 did not disclose any significant findings.

Recommendation 1
We recommend that SLGCA

a. establish independent review procedures to ensure the propriety of transactions processed under the administrator user account;
b. discontinue the use of shared user accounts;
c. ensure that the employee who processes vendor invoices for instant tickets obtains and reviews independent documentation verifying the receipt of all required tickets prior to approving the invoices for payment; and

d. obtain all required quality assurance reports directly from the independent accounting firm that prepared the reports, including for the aforementioned period, and perform a documented review of each report.

Video Lottery Terminal (VLT) Operations

Finding 2
Required monthly VLT testing procedures were not always properly performed to ensure proper operation and reporting.

Analysis
SLGCA did not always perform adequate testing procedures, including the maintenance of supporting test documentation, to ensure that individual VLTs were operating properly, and the activity was properly reported. Specifically, SLGCA's written policy requires monthly testing of a minimum number of VLTs at each casino to ensure that the actual amounts played, won, and cashed out on the VLTs are being accurately recorded on automated reports of player activity generated by the VLTs. However, SLGCA could not always provide support to document the results of the tests performed, and did not always conduct follow-up procedures when discrepancies were detected. Furthermore, SLGCA did not require supervisory review of the test results and did not always perform testing on the minimum quantity of VLTs, as required by its policy. The propriety and accuracy of VLT operations is critical for public confidence in the system to ensure that VLT financial data recorded by the terminals, and subsequently used to help verify VLT revenue is accurate and complete.

SLGCA' monthly testing procedures required selecting a minimum number of VLTs at each casino, inserting cash or a voucher for payment, playing five times on each VLT, and cashing out any remaining balance. The actual amounts associated with the testing were manually recorded and then compared with corresponding automated reports generated by the terminals. Our review of 10 monthly tests conducted by SLGCA, which included 110 VLTs at the State's 6 casinos during the period February 2016 through February 2017, disclosed the following conditions:

- SLGCA lacked sufficient documentation to support test work performed and related conclusions reached for 3 (34 VLTs) of the 10 tests we reviewed. For example, for 2 (22 VLTs) of these 3 tests, SLGCA could not provide copies of the automated reports that were used to compare the actual amounts played, won, and cashed out with the corresponding amounts as recorded by the VLTs. Therefore, the results of these tests could not be substantiated.

SLGCA's policy requires that the automated reports of VLT data associated with the testing be maintained.

- SLGCA did not always investigate and resolve discrepancies identified during testing for 2 (16 VLTs) of the remaining 7 tests we reviewed. For example, our review of one test of 6 VLTs disclosed differences between the amount of cash played according to the automated system reports and the amount of cash actually played for 5 VLTs. However, SLGCA did not follow up on and resolve the discrepancies with the casino. The aggregate differences between the amount of cash played according to the automated system reports ($775) and the amount of cash actually played ($83) for these 5 VLTs totaled $692 and ranged between $5 and $412 for each individual VLT. In each case, the amount of cash played as reported exceeded the amount actually played. SLGCA could not document whether these differences resulted from machine reporting errors or testing errors.

- SLGCA tested a total of 11 fewer VLTs than required by its written policy for these 10 tests. The policy requires that each test include the lesser of 15 VLTs or one percent of the VLTs in each casino at the time of the test. According to this policy, SLGCA should have tested 121 VLTs; however, it only tested 110. The shortages occurred during 3 of the 10 tests.

- None of the 10 test results had evidence of supervisory review and approval. The overall results were recorded on summary sheets; however, there was no evidence that these results and supporting documentation had been reviewed and approved by supervisory personnel.

Inadequate documentation and the lack of follow-up procedures were caused, at least in part, by the lack of a comprehensive written testing policy. SLGCA's written policy did not require that the operational tests be subject to supervisory review and approval, nor did it include specific instructions on how to address discrepancies.

According to SLGCA's records, during fiscal year 2016, revenues from VLT operations totaled $741.7 million. In addition, there were approximately 11,660 VLT's in operation as of December 2016.

Recommendation 2
We recommend that SLGCA

a. enhance its written policy for the monthly operational tests of VLTs to include requirements for supervisory review and approval of testing results and instructions for addressing discrepancies,

b. maintain documentation to support VLT operational tests performed and related conclusions reached,
c. ensure that the required minimum number of VLTs are tested monthly, and
d. conduct supervisory reviews and any additional procedures in accordance with the enhanced policy developed.

Information Systems Security and Control

Background
SLGCA's Division of Information Technology manages the development, maintenance, and support of SLGCA's information technology infrastructure, including all related networking, telecommunications, and business information systems. The Division's staff operates a mainframe computer which hosts numerous systems used for multiple purposes including SLGCA agent administration, tracking of SLGCA annuity winners, claims administration, financial systems operations and monitoring, and review of sales. In addition, the Division operates an internal network which includes application and database servers. Furthermore, the internal network connects to networkMaryland, the Internet, video lottery terminal operations, and the contractor networks used for support of SLGCA games.

The SLGCA wide area network has connections to the SLGCA Compliance Office in each of the State's casinos, which provide oversight and monitoring of the operations at the six VLT facilities.

SLGCA's public website provides information related to winning numbers, games, promotions, lottery news, and other resources. The website also acts as a portal for individuals to connect to a separate lottery loyalty program (where players can collect points by purchasing and entering codes from eligible, non-winning scratch-off tickets or eligible winning or non-winning draw game tickets). According to SLGCA's records, for January and February 2017, the website experienced an average of 155,320 daily visits.

The website is maintained and managed by a primary contractor which:

- oversees the management and daily operations of the website,
- writes and maintains the application code for the website, and
- monitors the performance of the website and subcontractor hosting the website

The primary contractor hired a subcontractor to host and:

- maintain all servers that support the website,
- maintain the firewalls and intrusion detection prevention system that help protect the website, and
- create and monitor the security logs related to the website.

Finding 3
Sensitive personally identifiable information (PII) maintained by SLGCA was stored without adequate safeguards.

Analysis
Controls over sensitive PII maintained on the SLGCA mainframe computer were not sufficient to properly protect this data.

- Over 60,000 unique Social Security Numbers along with related full names, dates of birth, and addresses were stored in clear text on the SLGCA mainframe computer in two databases and ten data files. Although the SLGCA did implement a Data Loss Prevention control to help protect this PII, this control procedure was not sufficient for certain file transfer techniques.

- SLGCA had not performed an inventory of PII contained on its systems. Accordingly, SLGCA lacked assurance as to the extent of the PII on its systems and whether this PII was encrypted and properly protected.

This personally identifiable information is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. The State of Maryland's *Information Security Policy* requires that agencies protect confidential data using encryption technologies and/or other substantial mitigating controls.

Recommendation 3
We recommend that SLGCA
a. perform a complete inventory of its systems and identify all sensitive PII,
b. determine if it is necessary to retain this PII and delete all unnecessary PII,
c. determine if all necessary PII is properly protected by encryption or other substantial mitigating controls, and
d. use approved encryption algorithms to encrypt all sensitive PII not otherwise properly protected.

Finding 4
SLGCA lacked assurance that its public website was properly secured in regard to the web application's underlying code and the security and availability control environment for the data center hosting the website.

Analysis
SLGCA lacked assurance that its public website was properly secured in regard to the web application's underlying code and the security and availability control environment for the data center hosting the website.

- SLGCA did not procure nor did it require the primary contractor to obtain a security vulnerability assessment to help identify the existence of any potentially serious security vulnerabilities within the web application code. A web application code vulnerability assessment is recognized as a necessary way to find and diagnose many security problems which cannot be found any other way. Accordingly, the web application could be exposed to web-based security vulnerabilities which, if exploited, could possibly result in improper changes to website data and program files. The *Information Security Policy* requires that system hardening procedures shall be created and maintained to ensure up-to-date security best practices are deployed at all levels of information technology systems.

- As of April 11, 2017 SLGCA had not obtained reports of independent, standards based security reviews of the hosting subcontractor, which would include tests of controls to ensure that sufficient controls were operational for the services provided by the subcontractor. In addition, the most recent contract with the website primary contractor did not require the hosting subcontractor to engage an independent auditing firm to conduct Service Organization Controls (SOC) 2 Type 2 reviews. As a result, SLGCA lacked assurance as to the operating effectiveness of the controls implemented by the subcontractor to secure the hosting of the website. However, after our requests for such reviews and related reports, SLGCA staff obtained and provided us with a copy of a SOC 2 Type 2 report of the subcontractor for the period from March 1, 2015 to February 29, 2016. We reviewed the aforementioned SOC report and found that it adequately addressed our security concerns.

  The American Institute of Certified Public Accountants has issued guidance concerning examinations of service providers. Based on this guidance, service providers (like the aforementioned subcontractor) may contract for an independent review of controls and resultant independent auditor's report referred to as a SOC report. There are several types of SOC reports, with

varying scopes and levels of review and auditor testing. A SOC 2 Type 2 report contains the service organization's description of its system and the results of the auditor's examination of the suitability of the system design, operating effectiveness for the period under review, and any evaluation of system security, availability, processing integrity, confidentiality, and privacy.

Recommendation 4

We recommend that the SLGCA

a. **either procure or require the primary contractor to obtain a security vulnerability assessment for the web application code, remediate all confirmed vulnerabilities identified by the assessment, document this process, and retain this documentation for future reference;**
b. **ensure that future contracts with the website primary contractor require that any subcontractor performing hosting services to engage an independent auditing firm to conduct SOC 2 Type 2 reviews;**
c. **promptly obtain from the primary contractor all of the SOC reports that relate to the public website's subcontractor hosting and review the reports to ensure that they provide SLGCA with adequate assurance as to the adequacy and operational effectiveness of the controls protecting the website hosting; and**
d. **ensure that any material security concerns identified in the reports are promptly addressed, document these processes, and retain the documentation for future reference.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the State Lottery and Gaming Control Agency (SLGCA) for the period beginning March 20, 2014 and ending January 2, 2017. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine SLGCA's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included the operation of lottery games, video lottery terminals, and table games, including the accountability over proceeds and payouts. In addition, the audit addressed purchases, disbursements, corporate purchasing cards, payroll, and information technology systems. We also determined the status of the findings contained in our preceding audit report.

Finally, we determined the status of the one finding included in our audit report on video lottery operation licensees – minority business participation, dated October 19, 2016. In this regard, Chapter 49, 2016 Laws of Maryland, eliminated the requirement that the Office of Legislative Audits separately audit, on an annual basis, information received by SLGCA from video lottery operation licensees regarding the attainment of minority business participation goals, and the licensees' efforts to maintain those goals. Consequently, the aforementioned October 19, 2016 report was our final report to be issued under that requirement. Nevertheless, the attainment of these goals will be subject to examination during our audits of SLGCA.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of SLGCA's operations, and tests of transactions. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the

tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these sources were sufficiently reliable for the purposes the data were used during this audit. In addition, we obtained data extracted from SLGCA's automated records for the purpose of testing casino and lottery financial activity. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

SLGCA's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect SLGCA's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant

findings were communicated to SLGCA that did not warrant inclusion in this report.

SLGCS's response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise SLGCA regarding the results of our review of its response.

APPENDIX

Maryland Lottery and Gaming Control Agency

Larry Hogan, Governor • Gordon Medenica, Director

Montgomery Park Business Center
1800 Washington Blvd., Suite 330
Baltimore, Maryland 21230

Tel: 410-230-8800
TTY users call Maryland Relay
www.mdlottery.com

March 5, 2018

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Re: Audit Report – March 20, 2017 - January 2, 2017

Dear Mr. Barnickel:

The Maryland Lottery and Gaming Control Agency has reviewed your audit report for the period beginning March 20, 2014 and ending January 2, 2017. As requested, our responses to the findings in the report are attached.

If you have any questions or need additional information, you may contact me at 410-230-8790 or Gina Smith, Deputy Director and CFO at 410-230-8763.

Sincerely,

Gordon Medenica
Director

cc: Gina Smith, Deputy Director and CFO

Finding 1
Controls over individual access to perform critical transactions on the Lottery Gaming System and for the payment of instant tickets printed were not sufficient. In addition, processes in place to ensure tickets met required specifications were not consistently performed.

Recommendation 1
We recommend that SLGCA

a. establish independent review procedures to ensure the propriety of transactions processed under the administrator user account;
b. discontinue the use of shared user accounts;
c. ensure that the employee who processes vendor invoices for instant tickets obtains and reviews independent documentation verifying the receipt of all required tickets prior to approving the invoices for payment; and
d. obtain all required quality assurance reports directly from the independent accounting firm that prepared the reports, including for the aforementioned period, and perform a documented review of each report.

Agency Response:

a. The Agency has established independent procedures to ensure the propriety of transactions processed under the administrator user accounts;
b. The Agency agrees to discontinue the use of shared user accounts;
c. The Agency agrees. The employee that processes vendor invoices for instant tickets obtains and reviews independent documentation to verify the receipt of all required tickets prior to approving the invoice for payment.
d. The Agency agrees. Independent quality assurance reports are now received directly from the independent account firm that prepared the reports and the Agency is documenting its review of each report. All prior reports have also been obtained and independently reviewed.

Finding 2
Required monthly VLT testing procedures were not always properly performed to ensure proper operation and reporting.

Recommendation 2
We recommend that SLGCA

a. enhance its written policy for the monthly operational tests of VLTs to include requirements for supervisory review and approval of testing results and instructions for addressing discrepancies,
b. maintain documentation to support VLT operational tests performed and related conclusions reached,
c. ensure that the required minimum number of VLTs are tested monthly, and
d. conduct supervisory reviews and any additional procedures in accordance with the enhanced policy developed.

Agency Response:

a and b - The Agency agrees. The written procedure has been updated to include a more comprehensive testing procedure, supervisory review, instructions for addressing discrepancies, and retention of documentation. The update has been circulated to gaming operations staff.

c. The Agency agrees to ensure that the volume of testing is performed according to the requirements moving forward unless there is documented supervisory approval for modification.

d. The Agency agrees. The written procedure has been updated to include a more comprehensive testing procedure, supervisory review, instructions for addressing discrepancies, and retention of documentation. The update has been circulated to gaming operations staff.

Finding 3
Sensitive personally identifiable information (PII) maintained by SLGCA was stored without adequate safeguards.

Recommendation 3
We recommend that SLGCA

a. perform a complete inventory of its systems and identify all sensitive PII,
b. determine if it is necessary to retain this PII and delete all unnecessary PII,
c. determine if all necessary PII is properly protected by encryption or other substantial mitigating controls, and
d. use approved encryption algorithms to encrypt all sensitive PII not otherwise properly protected.

Agency Response:

The Agency agrees to perform a complete inventory of its systems, identify all sensitive PII, and determine if the data is necessary to retain. Any data not necessary will be deleted. The Agency also agrees to ensure that all necessary PII is properly protected by encryption or other mitigating controls and will use approved encryption algorithms to encrypt all sensitive PII data.

Finding 4
SLGCA lacked assurance that its public website was properly secured in regard to the web application's underlying code and the security and availability control environment for the data center hosting the website.

Recommendation 4
We recommend that the SLGCA

a. either procure or require the primary contractor to obtain a security vulnerability assessment for the web application code, remediate all confirmed vulnerabilities identified by the assessment, document this process, and retain this documentation for future reference;

b. **ensure that future contracts with the website primary contractor require that any subcontractor performing hosting services to engage an independent auditing firm to conduct SOC 2 Type 2 reviews;**
c. **promptly obtain from the primary contractor all of the SOC reports that relate to the public website's subcontractor hosting and review the reports to ensure that they provide SLGCA with adequate assurance as to the adequacy and operational effectiveness of the controls protecting the website hosting; and**
d. **ensure that any material security concerns identified in the reports are promptly addressed, document these processes, and retain the documentation for future reference.**

Agency Response:

The Agency agrees with the recommendations. The current advertising contract will be put out to bid within the near future. The RFP has requirements in it that require any subcontractor performing hosting services to engage in an independent auditing firm to conduct SOC 2 Type 2 reviews. These reviews will be obtained and the Agency will ensure that all material security concerns are promptly addressed. This process will be documented and retained for future reference.

AUDIT TEAM

Mark S. Hagenbuch, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Adam M. Auerback
Senior Auditor

J. Gregory Busch
Edward O. Kendall
Information Systems Senior Auditors

Jessica A. Cacho, CPA, CFE
Stephanie A. Laciny
Marc E. Merius
Kush C. Patel
Staff Auditors

Robert H. Dean
Information Systems Staff Auditor