

Audit Report

---

**State Lottery and Gaming Control Agency**

April 2015

---



**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

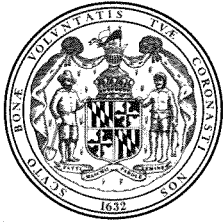
E-mail: [OLAWebmaster@ola.state.md.us](mailto:OLAWebmaster@ola.state.md.us)

Website: [www.ola.state.md.us](http://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 through the Office's website, by a toll-free call to 1-877-FRAUD-11, or by mail to the Fraud Hotline, c/o Office of Legislative Audits.**



*The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.*



Karl S. Aro  
Executive Director

DEPARTMENT OF LEGISLATIVE SERVICES  
OFFICE OF LEGISLATIVE AUDITS  
MARYLAND GENERAL ASSEMBLY

April 14, 2015

Thomas J. Barnickel III, CPA  
Legislative Auditor

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee  
Delegate Craig J. Zucker, 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 7, 2011 and ending March 19, 2014. 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.

Our audit disclosed a number of security and control deficiencies relating to SLGCA's information systems. For example, SLGCA's network and its workstations and servers were not adequately secured against external threats.

Our audit also disclosed that SLGCA did not distribute unclaimed funds from video lottery terminal (VLT) play in a manner consistent with State regulations. Rather, SLGCA distributed these funds in the same manner as VLT gambling proceeds. During calendar year 2013, unclaimed funds totaling \$347,000 were distributed to the casinos and others instead of to the State.

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**

<b>Background Information</b>	4
Agency Responsibilities and Name Change	4
Casino Gaming Program	4
Financial Information	5
Status of Findings From Preceding Audit Report	6
<b>Findings and Recommendations</b>	7
<b>Information Systems Security and Control</b>	
* Finding 1 – The SLGCA Network Was Not Adequately Secured	7
Finding 2 – Network Workstations and Servers Were Not Sufficiently Protected Against Malware	8
* Finding 3 – Mainframe Access Controls, Account and Password Controls, and Security Reporting Were Not Sufficient	10
<b>Unclaimed Video Lottery Terminal Funds</b>	
Finding 4 – Distributions of Unclaimed Funds Were Not Consistent with State Regulations	11
<b>Procurement</b>	
Finding 5 – Certain Contract Awards Were Not Published in eMaryland Marketplace	12
<b>Audit Scope, Objectives, and Methodology</b>	13
<b>Agency Response</b>	Appendix

\* Denotes item repeated in full or part from preceding audit report.

## **Background Information**

### **Agency Responsibilities and Name Change**

Chapter 1, Laws of Maryland 2013, effective October 1, 2012, changed the name of the State Lottery Agency to the State Lottery and Gaming Control Agency (SLGCA). This law also changed the name of the State Lottery Commission to the State Lottery and Gaming Control Commission. 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 as further detailed on page 5 of this report.

SLGCA administers and operates various lottery games. During fiscal year 2014, there were 4,721 lottery retail agents who sold instant tickets, as well as 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 and 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.

SLGCA also administers the video lottery terminal (VLT) program, including accounting for and distributing VLT revenues, managing the program's central system, and regulation and licensing operators. In 2012, SLGCA's responsibilities were further expanded to include the regulation of table games at previously authorized VLT facilities (casinos).

The 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.

### **Casino Gaming Program**

Chapter 1, Laws of Maryland 2013, expanded the State's casino gaming program. Specifically, the Maryland 2013 law authorized VLT operation licensees (casino operators) to operate table games, increased the number of authorized VLTs, and allowed for the future operation of a VLT and table game facility in Prince

George's County. Certain provisions of the law were subject to voter referendum and were upheld by Maryland voters on November 6, 2012.

Licenses required to operate six casinos in Maryland have been awarded. The licensees are responsible for the daily operation of the casino with onsite monitoring being performed by SLGCA. SLGCA has also entered into an agreement with a contractor to operate a central computer system that performs VLT accounting and provides monitoring, command, and control functions for the VLTs and table games. Casinos in Cecil, Worcester, Anne Arundel, and Allegany Counties, and in Baltimore City opened in September 2010, January 2011, June 2012, May 2013, and August 2014, respectively. A facility in Prince George's County is expected to open to the public during calendar year 2016.

## **Financial Information**

According to SLGCA's audited financial statements for the fiscal year ended June 30, 2014, gross revenue totaled approximately \$2.6 billion, of which approximately \$942 million was credited to various State funds or agencies as prescribed by law:

- \$1.0 billion was disbursed for prize claims;
- \$528 million was disbursed for agent and casino commissions and claims fees;
- \$148 million was used to pay SLGCA's operating expenses;
- \$501 million was credited to the State's General Fund;
- \$328 million was credited to the Education Trust Fund;
- \$20 million was transferred to the Maryland Stadium Authority; and
- \$93 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, 2012, 2013, and 2014, 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 Report**

Based on our assessment of significance and risk relative to our audit objectives, our audit included a review to determine the status of five of the six findings contained in our preceding audit report dated May 21, 2012. We determined that SLGCA satisfactorily addressed three of these five findings and the remaining two findings are repeated in this report. We did not follow up on the remaining finding which pertained to the licensing functions for VLT operations.



# Findings and Recommendations

## Information Systems Security and Control

### Background

The State Lottery and Gaming Control Agency's (SLGCA) Information Technology Unit manages the development, maintenance, and support of SLGCA's information technology infrastructure, including all related networking, telecommunications, and business information systems. The Unit'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 Unit operates an internal network which includes email, 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 (WAN) supports SLGCA staff, located at the State's casinos, who provide oversight and monitoring of casino operations at the following sites:

- Hollywood Casino, Perryville MD
- Ocean Downs Casino, Berlin MD
- Maryland Live Casino, Hanover MD
- Rocky Gap Casino, Cumberland MD
- Horseshoe Casino, Baltimore, MD

### Finding 1

**The SLGCA network was not adequately secured from untrusted traffic.**

### Analysis

The SLGCA network was not adequately secured from untrusted traffic.

- The firewalls installed to protect the SLGCA network allowed unnecessary and insecure connections to network devices on the internal network. The firewalls' rules were not configured to adequately secure connections into the network from the Internet, networkMaryland, and other untrusted sources. A similar condition was commented upon in our preceding audit report. In addition, many outdated rules existed on these firewalls. Therefore, critical network devices were susceptible to attack which could result in a loss of data integrity or the interruption of critical network services.

- Network traffic from a contractor to SLGCA’s secondary claims center and backup data center was not filtered by an SLGCA device. As a result, critical network devices at the centers were susceptible to attack. A similar condition was commented upon in our preceding audit report.
- An insecure connection protocol that transmitted unencrypted traffic, including userids and passwords was used for remote administration of the SLGCA Internet firewall. In addition, remote administrative connections to this firewall were not restricted to originating from only authorized source addresses and this firewall was not configured to uniquely identify individuals performing administrative actions on the firewall thereby precluding accountability for these actions.
- The SLGCA Internet firewall logs were only stored in its internal memory. As such, these logs were constantly overwritten and if the firewall was compromised the logs could be deleted thereby removing evidence of the compromise. In addition, the firewall logs were not regularly reviewed for unusual or suspicious entries.

#### **Recommendation 1**

**We recommend that SLGCA**

- a. configure its firewalls to achieve a “least privilege” security strategy giving individuals, entities, and devices only those network access privileges needed to perform assigned tasks (repeat);**
- b. use only secure protocols to connect to all firewalls, limit remote access to all firewalls to only authorized source addresses, and configure all firewalls to uniquely identify all individuals performing administrative actions on these firewalls; and**
- c. store firewall logs in a secure location, retain the most recent three months of logs, regularly review these logs, investigate unusual or suspicious log entries, document these reviews and investigations, and retain such documentation for future reference.**

#### **Finding 2**

**Network workstations and servers were not sufficiently protected against malware.**

#### **Analysis**

Network workstations and servers (approximately 220 devices) were not sufficiently protected against malware.

- Three of ten workstations tested were improperly configured with users having administrator rights. Administrator rights are the highest permission level that can be granted to users and it allows users to install software and change configuration settings. As a result, if these workstations were infected with malware, the malware would run with administrator rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights. In addition, as a result of the administrator rights assigned, these three users had the ability to disable the malware protection software on their workstations.
- Workstations and servers tested had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, SLGCA had not updated its workstations and servers for these patches. For example, our test of 13 workstations and servers for one of these software products disclosed that 11 of these devices were running older versions of this software that had not been updated for periods ranging from 4 months to over 3 years.
- Although SLGCA used an enterprise-wide management tool to provide anti-malware software on its workstations and servers, SLGCA did not use the management capabilities of this tool to verify that the malware protection software and related definition files were up to date on its devices. In this regard, SLGCA personnel advised that regular reviews of the management tool's dashboard and reports were not performed. Our test of 10 workstations disclosed that 8 of these workstations were running an outdated version of the anti-malware software and 1 workstation did not have any anti-malware software installed.

The Department of Information Technology (DoIT) *Information Security Policy* states that agencies should configure security settings of information technology products to the most restrictive mode consistent with operational requirements and protect against malicious code by implementing protections that, to the extent possible, include a capability for automatic updates.

## **Recommendation 2**

**We recommend that SLGCA**

- ensure that administrator rights on workstations are restricted to network administrators;**
- promptly install all critical security-related software updates; and**

- c. **monitor all workstations and servers to ensure the devices have malware protection software that is operational and up to date, and that the related definition files are also kept up to date.**

### **Finding 3**

**Mainframe access controls, account and password controls, and security reporting were not sufficient.**

#### **Analysis**

Mainframe access controls, account and password controls, and security reporting were not sufficient.

- As of January 2015, SLGCA had not generated mainframe security and audit event reports since September 2013. As a result, unauthorized or inappropriate activities affecting the integrity of the mainframe data could occur and go undetected by management. A similar condition was commented upon in our preceding audit report.
- Ninety active accounts (assigned to 76 users) had unnecessary access to a mainframe command that permitted these users to bypass menu security controls and directly access specific system screens. This condition may result in unauthorized access to critical mainframe functions, disclosure of sensitive information, or modification of critical production data.
- Six users were improperly granted the ability to make changes to the mainframe's security and auditing settings. As a result of this condition, these six users could initiate unauthorized and inappropriate activities that could affect the integrity of production data on the mainframe computer.
- Mainframe account and password settings did not comply with DoIT Information Security Policy account and password requirements. For example account lockout and password aging were not properly enforced.

The DoIT *Information Security Policy* requires that information systems must generate audit records for all security-relevant events and procedures must be developed to routinely review audit records for indications of unusual activities, suspicious activities, or suspected violations, and to report findings to appropriate officials for prompt resolution. The *Policy* also requires that system access be limited to only authorized individuals and that such access supports the concepts of "least possible privilege" and "need-to-know."

### **Recommendation 3**

**We recommend that SLGCA**

- a. generate reports of all critical mainframe security and audit events, review these reports and investigate unusual events, document these reviews and investigations and retain the documentation for future reference (repeat);**
- b. restrict access to critical mainframe commands and security and audit settings to only those individuals requiring such access; and**
- c. ensure that its mainframe account and password settings are in accordance with the DoIT *Information Security Policy* requirements.**

### **Unclaimed Video Lottery Terminal Funds**

#### **Finding 4**

**SLGCA did not distribute unclaimed video lottery terminal (VLT) funds in a manner consistent with State regulations.**

#### **Analysis**

SLGCA did not distribute unclaimed VLT funds in a manner consistent with State regulations. Although State law does not address how unclaimed VLT funds are to be distributed, State regulations provide that, after 182 days, unclaimed VLT funds shall become the property of the State. Rather than distributing all unclaimed VLT funds to the State, SLGCA distributed these funds in the same manner as specified in the law for VLT gambling proceeds, which are distributed to the State, the casinos, and for other purposes specified in the law. While SLGCA agreed that the regulations, as currently written, specify that unclaimed VLT funds should be distributed to the State, SLGCA also stated that it has always been its intent to distribute these funds in the same manner as VLT proceeds and would seek to revise the regulations accordingly.

VLT play, including wagers and winnings, is automatically recorded by VLTs. At the conclusion of play, each player's balance is recorded and printed on a voucher that the player may redeem at the casino for cash. According to SLGCA records, during calendar year 2013, vouchers totaling \$704,000 went unclaimed for more than 182 days and were distributed in the aforementioned manner to the State and other entities. Of this total, \$347,000 was distributed to non-state entities rather than to the State as provided for by State regulations.

#### **Recommendation 4**

**We recommend that unclaimed VLT funds be distributed to the State unless SLGCA receives approval to amend the regulations to conform with its current practices.**

### **Procurement**

#### **Finding 5**

**SLGCA had not published the award of three contracts, collectively valued at approximately \$106 million, on *eMaryland Marketplace* as required.**

#### **Analysis**

SLGCA had not published the award of three significant contracts on *eMaryland Marketplace* as required by State law. SLGCA awarded these three contracts, which collectively totaled \$106 million, during the period from June 2013 through February 2014; however, as of April 2014 the contract awards had not been published. These contracts were procured for advertising services, design and development of instant ticket games, and the purchase of certain instant lottery ticket machines and related services.

State regulations require that contract awards greater than \$25,000 be published on *eMaryland Marketplace* not more than 30 days after the execution and approval of the contract. After our inquiry, SLGCA published these three awards during May and June 2014.

#### **Recommendation 5**

**We recommend that SLGCA ensure that all applicable contract awards are published on *eMaryland Marketplace* not more than 30 days after the execution and approval of the contract as required.**

## **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 7, 2011 and ending March 19, 2014. 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, and information technology systems. We also determined the status of five of the six findings contained in our preceding audit report.

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. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data). 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 this source 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 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.

SLGCA'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



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

Tel: 410-230-8800  
TTY users call Maryland Relay  
[www.mdlottery.com](http://www.mdlottery.com)

April 13, 2015

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

Dear Mr. Barnickel:

Thank-you for the opportunity to respond to your audit report on the State Lottery and Gaming Control Agency for the period beginning March 7, 2011 and ending March 19, 2014.

Enclosed is our response to the recommendations contained in the audit report. We take these findings seriously and many of the recommendations have already been implemented or are in the process of being implemented.

Please let me know if any additional information is needed.

Sincerely,

Gina M. Smith  
Acting Director

Enclosure

cc: Kimberly Robertson Pannell, Chair, SLGCA Commission

**Finding 1**

**The SLGCA network was not adequately secured from untrusted traffic.**

**Recommendation 1**

**We recommend that SLGCA**

- a. configure its firewalls to achieve a “least privilege” security strategy giving individuals, entities, and devices only those network access privileges needed to perform assigned tasks (repeat);**
- b. use only secure protocols to connect to all firewalls, limit remote access to all firewalls to only authorized source addresses, and configure all firewalls to uniquely identify all individuals performing administrative actions on these firewalls; and**
- c. store firewall logs in a secure location, retain the most recent three months of logs, regularly review these logs, investigate unusual or suspicious log entries, document these reviews and investigations, and retain such documentation for future reference.**

**SLGCA Response:**

SLGCA agrees with the recommendations, and the following changes have or will be implemented.

- a. Problematic configurations identified in the firewall during the audit are ninety percent resolved to meet the principal of least privileged. The remainder of the required changes involves a process of “fine tuning” and will be completed by July of 2015.
- b. Connections to the firewalls have been changed to utilize a secure protocol, remote access to Agency firewalls is restricted to IP addresses of authorized users, and all users are uniquely identified. These changes were implemented in January of 2015.
- c. Firewall logs are retained for 90 days, and documented regular review of the logs is being performed. The retention change and review process was fully implemented in February of 2015.

**Finding 2**

**Network workstations and servers were not sufficiently protected against malware.**

**Recommendation 2**

**We recommend that SLGCA**

- a. ensure that administrator rights on workstations are restricted to network administrators;**
- b. promptly install all critical security-related software updates; and**
- c. monitor all workstations and servers to ensure the devices have malware protection software that is operational and up to date, and that the related definition files are also kept up to date.**

### **SLGCA Response:**

SLGCA agrees with the recommendations, and will ensure that the following items are implemented.

- a. Administrator rights on workstations are restricted to network administrators. Users with local administrative rights that were identified during the audit have been removed.
- b. Critical security updates will be promptly installed. Operating system patches are being installed regularly, and Adobe, Java, and Flash updates will be installed when new versions become available.
- c. Workstations will be actively monitored to ensure malware protection software is operational, up to date, and that related definition files are kept current.

### **Finding 3**

**Mainframe access controls, account and password controls, and security reporting were not sufficient.**

### **Recommendation 3**

**We recommend that SLGCA**

- a. **generate reports of all critical mainframe security and audit events, review these reports and investigate unusual events, document these reviews and investigations and retain the documentation for future reference (repeat);**
- b. **restrict access to critical mainframe commands and security and audit settings to only those individuals requiring such access; and**
- c. **ensure that its mainframe account and password settings are in accordance with the DoIT *Information Security Policy* requirements.**

### **SLGCA Response:**

SLGCA agrees with the recommendations, and the following changes have been implemented.

- a. A security report is being generated daily and is regularly reviewed for unusual events. The reviews are being documented and retained.
- b. Accounts have been reviewed and the appropriate changes were made to ensure accounts adhere to the principle of least privilege.
- c. Mainframe accounts and passwords meet the DoIT Information Security Policy to the extent that the system is capable of meeting the requirement.

**Finding 4**

**SLGCA did not distribute unclaimed video lottery terminal (VLT) funds in a manner consistent with State regulations.**

**Recommendation 4**

**We recommend that unclaimed VLT funds be distributed to the State unless SLGCA receives approval to amend the regulations to conform with its current practices.**

**SLGCA Response:**

The SLGCA has moved forward to change the regulation to reflect its practice. A revised regulation was submitted and approved by the MLGCA Commission on December 16, 2014 and was subsequently published in the Maryland Register on March 20, 2015. The regulation is open for public comment until April 20, 2015.

**Finding 5**

**SLGCA had not published the award of three contracts valued at approximately \$106 million, on *eMaryland Marketplace*, as required.**

**Recommendation 5**

**We recommend that SLGCA ensure that all applicable contract awards are published on *eMaryland Marketplace* not more than 30 days after the execution and approval of the contract as required.**

**SLGCA Response:**

The SLGCA agrees to ensure that all contract awards are published on *eMaryland Marketplace*.

The Request for Proposals (RFPs) for the three contracts in question were all posted on *eMaryland Marketplace* at the time of issuance. For each RFP, Pre-Proposal Conference summary, Question and Answer documents, amendments and other related documents were also posted on *eMaryland Marketplace*.

For large contracts including those in question, the SLGCA requires offerors to submit their proposals by hard copy. The SLGCA does not utilize the *eMaryland Marketplace* functions for electronic offer submission, electronic offer review, or electronic offer selection and posting of awards. Therefore, at the conclusion of a procurement process and after Board of Public Works approval of the award, the SLGCA must go back into the *eMaryland Marketplace* RFP files and post the award information manually.

These were the first large competitive procurements done by the SLGCA since the new *eMaryland Marketplace* system went into effect. The SLGCA believed that it had posted the

awards in *eMaryland Marketplace*. However, when verification of the posting of the awards was requested by the auditors, we were unable to locate such verification on the system so in May/June, we went back into the RFP files and posted the 3 awards.

On September 30, 2014 the SLGCA Director of Procurement attended training provided by DGS on the use of the new *eMaryland Marketplace* system including the procedures for input and posting of various procurement functions on the system.

AUDIT TEAM

**Mark S. Hagenbuch, CPA**

Audit Manager

**Richard L. Carter, CISA**

**Steven P. Jersey, CPA, CISA**

Information Systems Audit Managers

**Joel E. Kleiman, CPA**

Senior Auditor

**Eric Alexander, CPA, CISA**

**Christopher D. Jackson, CISA**

Information Systems Senior Auditors

**Jessica A. Foux**

**Annette L. Manning**

Staff Auditors

**J. Gregory Busch**

Information Systems Staff Auditor