Audit Report

Department of Labor, Licensing and Regulation

Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning

August 2014

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.

- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.

- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.

- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

August 12, 2014

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Labor, Licensing and Regulation (DLLR) – Office of the Secretary, Division of Administration, and Division of Workforce Development and Adult Learning (DWDAL) for the period beginning July 1, 2010 and ending June 30, 2013. The Office of the Secretary and the Division of Administration provide executive oversight, general administration, public information, fiscal services, information technology support, and comprehensive planning for the other DLLR divisions. DWDAL administers various employment and training activities, including certain workforce programs that are primarily funded by the federal government.

Our audit disclosed a number of information technology deficiencies regarding DLLR's network and the Maryland Workforce Exchange (MWE), which is used by job seekers, employers, State personnel, and local partner agencies. Specifically, DLLR's network was not adequately secured because its firewalls and intrusion detection and prevention systems were not properly configured, and current malware protection software had not been installed on all servers and computers. Additionally, DLLR's contract with a third-party service provider for the MWE did not contain critical requirements to protect sensitive data and limit security and operational risks.

We also noted that two DLLR divisions had not established sufficient controls to ensure certain collections were deposited. Additionally, DLLR did not have documentation supporting the propriety of year-end transactions totaling approximately $1 million that were made to reclassify federal, special, and reimbursable expenditures as general fund expenditures. DLLR's unspent general funds would have otherwise reverted to the State's general fund. Finally, DLLR did not adequately monitor adult education and literacy grants.

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

An executive summary of our findings can be found on page 5. DLLR'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 DLLR.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

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

Executive Summary

Legislative Audit Report on the
Department of Labor, Licensing and Regulation
Office of the Secretary, Division of Administration, and Division of Workforce Development and Adult Learning (DLLR)
August 2014

- **Various security and control weaknesses were noted with respect to DLLR's information systems and network. For example, DLLR's network was not adequately secured because its firewalls and intrusion detection and prevention systems were not properly configured, and current malware protection software had not been installed on all servers and computers (Findings 1, 2, and 4).**

  DLLR should take the recommended actions to address the identified security and control weaknesses in its information systems and network. For example, DLLR should perform a documented review of its network security risks and identify how to best apply its intrusion detection and prevention systems.

- **DLLR lacked assurance that its contractor for the Maryland Workforce Exchange (MWE) had adequate information technology security and operational controls. Specifically, the contract did not contain certain critical requirements to protect sensitive data, such as personally identifiable information, and limit operational and security risk (Finding 3).**

  DLLR should initiate efforts to amend the aforementioned contract, as recommended, to protect sensitive data and limit operational and security risks.

- **Cash receipts of two DLLR offices, which totaled $978,700 during fiscal year 2012, were not properly verified to deposit and the responsibilities for certain collections and the related fee waivers were not separated. Additionally, reconciliations of electronic licensing collections with the related State records were not adequately performed or documented. (Findings 5 and 6).**

  DLLR should establish the recommended controls over its cash receipts, including performing documented deposit verifications. DLLR should also maintain documentation to support proper electronic licensing

reconciliations for the Division of Occupational and Professional Licensing and the Division of Financial Regulation.

- **Documentation of certain year-end transactions totaling $1 million did not support the propriety of the reclassification of funds that otherwise would have reverted to the State's General Fund (Finding 7).**

  DLLR should only record year-end transactions that are appropriate and properly supported.

- **Certain grants were not adequately monitored. For example, DLLR did not verify that grant funds were spent in accordance with the grant agreements and did not obtain required annual financial and compliance audits from grantees (Finding 8).**

  DLLR should monitor grant activity, including grant expenditures, and should obtain the required grantee audits.

Background Information

Agency Responsibilities

The Department of Labor, Licensing and Regulation (DLLR) consists of the Office of the Secretary and seven operating divisions. This audit report includes the operations of the following units:

- Office of the Secretary
- Administration
- Workforce Development and Adult Learning

The Office of the Secretary and the Division of Administration provide executive oversight, general administration, public information, fiscal services, information technology support, and comprehensive planning for the other DLLR divisions. The Division of Workforce Development and Adult Learning administers various employment and training activities, including certain workforce programs that are primarily funded by the federal government.

The remaining divisions of DLLR (Unemployment Insurance, Financial Regulation, Labor and Industry, Occupational and Professional Licensing, and Racing) are included within the scope of, and reported upon, in separate audits. According to the State's records, during fiscal year 2013, total DLLR expenditures were approximately $326.7 million, of which $143.3 million related to the three units audited.

Questionable Grant Activity

In May 2012, DLLR was made aware of certain allegations involving questionable activity regarding grants made by the Division of Workforce Development and Adult Learning (DWDAL) and brought the matter to the attention of the Governor's Office. On July 13, 2012, the management employee responsible for the oversight of those grants was terminated. On August 3, 2012, the Department of Health and Mental Hygiene – Office of the Inspector General (DHMH – OIG) was directed by the Governor's Office to conduct an independent special investigation into these allegations. On June 10, 2013, the DHMH – OIG issued a report with numerous findings resulting from:

- programmatic and financial systemic weaknesses,
- a prior undisclosed business relationship between the aforementioned DWDAL management employee responsible for the oversight and

approval of federal sub-recipient grant awards and vendor payments and certain contracted vendors receiving payments from those grant funds, and

- actions on the part of that employee that exceeded the employee's authority.

These conditions contributed to certain questionable grant awards and related payments. For example, DWDAL awarded federal grant funds to two vendors, who over a 52-month period paid approximately $774,000 to the entity with whom the aforementioned DWDAL management employee had a prior undisclosed business relationship. According to the DHMH – OIG report, that entity provided grant writing and other technical assistance to DWDAL staff, including the subject employee, but "no services were delivered directly" to either vendor. The report contained multiple recommendations to strengthen programmatic and financial controls over grant activity and establish and implement policies and procedures to ensure compliance with State Procurement Regulations. On August 1, 2013, DLLR issued a corrective action plan that addressed each of the recommendations and indicated that the majority of the DHMH – OIG recommendations had been implemented and the remaining ones were in progress.

In accordance with State regulations, the alleged questionable grant activity was referred to the Office of the Attorney General – Criminal Division. A referral to the Criminal Division does not mean that a criminal act has actually occurred or that criminal charges will be filed. Additionally, since the grant awards and related payments involved federal funds, we were also advised that DLLR notified the appropriate federal authorities.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the nine findings contained in our preceding audit report dated October 4, 2011. We determined that DLLR satisfactorily addressed seven of the findings. The remaining two findings are repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The Department of Labor, Licensing and Regulation's (DLLR) Office of Information Technology (OIT), within the Division of Administration, provides information technology support for DLLR's divisions. In that capacity, OIT operates and maintains various servers and applications, including DLLR's website that provides several online services, such as occupational and professional licensing registration and renewal, and unemployment insurance applications and ongoing claim submissions. Connectivity for DLLR's applications is provided by an internal computer network and a wide area network for its headquarters locations and several branch offices. DLLR's internal network includes a firewall and an intrusion protection system to provide protection from connections to untrusted networks, including the Internet. In addition, DLLR's Maryland Workforce Exchange system is maintained by a third-party service provider.

Finding 1
DLLR's intrusion detection prevention system was not properly protecting the network.

Analysis

DLLR's intrusion detection prevention system (IDPS) was not properly protecting the network.

- Although DLLR used a network-based IDPS to monitor traffic, the Internet firewall was not configured to transmit all untrusted traffic to the IDPS and, as a result, traffic flowing from several untrusted network segments (including the Internet) to critical internal network devices was not subject to IDPS coverage.

- DLLR did not use host-based intrusion protection systems (HIPS) on critical web servers that processed encrypted traffic. The absence of HIPS coverage for such traffic created a network security risk. Specifically, DLLR's network-based IDPS cannot read encrypted traffic flowing into its network, whereas HIPS can read and analyze such traffic and protect critical web servers from malicious traffic.

Complete IDPS coverage includes the use of a properly-configured, network-based IDPS that is supplemented, where necessary, with HIPS to aid significantly

in the detection and prevention of, and response to, potential network security breaches and attacks.

Recommendation 1
We recommend that DLLR perform a documented review and assessment of its network security risks and identify how IDPS and HIPS coverage should be best applied to its network. Based on this review and assessment, we recommend that DLLR implement IDPS and HIPS coverage as necessary.

Finding 2
Malware protection on DLLR servers and workstations needs improvement.

Analysis
Malware protection on DLLR servers and workstations needs improvement.

- Anti-malware software was not installed on numerous DLLR servers. Specifically, our testing identified that 26 of the approximately 200 servers used by DLLR did not have any malware protection software installed. Additionally, DLLR did not have a formal procedure for ensuring that malware protection software was installed and operating properly on all servers prior to placement of these servers into production.

- Although DLLR used an enterprise-wide management tool to provide malware protection for its servers, DLLR did not use management capabilities of this tool to verify that anti-malware software and related definition files were current on all DLLR servers. Instead, DLLR advised that it manually performed sporadic reviews of servers to verify that anti-malware software and related definition files were current. Furthermore, there was no documentation supporting that these manual reviews were performed.

- The 8 workstations and 2 servers tested had not been updated with the latest releases of anti-malware software. Although current versions of the anti-malware software were available, which provided additional features and fixed some workstation problems, DLLR had not updated the software to the current versions.

Industry best practices recommend that organizations should employ automated tools to continuously monitor workstations, servers, and mobile devices for active up-to-date anti-malware protection.

Recommendation 2
We recommend that DLLR develop and implement enterprise-wide automated procedures to

a. ensure that all servers are configured with anti-malware software that is operating properly; and
b. regularly confirm that anti-malware software and the related definition files are properly updated on its workstations and servers, document these confirmation efforts, and retain documentation for future reference.

Finding 3
DLLR lacked assurance that adequate information technology security and operational controls existed over the Maryland Workforce Exchange.

Analysis
DLLR lacked assurance that adequate information technology security and operational controls existed over the Maryland Workforce Exchange (MWE) that, as of June 1, 2013, was hosted by a third-party service provider. Hosting the MWE system includes maintenance and operation of the related application and database. The MWE is used by job seekers and employers for job placement services, and State personnel and local partner agencies for case management and eligibility determination. The MWE system contains personally identifiable information of members who use this service. Specifically, the database stores the name, address, date of birth, and social security number for each individual. We determined that as of August 26, 2013 there were over 1.4 million active and inactive individuals in this database.

- DLLR's contract with the service provider did not adequately protect DLLR against certain significant information technology security and operational risks. For example, this contract, which expires June 30, 2015, did not require the service provider to perform the following:

    - encrypt data backups, data in transit, and data at rest to prevent improper disclosure or alteration;
    - implement mechanisms for vulnerability testing and patch management;
    - retain and review audit logs recording privileged user access activities, authorized and failed access attempts, system exceptions, and critical information security events;
    - restrict network connections between trusted and untrusted networks and protect networks via properly configured firewalls; and

- submit to periodic independent reviews (including testing) of its information technology security infrastructure and provide DLLR with reports of the results of these reviews.

Without contractual language that addresses the aforementioned responsibilities, DLLR lacked assurance that adequate security controls existed over its data. Best practices established by the Cloud Security Alliance, a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, include detailing the specific responsibilities mentioned above in clear and concise contractual language to limit operational and security risks.

- Although the service provider had obtained a Service Organizational Controls 2 Type I independent review and report covering the MWE's information technology security and operational controls, DLLR had not obtained a copy of the report. We obtained a copy of this independent report and noted that the report did not attest to the information technology controls in effect for the MWE since the review was procedural only and no testing of controls was performed. Furthermore, the independent report did not address several critical information technology controls such as encryption of backups, reviews of firewall configurations, and reviews of reports of privileged user access activities.

  Without periodic independent reviews and reports (that address all critical security concerns and controls and include testing of these controls) of the MWE hosted system, DLLR lacked assurance as to the adequacy of security over the system and its data.

Recommendation 3

We recommend that DLLR

a. initiate efforts to amend the contract to include provisions that address the aforementioned security and operational risks,

b. obtain independent reports covering MWE's information technology security and operational controls,

c. review the reports to verify that testing of all critical security and operational concerns was performed, and

d. ensure that the service provider implements all critical recommendations in the reports.

Finding 4
Adequate controls had not been established over a critical server and database.

Analysis
Adequate controls had not been established over the professional licensing application server and the MWE database.

- A total of 142 active accounts could bypass the structured application menu security on the licensing server and thereby modify critical production programs and files.

- Four users had unnecessary access to several critical commands on the licensing server that allowed these users to make unauthorized security-related changes that could be used to modify DLLR licensing information.

- Reports of logged audit and security-related events (for example, the creation and deletion of master file records) for the licensing server were not reviewed. A similar condition was commented upon in our preceding two audit reports. Furthermore, these reports did not include the activity of 5 critical users and direct modifications to 13 critical data files were not logged.

- For the MWE database, certain key system security and audit-related events (for example granting a privilege) were not monitored, although the capability to perform such monitoring existed. Furthermore, documentation did not exist to support the service provider's review and investigation of the database server's failed logon attempts. Therefore, significant database security violations could go undetected, thus permitting unauthorized or inappropriate activities to adversely affect the integrity of the production database. Similar conditions were commented upon in our two preceding audit reports.

The State of Maryland Department of Information Technology *Information Security Policy* states that agencies must ensure that only authorized individuals have access to confidential information and that such access is strictly controlled, audited, and configured to achieve a "least privilege" security strategy that grants privileges only needed to perform assigned tasks.

Recommendation 4
We recommend that DLLR
a. amend the settings on the aforementioned server to properly limit access to all critical programs and files and to critical server commands to only those individuals who require such access;

b. include the server activity of all critical users in security reports, regularly review these reports, and document and retain such reviews (repeat);
c. log direct modifications to all critical server data files; and
d. ensure that the MWE service provider monitors all key database security and audit events and documents its monitoring of these events including all failed logon attempts (repeat).

Cash Receipts

Background

According to the State's records, DLLR's collections totaled approximately $23 million during fiscal year 2012, consisting of $3.1 million collected through a lockbox account, $9.1 million collected by its divisions and Office of Budget and Fiscal Services (OBFS), and $10.8 million in credit card receipts from electronic licensing activity.

Finding 5
Sufficient controls were not established to ensure that certain collections were deposited.

Analysis

DLLR had not established adequate accountability and control over collections received at OBFS and the Division of Workforce Development and Adult Learning (DWDAL). OBFS cash receipts generally consisted of vendor and grantee refunds and DWDAL cash receipts were for General Education Development (GED) exam fees and grant refunds. According to DLLR's records, during fiscal year 2012, OBFS and DWDAL collected cash receipts totaling approximately $530,500 and $448,200, respectively.

- Collections were not properly verified to deposit. Specifically, OBFS did not use the initial record of receipt to perform the deposit verification. Rather, a subsequently prepared record was used for verification purposes. Additionally, the deposit verifications at DWDAL were not documented by the supervisor responsible for performing the verifications.

- Four DWDAL employees had the ability to waive the $45 GED exam fee and the $5 transcript fee on DLLR's Maryland General Educational Testing System (MGETS) and also had access to GED exam fee collections. Furthermore, exam fee waivers recorded on MGETS were not subject to an

independent verification for propriety. Such lack of separation of duties could result in the misappropriation of funds.

According to the Comptroller of Maryland's *Accounting Procedures Manual*, a verification of cash receipts should be performed from the initial record of receipt to deposit. Furthermore, the *Manual* also requires a separation of cash receipt duties from the related recordkeeping functions.

Recommendation 5
We recommend that DLLR

a. perform documented deposit verifications of collections from the initial receipt document to deposit; and

b. remove the capability to waive GED exam and transcript fees from employees with access to cash receipts, and verify waived fees for propriety on a test basis.

We advised DLLR on accomplishing the necessary separation of duties using existing personnel.

Finding 6
Certain reconciliations of electronic licensing collections were not always properly performed or documented.

Analysis
The reconciliation of licensing collections received through DLLR's website (that is, credit card receipts) with the related bank statements and State records were not always properly performed or documented.

- DLLR did not always document its monthly reconciliation of its records of electronic licensing receipts collected by its Division of Occupational and Professional Licensing (DOPL) with the related bank statements. Although DLLR monitored the electronic licensing activity on a daily basis and used the information to allocate the collections among the boards, DLLR did not always document its reconciliation of the monthly bank statements with its records to ensure all transactions (such as transactions in transit) were accounted for. Our review disclosed that the month-end reconciliation was not documented for 8 of 10 months tested. These reconciliations help ensure the State received credit for the transactions and the receipts were properly allocated among the boards in the State's records. According to DLLR's records, during fiscal year 2012, approximately $10.2 million was collected and allocated to the various DOPL boards.

- DLLR did not reconcile electronic licensing receipts collected by its Division of Financial Regulation (DFR) with the amounts recorded in the State's records. According to electronic licensing bank statements, DFR received approximately $598,000 during fiscal year 2012.

Similar conditions were commented upon in our preceding audit report.

Recommendation 6
We recommend that DLLR

a. maintain documentation to support the reconciliation of DOPL electronic licensing receipts allocated to the boards with the related bank statements (repeat), and

b. perform monthly reconciliations of electronic licensing receipts collected by DFR to ensure all receipts were recorded in the State's records (repeat).

Budgetary Closeout

Finding 7
Documentation of certain year-end transactions did not support the propriety of the reclassification of funds that otherwise would have reverted to the State's General Fund.

Analysis
Documentation of certain year-end transactions totaling $1 million did not support the propriety of the reclassification of federal, special, and reimbursable fund expenditures as general fund expenditures. During the fiscal 2012 and 2011 budgetary closeouts, transactions totaling $535,900 and $506,000, respectively, were recorded to reclassify other fund expenditures as general fund expenditures. At the time of our audit, according to representations of DLLR personnel who processed the reclassifications, these transactions were recorded to avoid reverting unused appropriations to the State's General Fund.

Subsequent to our audit fieldwork, we were advised by DLLR management that the reclassification transactions were recorded to adjust the allocation of general fund appropriations for matching federal grants or to correct general fund expenditures that were previously misapplied to other funds. However, no documentation was provided to support this explanation. There were no similar transactions recorded in fiscal year 2013.

Recommendation 7
We recommend that DLLR only record year-end transactions that are appropriate and properly supported.

Grant Monitoring

Finding 8
Adult education and literacy service grants were not adequately monitored.

Analysis
Adult education and literacy service grants were not adequately monitored. These grants are awarded to educational entities in each jurisdiction (such as, community colleges) to help fund classes for adults who are interested in improving basic skills in reading, writing, and math, or who are learning to speak and understand the English language. The grant awards are funded with both federal funds and State general funds and are based on a formula developed by DLLR's DWDAL that considers both jurisdictional need (based on population data) and demand (based on student enrollment data). According to DWDAL records, there were 30 grant awards totaling approximately $14.6 million, for fiscal year 2013.

- Grantees receiving $500,000 or more in federal funded grant awards are required by the grant agreements to obtain annual financial and compliance audits. However, DWDAL did not obtain and review annual audit reports from three grantees with grant awards totaling $4.6 million (of which $3.3 million was federal funds) for fiscal year 2013. These three grantees were the only ones with grants which exceeded $500,000 in federal funds.

- For those grantees not required to obtain annual audits, DWDAL did not employ alternative procedures to verify that grant funds, which were primarily used for payroll costs, were spent as intended by the grant agreements. Although grantees provided required expenditure reports on a monthly basis, DWDAL did not require the grantees to provide supporting documentation, such as payroll records. Furthermore, DWDAL did not perform periodic site visits to grantees as a means to verify the expenditures. The grant agreements authorize DWDAL to inspect, audit, and examine grantee records.

- DWDAL did not verify the accuracy of annual student enrollment data self-reported by grantees. Annual student enrollment data are used to determine the grantee award amounts.

Recommendation 8

We recommend that DLLR

a. obtain and review annual financial and compliance audits of grantees when required,

b. verify adult education and literacy service grantee expenditures by obtaining supporting documentation or conducting site visits, and

c. verify the accuracy of the grantee's self-reported student enrollment data.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Department of Labor, Licensing and Regulation (DLLR) – Office of the Secretary, Division of Administration, and Division of Workforce Development and Adult Learning for the period beginning July 1, 2010 and ending June 30, 2013. 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 DLLR'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 information system security, cash receipts, payroll, federal funds, procurement and disbursement activities, grants, corporate purchasing cards, and equipment. We also determined the status of the 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 DLLR'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) 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 various sources were sufficiently reliable for the purposes the data were used during this 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.

Our audit included a review of certain support services (for example, payroll, data processing, maintenance of accounting records, and related fiscal functions

including cash receipts processed through DLLR's online licensing system and bank lockbox accounts) provided by DLLR to its divisions.

Our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of DLLR's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including DLLR.

DLLR'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 significant deficiencies in the design or operation of internal control that could adversely affect DLLR'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, and regulations. Other less significant findings were communicated to DLLR that did not warrant inclusion in this report.

DLLR'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 DLLR regarding the results of our review of its response.

STATE OF MARYLAND
DLLR
DEPARTMENT OF LABOR, LICENSING AND REGULATION

APPENDIX

OFFICE OF THE SECRETARY
500 N. Calvert Street, 4th Floor
Baltimore, MD 21202

August 5, 2014

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

Dear Mr. Barnickel:

We are providing this letter as the official agency response to the draft audit report comments and recommendations for the Department of Labor, Licensing and Regulation – Office of the Secretary - Division of Administration and Division of Workforce Development and Adult Learning (DWDAL).

The Department appreciates the thorough examination of the Office of the Secretary - Division of Administration and DWDAL's financial transactions, records and internal controls, and the evaluation of its compliance with applicable State laws, rules and regulations, professionally conducted by your staff. The Agency and Divisions will work toward compliance with the report's recommendations in a manner outlined in the final responses.

Enclosed is our detailed agency response. As requested, an electronic version has also been forwarded by email. If you have any questions regarding this process, please contact me at 410-230-6020.

Sincerely,

Leonard J. Howie III
Secretary

Enclosure

Cc: Scott R. Jensen, Deputy Secretary, DLLR
Julie Squire, Assistant Secretary, DWDAL
Barbara A. Kittrell, Director, Office of Budget and Fiscal Services, DLLR
Samuel K. Smith, Internal Auditor Officer, DLLR

LJH/ss:ms

Department of Labor, Licensing and Regulation
Response to
Draft Legislative Audit Report Dated July 24, 2014

Information Systems Security and Control

Finding 1
DLLR's intrusion detection prevention system was not properly protecting the network.

Recommendation 1
We recommend that DLLR perform a documented review and assessment of its network security risks and identify how IDPS and HIPS coverage should be best applied to its network. Based on this review and assessment, we recommend that DLLR implement IDPS and HIPS coverage as necessary.

Response: **We concur.**

DLLR plans to implement the complete coverage using IDPS. A new firewall was procured after a review and assessment of the network. The new DLLR firewall has a much larger capacity IDPS unit and once it is installed, it will allow us the ability to cover the traffic not being inspected under the current configuration. The new firewall will be installed as part of a comprehensive upgrade/redesign of the DLLR network backbone. The full upgrade is slated to be completed by end of October 2014.

In 2014 DLLR is planning to install a load balancer that has Web Application Firewall capabilities and SSL Acceleration. This will allow DLLR to install the server certificates on the load balancing device thereby allowing it decrypt and inspect the traffic before passing it on to the actual web servers. This solution will obviate the need for the installation of HIPS software on each critical web server receiving encrypted traffic.

Finding 2
Malware protection on DLLR servers and workstations needs improvement.

Recommendation 2
We recommend that DLLR develop and implement enterprise-wide automated procedures to

a. ensure that all servers are configured with anti-malware software that is operating properly; and
b. regularly confirm that anti-malware software and the related definition files are properly updated on its workstations and servers, document these confirmation efforts, and retain documentation for future reference.

Response: **We concur:**

a. DLLR completed installing anti-malware on all the servers in March 2014.

b. DLLR will also document the confirmation efforts and will retain the documentation for future reference. This procedure will be put in place by End of August 2014

Finding 3
DLLR lacked assurance that adequate information technology security and operational controls existed over the Maryland Workforce Exchange.

Recommendation 3
We recommend that DLLR

a. initiate efforts to amend the contract to include provisions that address the aforementioned security and operational risks,
b. obtain independent reports covering MWE's information technology security and operational controls,
c. review the reports to verify that testing of all critical security and operational concerns was performed, and
d. ensure that the service provider implements all critical recommendations in the reports.

Response: **We concur:**

a. **The current contract with the MWE vendor contains neither the scope of service nor the fee structure that would be needed to address the recommended security and operational controls. However, the existing contract is expiring and DLLR is in the process of drafting a new RFP which will address recommendations b, c, and d. DLLR plans to complete the RFP process by April 2015.**

Finding 4
Adequate controls had not been established over a critical server and database.

Recommendation 4
We recommend that DLLR

a. **amend the settings on the aforementioned server to properly limit access to all critical programs and files and to critical server commands to only those individuals who require such access;**
b. **include the server activity of all critical users in security reports, regularly review these reports, and document and retain such reviews (repeat);**
c. **log direct modifications to all critical server data files; and**
d. **ensure that the MWE service provider monitors all key database security and audit events and documents its monitoring of these events including all failed logon attempts (repeat).**

Response: **We concur:**

a. **DLLR is currently implementing a process for logging, reviewing and limiting the access to critical programs, files and commands. DLLR plans to complete this by end of October 2014.**

b. **DLLR completed implementation of a review process for server activity reports in May 2014.**

c. **DLLR is currently implementing a process for logging direct modifications to all critical server data files. DLLR plans to complete this by end of October 2014.**

d. **The current contract is expiring and DLLR is in the process of drafting a new RFP which will address this recommendation. DLLR plans to complete the RFP process by April 2015.**

Cash Receipts

Finding 5
Sufficient controls were not established to ensure that certain collections were deposited.

Recommendation 5
We recommend that DLLR

a. perform documented deposit verifications of collections from the initial receipt document to deposit; and
b. remove the capability to waive GED exam and transcript fees from employees with access to cash receipts, and verify waived fees for propriety on a test basis.

We advised DLLR on accomplishing the necessary separation of duties using existing personnel.

Response: **We concur:**

a. Effective September 12, 2013, DLLR implemented the corrective action to use the daily cash record as the initial receipt document to perform documented verifications. This document is submitted to staff personnel who are independent of the cash receipts function to verify the original log against the validated deposits processed from the bank the following day.

b. As of January 1, 2014 with the conversion of GED testing to a computer based test, all GED exam fees will be collected by GED Testing Services, LLC and not by DLLR's GED testing staff. The GED staff will only collect fees and process fee waivers for transcripts, duplicate diplomas, and related bounced check fees. The greatly reduced volume of fee collections will allow improved segregation of duties between fee collection and fee waiver, and allow a verification of fee waivers process to be implemented. A new segregation of duties and fee waiver verification process will be implemented by September 30, 2014.

Finding 6
Certain reconciliations of electronic licensing collections were not always properly performed or documented.

Recommendation 6
We recommend that DLLR

a. maintain documentation to support the reconciliation of DOPL electronic licensing receipts allocated to the boards with the related bank statements (repeat), and

b. perform monthly reconciliations of electronic licensing receipts collected by DFR to ensure all receipts were recorded in the State's records (repeat).

Response: **We concur.**

a. As of 10/15/13 the reconciliation of the Pay Pal statements to the Merchant bank statements have been documented and verified to the RSTARS e-licensing clearing account. The funds collected have been further allocated among the various Occupational and Professional Licensing Boards based on the daily AS 400 report of licensee registrations. The allocation package which is signed by an independent reviewer includes the merchant statement, the pay pal statement, the report from the AS 400, and a reconciliation to RSTARS. Monthly reconciliations document the comparison of RSTARS and Pay Pal to the Merchant Bank statements and the Merchant Bank statements back to the AS 400.

b. Effective July 2014, the Office of Budget and Fiscal Services (OBFS) shall assist the Division of Financial Regulation (DFR) with the reconciliation of its e-licensing receipts. To ensure that all receipts collected are properly allocated and posted to RSTARS, on a monthly basis, OBFS shall perform an independent review and document the comparison of the RSTARS and Pay Pal to the Merchant Bank statements and the Merchant Bank statements back to the AS 400.

Budgetary Closeout

Finding 7
Documentation of certain year-end transactions did not support the propriety of the reclassification of funds that otherwise would have reverted to the State's General Fund.

Recommendation 7
We recommend that DLLR only record year-end transactions that are appropriate and properly supported.

Response: **We concur:**

DLLR's policy is to process transactions that are appropriate and properly supported according to federal and state requirements. DLLR's accounting structure is very complex and diverse within each division and across the department using various combinations of general, special federal and reimbursable funding. Each fund (federal, special and reimbursable) may have several sub-funds that have separate spending and matching provisions that must be adhered to, and personnel were not always well-versed in those provisions. In fiscal years 2012 and 2013, OBFS eliminated the root cause of this finding by creating the relevant policies and procedures that addressed funding allocation issues, and by implementing a training program for the relevant units.

Grant Monitoring

Finding 8
Adult education and literacy service grants were not adequately monitored.

Recommendation 8
We recommend that DLLR

a. **obtain and review annual financial and compliance audits of grantees when required,**
b. **verify adult education and literacy service grantee expenditures by obtaining supporting documentation or conducting site visits, and**
c. **verify the accuracy of the grantee's self-reported student enrollment data.**

Response: **We concur:**

a. **DLLR will specifically request the annual financial and compliance audits of grantees receiving in excess of $500,000 in federal adult education funds through DLLR (currently the requirement to submit this information is printed in Assurances signed by all grant funded providers at the time of annual application for funds). The audits will be reviewed by the Division of Workforce Development (DWDAL) finance personnel as well as the DLLR Office of Budget and Fiscal Services.**

b. **Historically all grant funded providers have provided a detailed annual financial report which is kept on file at DLLR. This practice will continue in addition to onsite fiscal monitoring and review visits that were implemented in 2013. As of this date, over a third of all grantees have been subject to this intense monitoring of grant funds. Priority programs were selected via a risk analysis checklist that was developed based on a list of risks provided in "Smart Fiscal Management for Adult Education Programs," a training session of the U.S. Department of Education, Office of Vocational and Adult Education and the National Reporting System for Adult Education. All programs will be monitored on a three-year cycle. If there are findings, the Programs will be subjected to regular monitoring until the findings are corrected.**

c. **Grantees report student data by entering demographic, assessment, attendance and achievement information into an online reporting system, as mandated by the National Reporting System for Adult Education. Additionally, the grant administrator for each organization signs a data quality certification annually to provide assurance that the data meets the exemplary quality on all standards issued by the National Reporting System. As of 2014, DLLR will verify the data by randomly selecting student names from the database and verify onsite that enrollment forms and attendance forms signed by the students, along with assessment data are available at the program site. For programs with 500 or fewer students, 5 records will be randomly selected from the database for verification. For programs with more than 500 students, 10 names will be selected for verification.**

AUDIT TEAM

Matthew L. Streett, CPA, CFE
Audit Manager

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

Menachem Katz, CPA
Elaine D. Portnoy
Senior Auditors

R. Brendan Coffey, CPA, CISA
John C. Venturella
Information Systems Senior Auditors

Megan A. Axenfeld
Amanda L. Howell
Jeneba R. Jalloh
Olajide S. Mustapha
Staff Auditors

J. Gregory Busch
Matthew D. Walbert
Information Systems Staff Auditors