

Audit Report

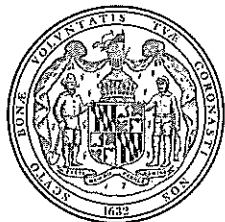
**Department of Labor, Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning**

October 2011



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

Bruce A. Myers, CPA
Legislative Auditor

October 4, 2011

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

Ladies and Gentlemen:

We have audited the following units of the Department of Labor, Licensing and Regulation (DLLR) for the periods noted:

Office of the Secretary and Division of Administration - September 1,
2007 to June 30, 2010

Division of Workforce Development and Adult Learning - July 1, 2008 to
June 30, 2010

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.

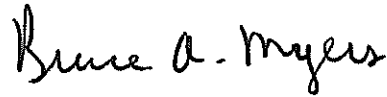
Our audit disclosed a number of information technology deficiencies regarding online services offered on the DLLR website that supports the activities of other DLLR divisions. For example, sensitive personal and financial information from unemployment insurance claimants was not adequately protected, and controls were inadequate over the credit card service provider accounts used to process occupational and professional license fees. Furthermore, logged activity of the electronic licensing website was not reviewed to identify unusual activity.

Two DLLR offices had not established adequate controls over their cash receipts and verifications of collections deposited were not always performed. In addition, although DLLR had fully implemented remote deposit practices, controls were not in place in accordance with guidance issued by the Office of the State Treasurer. Finally, various internal control weaknesses and other procedural deficiencies were noted in the areas of payroll and equipment.

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Other areas in Maryland 877-486-9964

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,

A handwritten signature in black ink that reads "Bruce A. Myers". The signature is written in a cursive, flowing style.

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

Executive Summary	5
Background Information	7
Agency Responsibilities	7
Organizational Changes	7
Status of Findings From Preceding Audit Report	8
Findings and Recommendations	9
Information Systems Security and Control	
* Finding 1 – Sensitive Information for Unemployment Insurance Claims Was Not Adequately Protected	9
* Finding 2 – Proper Security Measures Were Not Established Over the Electronic Licensing Application	11
* Finding 3 – Electronic Licensing Application Was Not Properly Monitored Or Protected	13
* Finding 4 – Adequate Controls Had Not Been Established Over a Critical Server and Database	14
Cash Receipts	
Finding 5 – Sufficient Controls Were Not Established Over Certain Collections	15
Finding 6 – Controls Over Processing Cash Receipts Using Remote Deposit Need Improvement	17
Finding 7 – Reconciliations of Electronic Licensing Collections With Amounts Allocated to Boards or Recorded Were Not Adequate	18
Payroll	
Finding 8 – Controls Over Personnel and Payroll Transactions Were Not Adequate	19
Equipment	
* Finding 9 – Proper Controls Were Not Established Over DLLR’s Equipment	20

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

Audit Scope, Objectives, and Methodology

23

Agency Response

Appendix

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)
October 2011**

- **The Office of Information Technology (OIT), within the Division of Administration, operates and maintains a Department website that provides several online services. Sensitive personal and financial information relating to unemployment insurance claims submitted through the Department's website and processed by DLLR's Division of Unemployment Insurance was not adequately protected. For example, files containing sensitive personal and financial information, including names, social security numbers, and dates of birth, transferred from the Annapolis Data Center to a DLLR server, were not encrypted, and access to the claims records stored on the file server was not properly restricted.**

DLLR should take the recommended actions to adequately protect sensitive personal and financial information related to unemployment insurance claims, including encrypting unemployment insurance claim records in transit and restricting access to the file transfer server.

- **Proper security measures were not established over the electronic licensing application administered by the Divisions of Occupational and Professional Licensing and Financial Regulation. For example, controls over the credit card service provider account used to process occupational and professional license fees were inadequate and appropriate controls were not established over credit transactions. Furthermore, personal information of new licensees on the web server was not sufficiently protected and the website's logged activity was not reviewed to identify unusual activity.**

DLLR should improve security over the electronic licensing application by taking the recommended actions, including improving controls over the credit card service provider account, implementing controls over credit transactions, adequately protecting sensitive personal information of new licensees, and reviewing web server logs and taking appropriate follow-up action.

- **Cash receipts of two DLLR offices, which totaled \$1.2 million during fiscal year 2010, were not adequately controlled. For example, certain collections were not restrictively endorsed and recorded immediately upon receipt, and verifications of deposits were not always performed or were not performed by personnel independent of the cash receipts process. Furthermore, although a remote deposit process was implemented, related controls need to be strengthened.**

DLLR should establish adequate controls, as recommended, over its cash receipts and should establish procedures over the remote deposit process consistent with guidance issued by the Office of the State Treasurer.

- **Internal control and record keeping deficiencies were noted with respect to DLLR's payroll and equipment. For example, individuals who approved online personnel transactions and payroll adjustments did not review related supporting documentation when doing so.**

DLLR should take the recommended actions to improve controls and record keeping in these areas.

Background Information

Agency Responsibilities

The Department of Labor, Licensing and Regulation (DLLR) consists of the Office of the Secretary and the following seven operating divisions:

- Administration
- Workforce Development and Adult Learning
- Unemployment Insurance
- Financial Regulation
- Labor and Industry
- Occupational and Professional Licensing
- Racing

The Office of the Secretary, the Division of Administration, and the Division of Workforce Development and Adult Learning (as of July 1, 2008) are included in the scope of this audit. 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.

According to the State's records, during fiscal year 2010, these three units had operating expenditures totaling approximately \$135.3 million. The remaining Divisions, which are addressed in separate audits, had operating expenditures totaling approximately \$108.2 million.

Organizational Changes

Chapter 134, Laws of Maryland 2008, effective July 1, 2008, transferred the responsibility for Adult Education and Literacy Services, and Education Programs for Correctional Facilities from the Maryland State Department of Education (MSDE) to DLLR's Division of Workforce Development. Furthermore, the law transferred the special fund used for the operation of educational programs in correctional institutions, as well as related federal appropriations, from MSDE to DLLR's Division of Workforce Development. The scope of our audit of DLLR includes these programs beginning July 1, 2008. In the past, these programs were included in the scope of our MSDE audit. Finally, Chapter 309, Laws of Maryland

2009, renamed the Division of Workforce Development to the Division of Workforce Development and Adult Learning, effective July 1, 2009.

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 November 21, 2008, of the Office of the Secretary and the Division of Administration. We determined that DLLR satisfactorily addressed five of these findings. The remaining four findings are repeated as five items in this report. Our preceding audit report of the Division of Workforce Development, dated January 9, 2009, had no findings.

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 the DLLR divisions. In that capacity, OIT operates and maintains various servers and applications, including a Department website that provides several online services, including 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 to provide protection from connections to untrusted networks, including the Internet.

Finding 1

Sensitive information relating to unemployment insurance claims was not adequately protected.

Analysis

Sensitive personal and financial information relating to unemployment insurance claims processed by DLLR's Division of Unemployment Insurance was not adequately protected. In support of the Division of Unemployment Insurance, DLLR's OIT transferred records of initial unemployment insurance claims from a mainframe computer on the State's Annapolis Data Center to a DLLR file transfer server on a daily basis. Two commercial payroll service providers periodically retrieved records from the file transfer server, updated the records, and transferred the records back to the DLLR file transfer server.¹ Files were also transferred from the DLLR file transfer server to a major financial institution to support debit card replenishment for approved unemployment claimants. These files included records containing sensitive personal and financial information (including the

¹ These commercial payroll service providers provide payroll services to numerous employers and, as agents for these employers, report employee separation information to DLLR's Division of Unemployment Insurance (DUI) as required by Maryland law. Periodically, DLLR places separate files of unemployment insurance claims on its file transfer server. The payroll providers extract these files, update the separation information, and submit the files back to DUI for claims processing.

claimants' names, social security numbers, dates of birth, addresses, and income amounts). We noted the following conditions:

- The records for unemployment insurance claims that were retrieved from the State mainframe computer, over the Statewide Intranet network, were transmitted to the DLLR file transfer server in clear text. Specifically, these records were not encrypted even though the mainframe computer software was capable of providing such encryption. This condition was commented upon in our preceding audit report.
- DLLR did not encrypt records for unemployment insurance claims while the information was stored on its file transfer server. This condition was commented upon in our preceding audit report.
- Records transferred over the Internet from the DLLR's file transfer server to two commercial payroll service providers and from these providers back to the file transfer server were encrypted. However, the encryption level used was not adequate for encrypting critical information transmitted across the Internet, increasing the risk that the information could be converted into readable text. This condition was commented upon in our preceding audit report.
- DLLR did not properly restrict access to the unemployment insurance claim records stored on the DLLR file transfer server. Accordingly, each of the two payroll service providers had unnecessary read access to the unemployment insurance claim records pertaining to the other service provider. This condition was commented upon in our preceding audit report. In addition, numerous employee accounts on the State mainframe computer had unnecessary access to the DLLR file transfer server.
- The DLLR file transfer server was not properly protected from unauthorized Internet access. Specifically, traffic from the Internet to this server was not filtered by any device and the server was not located behind the DLLR firewall.

This sensitive personal and financial information is commonly sought by criminals for use in identity theft. Accordingly, appropriate information system security controls, as required by the Department of Information Technology's (DoIT) *Information Security Policy*, need to exist to ensure that this information is safeguarded and not improperly disclosed.

Recommendation 1

We recommend that DLLR

- a. encrypt unemployment insurance claim records in transit and on the DLLR network in compliance with the DoIT's *Information Security Policy* (repeat),**
- b. allow each payroll service provider access to only its unemployment insurance claim information (repeat),**
- c. restrict access to the DLLR file transfer server to only those accounts which require such access, and**
- d. locate the DLLR file transfer server on the internal network behind the DLLR firewall and properly filter all traffic destined for this server.**

Finding 2

Proper security measures were not established over the electronic licensing application.

Analysis

Proper security measures were not established over the electronic licensing application administered by the Divisions of Occupational and Professional Licensing and Financial Regulation. Specifically, we noted the following conditions:

- Controls over the credit card service provider account used to process credit card payments for license fees for the Occupational and Professional Licensing Division were inadequate. A credit card service provider account was used for service management (that is, to manage credit card verification and payment settings), as well as to process credit card payments. Rather, separate accounts should be established for credit card payment transaction processing and service management to provide for an adequate separation of duties and to limit security risks. In addition, the use of this account was not limited to specific Internet addresses. Limiting such access to specific Internet addresses enhances security over who could attempt to use these accounts. Similar conditions were commented upon in our preceding audit report.
- For the Occupational and Professional Licensing Division, the credit card provider account and its password were stored on the web server in plain text, exposing the name and password to anyone capable of accessing these files. A similar condition was commented upon in our preceding audit report.

- Appropriate controls were not established over credit (refund) transactions. Specifically, a maximum credit transaction amount was not established, credit transactions could be greater than the original transaction amounts, and credits could be issued without an original transaction.
- New Occupational and Professional licensees' personal information, including names, addresses, dates of birth, and social security numbers, were unnecessarily stored in plain text log files on the DLLR web server supporting the electronic licensing function. According to DLLR records, during fiscal year 2010, personal information for 19,918 individuals was recorded in these log files. This information is commonly sought by criminals for use in identity theft. This condition was commented upon in our preceding audit report.
- The electronic licensing web server account was granted unnecessary modification access to critical files. Such unnecessary access included modification access to the host server's system registry that contains the settings for the server and resident applications. Proper internal control requires that web server accounts be granted limited access to sensitive system resources, to reduce security risks and attacks. A similar condition was commented upon in our preceding audit report.
- The electronic licensing web application account and passwords settings were not in compliance with DoIT's *Information Security Policy* requirements. Specifically, account lockout was not enabled, password complexity was not enforced, and the password minimum length was set at only four characters.

Recommendation 2

We recommend that DLLR

- use separate credit card service provider accounts for credit card payment processing and service management (repeat);**
- restrict the use of its credit card service provider service management account to only authorized Internet addresses (repeat);**
- either encrypt the credit card provider account name and related password on the web server or remove them from the web server (repeat);**
- limit credit amounts and require that credits be less than, or equal to, previous transaction amounts;**
- either encrypt the plain text log files containing new licensee personal information or remove the log files from the web server (repeat);**
- limit the electronic licensing web server account's access to critical files to only those files needed to perform required operations (repeat); and**

- g. ensure that the electronic licensing web application account and password settings are in compliance with the DoIT's *Information Security Policy* requirements.**

Finding 3

The electronic licensing system was not properly monitored or protected from external threats.

Analysis

The electronic licensing system was not properly monitored or protected from external threats. Specifically, we noted the following conditions:

- Reviews of the website's logged activity to identify any unusual events and trends in activity were not performed. The only reviews performed were to monitor the extent of website usage, and these reviews were only performed on a monthly basis and were not documented. A similar comment was made in our preceding audit report.
- Web application security tools were not used to help protect the electronic licensing application and backend database. Specifically, web application vulnerability scanning software had not been used to help identify the existence of potentially serious security vulnerabilities within the application's program code, and although basic firewalls were used for the network, a web application firewall was not used to provide enhanced protection over the application and backend database.
- There were unusually high levels of website traffic originating from suspicious sources (traffic from Latvia). This suspicious traffic occurred during August 2010, March 2010, and September 2009 and was also identified during our prior audit. Since the application's logging was limited, the exact nature of this traffic could not be determined. Because DLLR did not use web application security tools, as mentioned above, the application's vulnerability to a web-based attack is unknown. During a web-based attack, sensitive information residing on the backend database could be subject to modification or disclosure.

Recommendation 3

We recommend that DLLR

- a. perform weekly, documented reviews of web server log files, expanded to include unusual events and trends in activity (repeat);**

- b. pursue any unusual events or trends identified to ascertain if there has been any system compromise and take all actions necessary if a compromise has occurred;**
- c. enhance application logging capabilities to help identify the nature and specifics of any attacks;**
- d. assess the costs and benefits of using a web application firewall to help protect the electronic licensing system;**
- e. periodically utilize web application security tools to help identify any web application software vulnerabilities and remediate all confirmed critical vulnerabilities; and**
- f. for past suspicious website traffic, consider obtaining the services of a computer system forensic expert to determine if any sensitive information has been compromised.**

Finding 4

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

Analysis

Adequate controls had not been established over a critical server and database. Specifically, we noted the following conditions:

- Account, password, and access controls over the professional licensing application server were not sufficient to properly secure the server and did not comply with DoIT's *Information Security Policy*. In this regard, users' workstations allowed for automatic connection to the server with the system rights of a workstation's owner. Accordingly, anyone with physical access to a workstation could access the server with the workstation owner's rights, such as to add or modify accounts. In addition, 7 accounts were using default passwords (where the userids were the same as the passwords), 21 accounts had not been used for periods up to 603 days, and 7 accounts belonged to terminated employees.
- For the professional licensing application server, two individuals had conflicting duties regarding security functions and programming. As a result, these two individuals had complete system access and control over this server.
- For the professional licensing application server, certain security-related operations were not logged (for example, the creation and deletion of master file records). In addition, for events that were logged, DLLR did not have

documentation of the reviews performed for these events. A similar condition was commented upon in our preceding audit report.

- For a critical database, certain key system security and audit-related events (for example granting a privilege) were not logged, although the capability to perform such logging existed. Furthermore, documentation did not exist to support DLLR'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. A similar condition was commented upon in our preceding audit report.

DoIT's *Information Security Policy* establishes the minimum security standards, including access, account, password, and monitoring controls, for information technology systems in the State.

Recommendation 4

We recommend that DLLR comply with DoIT's *Information Security Policy* and establish adequate access, account, password, and monitoring controls over the aforementioned professional licensing application server and database. We made detailed recommendations, which if implemented, should provide for adequate controls in these areas (repeat).

Cash Receipts

Background

According to the State's records, DLLR's collections totaled approximately \$22.6 million during fiscal year 2010, consisting of \$3.3 million collected through the DLLR lockbox account, \$10.3 million collected by DLLR divisions and DLLR's Office of Budget and Fiscal Services, and \$9 million in credit card receipts from electronic licensing activity.

Finding 5

Sufficient controls were not established over certain collections.

Analysis

DLLR had not established adequate accountability and control over collections received at DLLR's Office of Budget and Fiscal Services (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

transcript release fees. According to DLLR's records, these two locations directly collected and deposited cash receipts totaling approximately \$1.2 million during fiscal year 2010 (approximately \$761,000 at OBFS and approximately \$459,000 at DWDAL). Specifically, our review disclosed the following deficiencies:

- Mail-in check receipts and walk-in collections received by OBFS and DWDAL were not always restrictively endorsed immediately upon receipt.
- DWDAL collections were not recorded immediately upon receipt and were not timely deposited. Before recordation, these collections were stored in a locked cabinet awaiting deposit. We were advised that the collections were often not recorded for up to a month after receipt. In addition, our test of 10 days of collections, totaling approximately \$21,000, disclosed that all collections were deposited between 13 and 31 business days after recordation.
- Deposit verifications were not performed for DWDAL collections, and the deposit verifications at OBFS were not adequately documented, were not performed by personnel independent of the cash receipts process, and were not made using the initial record of receipt. Although our limited testing at both locations did not disclose any improprieties, because of DLLR's failure to perform adequate deposit verifications, one instance was disclosed during the audit period in which DWDAL receipts totaling \$1,130 were not deposited until five months after being recorded.
- Six 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. The lack of segregation of duties over these functions could result in the misappropriation of funds.

According to the Comptroller of Maryland—General Accounting Division's *Accounting Procedures Manual*, checks and money orders are to be restrictively endorsed immediately upon receipt. Furthermore, cash receipts are to be recorded immediately upon receipt and should be deposited no later than the first working day after the day of receipt. Finally, a verification of cash receipts from initial recordation to deposit is to be performed by an employee independent of the cash receipts function.

Recommendation 5

We recommend that DLLR

- a. restrictively endorse all checks and money orders immediately upon receipt;**
- b. record collections immediately upon receipt and deposit collections within a one working day;**
- c. perform documented deposit verifications of collections from the initial receipt document to deposit by an employee independent of the related collections; and**
- d. 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.**

Finding 6

Controls over processing cash receipts using remote deposit need improvement.

Analysis

Controls over processing cash receipts using remote deposit need improvement. The remote deposit process allows DLLR to electronically scan the images of cash receipts (that is, checks and money orders) and electronically transmit the images to the State's bank for deposit instead of physically taking the receipts to the bank for deposit. With approval from the State Treasurer's Office, DLLR began implementing the remote deposit process in November 2009 and, by February 2010, the remote deposit process was fully implemented in all divisions. For example, our review noted the following conditions:

- Cash receipts deposited through the remote deposit system in the Office of Budget and Fiscal Services (OBFS) were not safeguarded after being processed and awaiting destruction. In this regard, these cash receipts were maintained in an unsecured file folder located under an employee's desk, instead of being locked in a secure location, such as a safe.
- Cash receipts deposited remotely in the Division of Workforce Development and Adult Learning (DWDAL) were not voided after they had been processed and, as of October 25, 2010, DWDAL had not destroyed any cash receipts processed through remote deposit system since it began using it in February 2010.
- DLLR has not developed formal written procedures outlining the proper controls over the use of the remote deposit system by DLLR's divisions.

The Office of the State Treasurer's *Policy on the Use of Remote Deposit Services by Maryland State Agencies* establishes controls that State agencies should have in place over the remote deposit process. For example, cash receipts should be secured both before and after scanning until the checks are destroyed, scanned and transmitted cash receipts should be marked as void after the bank has accepted the scanned images, and the accepted cash receipts should be stored no longer than 30 days before they are destroyed. Although the aforementioned policy was not formally issued until June 2010, DLLR should have consulted with the Office of the State Treasurer to implement proper controls.

Recommendation 6

We recommend that DLLR

- a. comply with the State Treasurer's *Policy on the Use of Remote Deposit Services by Maryland State Agencies*; and**
- b. establish written procedures, consistent with the State Treasurer's *Policy*, describing the proper controls over the use of the remote deposit system by each DLLR division.**

Finding 7

Reconciliations of electronic licensing collections with the amounts allocated to the various boards or recorded in State records were not adequate.

Analysis

Electronic licensing collections received through the DLLR website were not properly reconciled to the amounts allocated to the various boards or recorded in State's records. Specifically, our review disclosed the following conditions:

- DLLR did not adequately reconcile electronic licensing receipts of the Division of Occupational and Professional Licensing (DOPL) with the allocation of the receipts among its various boards. According to DLLR's licensing records, approximately \$9 million was collected during fiscal year 2010 and approximately \$9.2 million was allocated to the DOPL boards. Although DLLR performed a monthly reconciliation of the amounts received and allocated, supporting documentation for these reconciliations was not maintained, and DLLR could not adequately explain this difference.
- DLLR did not reconcile electronic licensing receipts collected by DLLR's Division of Financial Regulation (DFR) with the amounts recorded in the State's records. During the period September 2007 to June 2010,

approximately \$14.1 million was recorded as DFR electronic licensing revenue.

Recommendation 7

We recommend that DLLR

- a. maintain documentation to support a proper reconciliation of DOPL electronic licensing receipts with amounts allocation to the boards,**
- b. perform monthly reconciliations of electronic licensing revenues collected by DFR to ensure all revenues were properly accounted for in the State's records, and**
- c. investigate the aforementioned difference and take appropriate corrective action.**

Payroll

Finding 8

Controls over personnel and payroll transactions were not adequate.

Analysis

DLLR had not established adequate controls over its personnel, payroll, and time and leave transactions. According to State records, DLLR employed approximately 1,675 regular and 311 contractual employees as of June 30, 2010, and payroll expenditures totaled approximately \$122.8 million during fiscal year 2010 for all DLLR units. Specifically, our review disclosed the following conditions:

- The individuals responsible for approving online personnel transactions (such as adding or deleting employees, and salary adjustments) and the individuals responsible for approving payroll adjustments (such as payments for overtime and unused sick leave) did not review supporting documentation. Rather, these individuals relied on the reviews performed by the individuals responsible for initiating these transactions. As a result, there is an increased risk of improper transactions being processed.
- Although DLLR received quarterly reports from the Comptroller of Maryland's Central Payroll Bureau (CPB) of DLLR employees that appeared on multiple State payrolls (for example, worked for both DLLR and another State agency), DLLR did not investigate employees appearing on the reports to ensure the propriety of the payroll payments. During the period from April 2008 to June 2010, a total of 60 employees appeared on CPB's multiple payroll reports; payments made by DLLR to these employees during this

period totaled approximately \$599,000 and payments made by other state agencies totaled approximately \$545,200. While our limited test of these payrolls disclosed no overlapping hours, without a thorough review, DLLR cannot ensure these payments are proper. CPB requires State agencies to investigate all employees appearing on these reports to ensure the employees are not claiming hours for multiple jobs during the same time periods.

- Certain employees had the capability to electronically approve their own timesheets on DLLR's time and leave accounting system. Specifically, during the period from January 2009 through June 2010, 28 employees prepared and approved their own timesheets. Six of these employees approved their own timesheet between 11 and 40 times. Additionally, there was no independent approval of timesheet adjustments and leave adjustments processed by six other employees who had full system access to DLLR's time and leave accounting system. These employees had the ability to modify their access, as well as other employees' access to the system; initiate and approve timesheets; and process adjustments to leave records.

Recommendation 8

We recommend that DLLR

- a. ensure that the individuals responsible for approving personnel transactions and payroll adjustments review supporting documentation, at least on a test basis;**
- b. review the quarterly CPB reports, properly investigate all employees on multiple State payrolls, and take appropriate action when overlapping hours are identified;**
- c. ensure that the individuals cannot both prepare and approve timesheets on DLLR's electronic time and leave accounting system; and**
- d. ensure that time and leave transactions processed by employees with full system access are independently reviewed, at least on a test basis, and that such review is documented and retained for future reference.**

Equipment

Finding 9

Proper controls were not established over DLLR's equipment.

DLLR had not established adequate controls over its equipment and related record keeping functions, nor did its physical inventory procedures comply with certain provisions of the Department of General Services' (DGS) *Inventory Control Manual*. As of June 30, 2010, the book value of DLLR's equipment reported on

the State's records totaled approximately \$18.3 million. Our review disclosed the following conditions:

- Proper separation of duties was not established over the record keeping and equipment custody functions. Specifically, three employees had custodial responsibilities over certain DLLR equipment and also had the ability to update the automated detail equipment records.
- DLLR did not maintain an independent control account as required. Specifically, activity posted to DLLR's control account for equipment additions, disposals, and adjustments was obtained from the detail equipment records and not from an independent source. A control account is a continuous summary of transactions and serves as a total dollar value control over amounts in the detail equipment records.
- We were advised that physical inventories were conducted annually by various equipment officers who are responsible for equipment in their respective locations, along with a representative from DLLR's Office of General Services; however, inventory count sheets did not contain documentation of who conducted the physical inventories. Additionally, our test of four locations, with equipment totaling approximately \$2.3 million, disclosed that adequate documentation did not exist to determine if the most recent inventory counts were reconciled to the related detail records; furthermore, any related missing items were not reported to the Department of General Services (DGS). According to the detailed records, as of September 29, 2010, we determined that equipment items totaling approximately \$174,800 from these four locations had not been inventoried in the past year, indicating items may be missing. Furthermore, inventory count sheets to support the inventory results were not available for one location with equipment totaling approximately \$806,300.

Similar conditions related to the control account and physical inventories have been commented upon in our preceding audit reports on DLLR since 1996. The Department of General Services' (DGS) *Inventory Control Manual* requires that the duties of inventory record keeping, custodian, and physical inventory taking be segregated. In addition, the *Manual* requires that a control account and detail records be properly maintained for equipment and that the control account be reconciled at least quarterly with the aggregate balance of the detail records. The inventory results should be reconciled to the detail records, and discrepancies should be investigated and resolved. Based on the inventory results, equipment items that cannot be resolved should be reported to DGS following proper investigation.

Recommendation 9

We recommend that DLLR

- a. establish proper segregation of duties between the functions of record keeping and equipment custody;**
- b. establish and maintain an independent control account, periodically document a reconciliation of the account to the related detail records, and investigate any discrepancies (repeat);**
- c. reconcile the physical inventory counts to the detail records in a timely manner;**
- d. maintain support of the physical inventories including count sheets, documentation of who performed the inventories, and the reconciliation of the counts to the detail records; and**
- e. investigate and resolve discrepancies between the inventory results and the detail records, including the reporting of missing or stolen items to DGS and the removal of the items from the detail records, as necessary (repeat).**

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

Audit Scope, Objectives, and Methodology

We have audited the Department of Labor, Licensing and Regulation – Office of the Secretary and Division of Administration for the period beginning September 1, 2007 and ending June 30, 2010, as well as the Division of Workforce Development and Adult Learning for the period beginning July 1, 2008 and ending June 30, 2010. 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. We also determined the status of the findings contained in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. The areas addressed by the audit included information system security, cash receipts, payroll, federal funds, purchasing and disbursement activities, and equipment. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DLLR's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

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

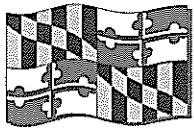
assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

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

September 27, 2011

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, Maryland 21201

RE: Department of Labor, Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and
Adult Learning
Responses to Draft Legislative Audit Report
Dated August 2011

Dear Mr. Myers:

Enclosed you will find the Department of Labor, Licensing and Regulation's responses to your draft report covering the examination of accounts and records of our Office of the Secretary, Division of Administration and Division of Workforce Development and Adult Learning.

Very truly yours,

Alexander M. Sanchez
Secretary

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

Information Systems Security and Control

Finding 1

Sensitive information relating to unemployment insurance claims was not adequately protected.

Recommendation 1

We recommend that DLLR

- a. encrypt unemployment insurance claim records in transit and on the DLLR network in compliance with the DoIT's *Information Security Policy* (repeat),**
- b. allow each payroll service provider access to only its unemployment insurance claim information (repeat),**
- c. restrict access to the DLLR file transfer server to only those accounts which require such access, and**
- d. locate the DLLR file transfer server on the internal network behind the DLLR firewall and properly filter all traffic destined for this server.**

Response: We concur. DLLR will increase protection of sensitive information relating to unemployment insurance claims. Specifically:

- a. DLLR will encrypt UI claim records in transit and on the DLLR network in compliance with DoIT's Information Security Policy. This is scheduled to be implemented 12/11.
- b. DLLR will allow each payroll service provider to be able to access only their own UI claim information. This is scheduled to be implemented 12/11.
- c. DLLR restricted access to the file transfer server to only those accounts requiring access. This recommendation was implemented.
- d. The file transfer server will be moved behind the firewall by 12/11. All traffic destined to this server is now properly filtered.

Finding 2

Proper security measures were not established over the electronic licensing application.

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

Recommendation 2

We recommend that DLLR

- a. use separate credit card service provider accounts for credit card payment processing and service management (repeat);**
- b. restrict the use of its credit card service provider service management account to only authorized Internet addresses (repeat);**
- c. either encrypt the credit card provider account name and related password on the web server or remove them from the web server (repeat);**
- d. limit credit amounts and require that credits be less than, or equal to, previous transaction amounts;**
- e. either encrypt the plain text log files containing new licensee personal information or remove the log files from the web server (repeat);**
- f. limit the electronic licensing web server account's access to critical files to only those files needed to perform required operations (repeat); and**
- g. ensure that the electronic licensing web application account and password settings are in compliance with the DoIT's *Information Security Policy* requirements.**

Response: We concur. DLLR will establish proper security measures over the electronic licensing application. Specifically:

- a. Separate credit card service provider accounts for credit card payment processing and service management are now used.
- b. The use of its credit card service provider service management account is now restricted to only authorized Internet addresses.
- c. The credit card provider account name was removed from the web server.
- d. Credit amounts are limited and credits must be less than, or equal to, the previous transaction amounts.
- e. The plain text log files containing new licensee personal information were removed from the web server.
- f. The electronic licensing web server account's access to critical files was limited to only those files needed to perform required operations.

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- g. DLLR is currently investigating the ramifications of making the electronic licensing web application account and password settings in compliance with the DoIT's Information Security Policy requirements.

Finding 3

The electronic licensing system was not properly monitored or protected from external threats.

Recommendation 3

We recommend that DLLR

- a. perform weekly, documented reviews of web server log files, expanded to include unusual events and trends in activity (repeat);**
- b. pursue any unusual events or trends identified to ascertain if there has been any system compromise and take all actions necessary if a compromise has occurred;**
- c. enhance application logging capabilities to help identify the nature and specifics of any attacks;**
- d. assess the costs and benefits of using a web application firewall to help protect the electronic licensing system;**
- e. periodically utilize web application security tools to help identify any web application software vulnerabilities and remediate all confirmed critical vulnerabilities; and**
- f. for past suspicious website traffic, consider obtaining the services of a computer system forensic expert to determine if any sensitive information has been compromised.**

Response: We concur. DLLR will improve the monitoring and protection of the electronic licensing system. Specifically:

- a. Weekly, documented reviews of web server log files, expanded to include unusual events and trends in activity are now performed.
- b. Unusual events or trends identified and necessary actions are taken.
- c. Logging capabilities were improved to help identify the nature and specifics of any attacks.
- d. DLLR is in the process of assessing the costs and benefits of using a web application firewall to help protect the electronic licensing system.

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- e. DLLR will periodically utilize web application security tools to identify any web application software vulnerabilities and will remediate all confirmed critical vulnerabilities.
- f. DLLR now uses IBM as computer system forensic expert to determine whether any sensitive information was compromised.

Finding 4

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

Recommendation 4

We recommend that DLLR comply with DoIT's *Information Security Policy* and establish adequate access, account, password, and monitoring controls over the aforementioned professional licensing application server and database. We made detailed recommendations, which if implemented, should provide for adequate controls in these areas (repeat).

Response: We concur. DLLR improved the controls over a critical server and database. DLLR implemented the detailed recommendations made by OLA. DLLR established adequate access, account, password, and monitoring controls over the professional licensing application server and database.

Cash Receipts

Finding 5

Sufficient controls were not established over certain collections.

Recommendation 5

We recommend that DLLR

- a. restrictively endorse all checks and money orders immediately upon receipt as required by GAD;
- b. record collections immediately upon receipt and deposit collections in a timely manner as required by GAD;

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- c. perform documented deposit verifications of collections from the initial receipt document to deposit by an individual independent of the related collections; and**
- d. 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.**

Response: We concur. DLLR will provide training to appropriate personnel in order to ensure the current written policies are understood and incorporated into the Division's policies and procedures. Further, we emphasized the critical need to process items more quickly and promptly forward the paperwork to Accounting. Specifically:

- a. We reissued the procedural memo to all cash receipts personnel & directors, reiterating the need to restrictively endorse checks immediately upon receipt
- b. We advised the Division of the GAD requirement to record all collections within two (2) business days of receipt. Also, "a." above addresses this issue.
- c. Deposit verifications are now performed and documented by staff independent of the cash receipt process. Also, DWDAL explored additional funding and implemented procedural changes to assist with GED staffing issues. This ensures compliance with cash receipts processing time requirements and improves processing time for cash receipts.
- d. The GED staff involved in processing cash receipts no longer have the authority to process fee waivers in the MGETS System. Fee waivers are now handled by the GED Staff Specialists, based on the authorization of the Deputy Assistant Secretary of Adult Education and the Director of the GED program. The waiver of exam fees is now verified by staff independent of the waiver process.

Finding 6 Controls over processing cash receipts using remote deposit need improvement.
--

Recommendation 6

We recommend that DLLR

- a. comply with the State Treasurer's *Policy on the Use of Remote Deposit Services by Maryland State Agencies*; and**

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- b. establish written procedures, based on the aforementioned State Treasurer's policy, outlining the proper controls over the use of the remote deposit system by each DLLR division.**

Response: We concur. We will comply with the State Treasurer's Policy on the Use of Remote Deposit Services by Maryland State Agencies policy issued on 06/15/10. We will modify our written procedures, provided to the auditors during the audit, outlining the proper controls over the use of the remote deposit system by each DLLR division, based on the aforementioned State Treasurer's policy. Specifically:

- a. We are in the process of establishing the approval hierarchy necessary to be in compliance with the Treasurer's policy.
- b. The aforementioned DLLR formal written policy was drafted and issued to ALL remote deposit users. It will be reissued after inclusion of the recommended modifications.

Finding 7

Reconciliations of electronic licensing collections with the amounts allocated to the various boards or recorded in State records were not adequate.

Recommendation 7

We recommend that DLLR

- a. maintain documentation to support a proper reconciliation of DOPL electronic licensing receipts with amounts allocation to the boards,**
- b. perform monthly reconciliations of electronic licensing revenues collected by DFR to ensure all revenues were properly accounted for in the State's records, and**
- c. investigate the aforementioned difference and take appropriate corrective action.**

Response: We concur. DLLR will provide training to appropriate personnel in order to ensure current written policies are understood and incorporated into the division's policies and procedures. Recent staffing and procedural changes greatly improved the process by which these accounts are reconciled and validated. In addition, we will confer with the legislative auditors as we move forward with measures to streamline and better document the process. Specifically:

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- a. We will ensure identified discrepancies are properly noted and documented when performing the reconciliation.
- b. In the future, General Accounting will work with IT to obtain the necessary reports and begin performing the reconciliation of the Financial Regulation e-licensing receipts to ensure all receipts collected are properly allocated and posted to R*STARS.
- c. We will comply with the auditors' recommendation and investigate the aforementioned difference and take appropriate corrective action.

Payroll

Finding 8

Controls over personnel and payroll transactions were not adequate.

Recommendation 8

We recommend that DLLR

- a. ensure that the individuals responsible for approving personnel transactions and payroll adjustments review supporting documentation, at least on a test basis;
- b. review the quarterly CPB reports, properly investigate all employees on multiple State payrolls, and take appropriate action when overlapping hours are identified;
- c. ensure that the individuals cannot both prepare and approve timesheets on DLLR's electronic time and leave accounting system; and
- d. ensure that time and leave transactions processed by employees with full system access are independently reviewed, at least on a test basis, and that such review is documented and retained for future reference.

Response: We concur:

- a. Our Office of Human Resources will continue to approve personnel transactions and payroll time reports. The Office of Human Resources initiated changes in the process to ensure individuals responsible for approving personnel transactions (such as, adding or deleting employees, and salary adjustments) review supporting documentation, at least on a test basis. In addition, they will continue to work with DBM to improve the processes and systematic programming errors within MD Time.

**Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011**

- b. The Office of Human Resources will review the quarterly CPB reports, investigate all employees on multiple State payrolls and take appropriate corrective action when overlapping hours are identified;
- c. The Office of Human Resources will continue to work with supervisors and programmers to ensure individuals cannot both prepare and approve timesheets on DLLR's electronic time and leave accounting system;
- d. The Office of Human Resources will ensure time and leave transactions processed by employees with full system access are independently reviewed, at least on a test basis and such reviews are documented and retained for future reference.

Equipment

Finding 9

Proper controls were not established over DLLR's equipment.

Recommendation 9

We recommend that DLLR

- a. **establish proper segregation of duties between the functions of record keeping and equipment custody;**
- b. **establish and maintain an independent control account, periodically document a reconciliation of the account to the related detail records, and investigate any discrepancies (repeat);**
- c. **reconcile the physical inventory counts to the detail records in a timely manner;**
- d. **maintain support of the physical inventories including count sheets, documentation of who performed the inventories, and the reconciliation of the counts to the detail records; and**
- e. **investigate and resolve discrepancies between the inventory results and the detail records, including the reporting of missing or stolen items to DGS and the removal of the items from the detail records, as necessary (repeat).**

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

Response: We concur.

Department of Labor Licensing and Regulation
Office of the Secretary
Division of Administration
Division of Workforce Development and Adult Learning
Draft Legislative Audit Report, Dated August 2011
Responses to Draft Legislative Audit
September, 2011

- a. As of June 2010, two employees in the Inventory Unit of OGS were able to update records. The Property Manager could view but not update records. Another employee, who moved to the Deputy Director position within OGS, still had the update ability for technical support, but did not have custodial responsibilities over DLLR equipment. Custodial responsibilities for equipment are delegated to the accountable officers in the various DLLR units, and these individuals do not have access to the detail records residing in the ATRACK system.
- b. The Office of Budget and Fiscal Services will confer with the legislative auditors to ascertain the appropriate method to maintain a control account which is independent from the detail records. In addition, we will ensure these accounts are reconciled on at least a quarterly basis and all discrepancies are resolved and documented.
- c. DLLR will develop a sign-off sheet for accountable officers who assist the OGS Inventory personnel in performing physical inventories. This sign-off sheet will become part of the count sheet documentation. The accountable officer's name is currently in the ATRACK system associated with each equipment item.
- d. DLLR will develop a system to maintain support of the physical inventories including count sheets, documentation of who performed the inventories, and the reconciliation of the counts to the detail records; and
- e. OGS recognizes follow-ups to physical inventories need to be standard operating procedure in order to reconcile the detailed records. Our efforts in the past proved the data acquired through an initial physical inventory yields a list of possible missing items, but a follow-up inventory significantly decreases or eliminates this list. OGS is aggressively setting procedures in place to perform follow-up inventories to enable yearly reconciliation.

AUDIT TEAM

Matthew L. Streett, CPA, CFE
Audit Manager

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

Nelson W. Hopkins, CPA
Rick E. Pyles
Senior Auditors

Omar A. Gonzalez, CPA
Albert E. Schmidt, CPA
Information Systems Senior Auditors

Eoghan J. Doherty
Alexander M. Prodey
Timothy S. Rice
Staff Auditors

Eric Alexander
Michael K. Bliss
Christopher D. Jackson
Jeffrey T. Zankowitz
Information Systems Staff Auditors