Audit Report

Department of Labor, Licensing and Regulation

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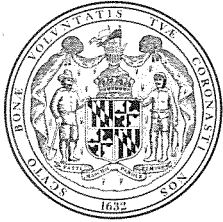**Division of Workforce Development and Adult Learning**

August 2017

For further information concerning this report contact:

Warren G. Deschenaux
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

August 7, 2017

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

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Labor,
Licensing and Regulation (DLLR) – Office of the Secretary, Division of
Administration, and the Division of Workforce Development and Adult Learning
(DWDAL) for the period beginning July 1, 2013 and ending August 16, 2016.
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 that appropriate safeguards were not established to protect
sensitive personally identifiable information of licensees in a critical server. In
addition, there was no disaster recovery plan for the recovery of DLLR
information system operations. Also, password, account, and malware protection
controls were not sufficient to properly protect DLLR's network.

Additionally, DLLR could not substantiate approximately $9.9 million in federal
fund revenues recorded at the end of fiscal year 2016, and could not substantiate
that any of the funds had been recovered. The revenue related to receivables
recorded for indirect costs incurred during fiscal years 2014, 2015, and 2016 for
several federal programs. Because of the length of the reimbursement delays, the
extent to which funds will be received is uncertain and State general funds may be
needed to eliminate the resulting deficits.

We also noted that DLLR did not publish contract awards totaling $12 million on
eMaryland Marketplace as required. Finally, DLLR did not reconcile credit card
collections received through its website for the Division of Financial Regulation

with amounts recorded in the State's accounting records and the related bank statements. Such collections totaled $2.4 million during fiscal year 2016.

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**

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
- Division of Administration
- Division of 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 funded primarily by the federal government.

According to the State's records, during fiscal year 2016, total DLLR expenditures were approximately $330.6 million, of which $115.5 million related to the three units audited.

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.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the eight findings contained in our preceding audit report dated August 12, 2014. We determined that DLLR satisfactorily addressed seven of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background
The Department of Labor, Licensing and Regulation (DLLR) Office of Information Technology (OIT) was solely responsible for the Department's information technology (IT) support until DLLR began using the State of Maryland Department of Information Technology's (DoIT) IT support services, as follows:

- During June 2016, DLLR began using the DoIT firewalls including network and IT security services (such as firewall and intrusion detection prevention systems operations and maintenance).
- During August 2016, DLLR began receiving IT service desk assistance, hardware support, and software support (including malware protection support).

OIT operates several critical computer applications and databases on DoIT supported hardware and on the Comptroller of Maryland's Annapolis Data Center mainframe. These applications include online services such as occupational and professional licensing registration and renewal, and unemployment insurance applications and ongoing claim submissions. DoIT operates a statewide network for DLLR that connects DLLR's local branch offices and the DLLR headquarters. The statewide network provides DLLR users access to various information technology services including the aforementioned services, network services, email services, and Internet access. In addition, DLLR's Maryland Workforce Exchange system is maintained by a third-party service provider.

Finding 1
Licensees' sensitive personally identifiable information (PII) was stored without adequate safeguards.

Analysis
DLLR inappropriately stored sensitive PII in clear text. Specifically, as of November 29, 2016, we determined that a critical server contained 23 licensing files that contained 589,836 unique social security numbers (SSN) in clear text along with full names of licensees and dates of birth. In addition, we were advised that this sensitive PII was not protected by other substantial mitigating controls. Furthermore, DLLR had not performed an inventory of its systems to

identify all sensitive PII, determined if it was necessary to retain the PII, and deleted PII identified as unnecessary.

PII is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that PII is safeguarded and not improperly disclosed.

The State of Maryland *Information Security Policy* requires that agencies protect confidential data using encryption technologies and/or other substantial mitigating controls.

Recommendation 1
We recommend that DLLR
a.   **perform an inventory of its systems and identify all sensitive PII,**
b.   **determine if it is necessary to retain this PII and delete all unnecessary PII,**
c.   **determine if all necessary PII is properly protected by encryption or other substantial mitigating controls, and**
d.   **use approved encryption algorithms to encrypt all sensitive PII not otherwise properly protected.**

Finding 2
DLLR did not have an information technology disaster recovery plan (DRP) for the recovery of its information systems operations.

Analysis
DLLR did not have an information technology DRP for recovering computer operations from disaster scenarios (for example a fire). The State of Maryland *Information Technology (IT) Disaster Recovery Guidelines* provide best practices on the minimum required elements needed for a DRP. Examples of minimum required elements include alternate site processing arrangements, required hardware and software components, and restoring network connectivity.

Without a complete and tested DRP, a disaster could cause significant delays (for an undetermined period of time) in restoring information systems operations above and beyond the expected delays that would exist in a planned recovery scenario.

Recommendation 2
We recommend that DLLR, in conjunction with DoIT, create a comprehensive DRP that covers all of its information technology operations

and is in compliance with the best practices identified in the *IT Disaster Recovery Guidelines*.

Finding 3
Password, account, and malware protection controls were not sufficient to properly protect DLLR's network.

Analysis
Password, account, and malware protection controls were not sufficient to properly protect DLLR's network. Specifically, we noted the following conditions:

- Domain password and account settings were not sufficient to properly protect DLLR's network. For example, we noted that domain passwords were not subject to any complexity requirements and never expired. As a result, passwords could be easily compromised and accounts could be used inappropriately for extended periods. The State of Maryland *Information Security Policy* specifies requirements for passwords and accounts including password complexity and age requirements.

- We identified 239 DoIT supported workstations whose users had administrative rights over these workstations. None of these users were network or system administrators, or had been specifically authorized in writing to have such rights. Administrative rights are the highest permission level that can be granted to users and allow users to install software and change configuration settings. If these workstations were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights. In addition, we identified 31 additional workstations with the local administrators group defined to include a large number of individuals who did not require this privilege.

- Certain DoIT supported workstations had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, DoIT had not updated these workstations for these patches. For example, we identified 1,862 instances of an outdated commonly vulnerable application on the DoIT supported DLLR workstations with some of the instances in excess of five years old.

Recommendation 3
We recommend that DLLR, in conjunction with DoIT,
a. **establish password and account settings in accordance with the aforementioned State of Maryland *Information Security Policy*;**
b. **limit the assignment of administrative rights on workstations to system and network administrators and those users specifically allowed such rights, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether such rights are still needed; and**
c. **ensure that all workstations are kept up-to-date for critical security-related updates for commonly vulnerable applications.**

Federal Funds

Finding 4
DLLR could not substantiate approximately $9.9 million in federal fund revenues recorded at the end of fiscal year 2016, and could not substantiate that any funds had been received.

Analysis
DLLR could not substantiate approximately $9.9 million in federal fund revenues recorded at the end of fiscal year 2016, and could not substantiate that any of the funds had been received as of January 2017. This revenue related to receivables recorded for indirect costs incurred and uncollected during fiscal years 2014, 2015, and 2016 for several federal programs. Because of the length of the reimbursement delays, the extent to which the amounts outstanding will be received is uncertain.

DLLR management could not provide any documentation to support how the recorded amounts were determined or that any of the funds had been received. While DLLR management advised us that a portion of the fiscal year 2014 revenue was recovered, as of January 2017, DLLR personnel could not provide any documentation of the receipt of funds. DLLR management advised us that DLLR is currently working with the federal granting agency to recover the amounts outstanding. To the extent that recorded federal fund revenues are not received, general funds may be needed to eliminate the remaining deficits. This issue was commented upon in our January 25, 2017 report on the Statewide Review of Budget Closeout Transactions for Fiscal Year 2016.

Recommendation 4
We recommend that DLLR
a. **ensure that all year-end revenue transactions are properly supported, and**
b. **continue its efforts with the federal granting agency to recover the aforementioned revenues.**

Contract Procurements

Finding 5
DLLR did not publish contract awards totaling $12 million on *eMaryland Marketplace* as required.

Analysis
DLLR did not always publish contract awards on *eMaryland Marketplace* (*eMM*) as required by State laws and regulations. *eMM* is an Internet-based, interactive procurement system managed by the Department of General Services. We tested eight information technology, maintenance, and professional services contract awards made by DLLR during the period from May 2014 through December 2016, which totaled approximately $12 million. As of February 2017, none of the eight contract awards had been published on *eMM* as required. Individually, these contracts ranged in value from $33,000 to $9.4 million.

State laws and regulations generally provide that *eMM* is to be used by State agencies to publish awards greater than $25,000 within 30 days of the award. Publishing awards on *eMM* provides transparency over State procurements including information about the winning bidder and the amount of the related award.

Recommendation 5
We recommend that DLLR comply with State laws and procurement regulations by publishing contract awards on *eMM* within 30 days of the contract award.

Cash Receipts

Finding 6
DLLR did not reconcile electronic receipts collected by its Division of Financial Regulation (DFR) with amounts recorded in the State's accounting records and with the related bank statements.

Analysis
DLLR did not perform monthly reconciliations of electronic collections received through its website (that is, credit card receipts) for DFR with amounts recorded in the State's accounting records and with the related bank statements. Specifically, as of September 2016, the only reconciliation conducted was for the month of June 2016. Furthermore, this June 2016 reconciliation was not comprehensive because it did not include a verification of foreclosed property registration fee collections with the original source documents (that is, detailed transaction reports). As a result, assurance was lacking that the State was properly credited for all of DFR's electronic receipts and that the receipts were properly accounted for.

DFR collects credit card payments primarily for fees associated with business licenses (such as for banks and consumer lenders) and for the registration of foreclosed properties. According to DLLR's records, DFR collections totaled approximately $2.4 million during fiscal year 2016, which included foreclosed property registration fees of approximately $950,000. Similar conditions were commented upon in our two preceding audit reports.

Recommendation 6
We recommend that DLLR
a. **perform monthly reconciliations of DFR electronic licensing receipt collections with related bank statements and receipts recorded in the State's records (repeat), and**
b. **ensure the reconciliations are comprehensive.**

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, 2013 and ending August 16, 2016. 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, and grants. Our audit included a review of certain support services (such as 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. We also determined the status of the findings contained in our preceding audit report.

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

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. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these sources were sufficiently reliable for the purposes the data were used during this audit. We also extracted data from DLLR's automated online financial systems for the purpose of testing certain areas, such as electronic licensing collections. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

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 to be 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, or 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

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

August 3, 2017

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 120
Baltimore, MD 21202

Dear Mr. Barnickel,

The Department of Labor, Licensing and Regulation (Dept. of Labor) respectfully submits the enclosed response to the Office of Legislative Auditor's (OLA) report on the Office of the Secretary (OOS), Office of Administration, (OOA) and Division of Workforce Development and Adult Learning, (DWDAL) for the period beginning July 1, 2013 and ending August 16, 2016.

Of the six (6) audit findings, the department has initiated measures to strengthen internal controls and improve processes to mitigate deficiencies identified in the July 2017 audit report.

The Department of Labor would like to thank the audit staff who conducted the audit of the OOS, OOA and DWDAL. Their professionalism and respect to our staff and processes is much appreciated.

Should you have any questions, feel free to contact me or Deputy Secretary McGlone of my office.

Best Regards,

Kelly M. Schulz
Secretary

KMS/dm/jma

Information Systems Security and Control

> **Finding 1**
> **Licensees' sensitive personally identifiable information (PII) was stored without adequate safeguards.**

Recommendation 1
We recommend that DLLR
a. **perform an inventory of its systems and identify all sensitive PII,**
b. **determine if it is necessary to retain this PII and delete all unnecessary PII,**
c. **determine if all necessary PII is properly protected by encryption or other substantial mitigating controls, and**
d. **use approved encryption algorithms to encrypt all sensitive PII not otherwise properly protected.**

DLLR Response:

DLLR Agrees with this finding. The agency is currently working on an inventory of systems containing PII that will be completed by August 31, 2017. Once the inventory is complete the IT division will review with the departments having ownership of the data and determine whether it is still required. The agency is also capturing information on encryption status and purging policies on the PII data during the inventory. Purging policies will be implemented where possible and a review if effort/cost will be done for any unencrypted PII data found. Any unencrypted data will be likely be associated with legacy systems that are at or near end of life. A determination will be made if it is of best benefit to encrypt the older end of life systems or to pursue replacements that will have encryption in place. The complete analysis will be completed by the end of December, 2017.

> **Finding 2**
> **DLLR did not have an information technology disaster recovery plan (DRP) for the recovery of its information systems operations.**

Recommendation 2
We recommend that DLLR, in conjunction with DoIT, create a comprehensive DRP that covers all of its information technology operations and is in compliance with the best practices identified in the *IT Disaster Recovery Guidelines*.

DLLR Response:

DLLR and DoIT agree with this finding. DLLR is in the process of being migrated into DoIT's Enterprise, so a discussion and review of timelines for completion of the migration will have to be reviewed to determine the best course for implementing an effective disaster recovery plan; that is whether one should be implemented in DLLR's current system, or one put in place at the time DLLR is migrated to DoIT's data center. DLLR and DoIT have already begun some initial discussions and fact finding exercises to begin the process. A complete disaster recovery plan should be completed within 12 to 18 months depending on the option chosen for implementation.

Finding 3
Password, account, and malware protection controls were not sufficient to properly protect DLLR's network.

Recommendation 3
We recommend that DLLR, in conjunction with DoIT,
a. **establish password and account settings in accordance with the aforementioned State of Maryland *Information Security Policy*;**
b. **limit the assignment of administrative rights on workstations to system and network administrators and those users specifically allowed such rights, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether such rights are still needed; and**
c. **ensure that all workstations are kept up-to-date for critical security-related updates for commonly vulnerable applications.**

DLLR Response:

DLLR and DoIT agree with this finding. The correct Group Policy Object (GPO) for enforcing password policy will be back in place by September 30, 2017. DLLR is also working with DoIT to ensure that all workstations are under their patch management program and will continue to receive future patches and application updates on a regular basis. DLLR and DoIT will also review user rights to workstations to remove any unnecessary privileges and to document any instances where the elevated privileges are required. An annual review of the users/systems with elevated privileges will be conducted on an annual basis going forward. The patch management and user rights review will be completed by December 31. 2017.

2

Federal Funds

> **Finding 4**
> **DLLR could not substantiate approximately $9.9 million in federal fund revenues recorded at the end of fiscal year 2016, and could not substantiate that any funds had been received.**

Recommendation 4
We recommend that DLLR
a. **ensure that all year-end revenue transactions are properly supported, and**
b. **continue its efforts with the federal granting agency to recover the aforementioned revenues.**

DLLR Response:

The Department of Labor, Licensing and Regulation concurs with the recommendations. The agency acknowledges the federal fund revenues (Schedule G) submitted for SFY 2016 reflected a $9.9M federal fund receivable that raises concern regarding whether the full amount is collectable.

For reimbursement of indirect costs, the agency uses a fixed rate with carry-forward provision. This U.S. Department of Labor (USDOL) approved method establishes an indirect rate that will be charged to future federal programs to recover the indirect federal costs.

On July 27, 2017, the agency received approval of its previously submitted indirect cost rate, submitted in December 2016. During the next 120 days, the agency plans to submit two additional indirect cost rates for approval, bringing the submissions current. The recently approved indirect cost rate verifies carryforward amounts for two periods – fiscal year ending 2015 of $3,890,350 and fiscal year ending 2016 of $1,391,569. These carryover amounts total $5,281,919 and will be recovered in the current fiscal year. Under this method of indirect cost reimbursement, the carryforward amount in the indirect receivable figure for the federal fund revenues of the closing statement does not meet the definition of the Comptroller's closing receivable. The Comptroller defines accrued revenues as both measurable and available to liquidate liabilities within 60 days. This reimbursement will occur during the full fiscal year.

Of the $9.9M federal receivable documented in the closing federal fund revenues for SFY 2016, $5.282M is in the process of collection as the carryover portion of the current approved indirect rate. The remaining balance of $4.618M will

require a deficiency appropriation. The agency has determined that it failed to properly allocate the indirect expenditures according to the approved indirect cost rate proposals for several of the past fiscal years which led to the need for a deficiency appropriation. The agency will continue its analysis and corrective actions and work with their control agencies to finalize a deficiency appropriation.

Lastly, the agency acknowledges it is unacceptable that management could not provide the appropriate supporting documentation or substantiate receipt of federal funds. Appropriate personnel action is being taken to ensure managers are held accountable for the actions resulting in this finding and that it does not reoccur. Additional training in revenue accounting, along with fiscal grants management, will be scheduled for all fiscal managers and supervisors.

Contract Procurements

Finding 5
DLLR did not publish contract awards totaling $12 million on *eMaryland Marketplace* as required.

Recommendation 5
We recommend that DLLR comply with State laws and procurement regulations by publishing contract awards on *eMM* within 30 days of the contract award.

DLLR Response:

The Department of Labor, Licensing and Regulation agrees with the recommendation. The agency will ensure that all contract awards over $25,000 are published on eMarylandMarketplace.

The agency did notify all offerors of contract awards by letter and corrected previous award notifications via eMaryland Marketplace on February 17, 2017.

Cash Receipts

Finding 6
DLLR did not reconcile electronic receipts collected by its Division of Financial Regulation (DFR) with amounts recorded in the State's accounting records and with the related bank statements.

Recommendation 6
We recommend that DLLR
a. **perform monthly reconciliations of DFR electronic licensing receipt collections with related bank statements and receipts recorded in the State's records (repeat), and**
b. **ensure the reconciliations are comprehensive.**

DLLR Response:

The Department of Labor, Licensing and Regulation concurs with the recommendations. The agency has performed all monthly reconciliations, through May 2017 and June 2017 is in process. The reconciliation is four way and comprehensive, including all information from the official source documents detailed in the audit. All receipts will be properly accounted for through a review of source documents and any discrepancies will be noted and followed through including those noted in the audit.

Audit Team

Matthew L. Streett, CPA, CFE
Audit Manager

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

Jonathan H. Finglass, CPA
Senior Auditor

R. Brendan Coffey, CPA, CISA
Edwin L. Paul, CPA, CISA
Information Systems Senior Auditors

James J. Podhorniak, CPA, CFE
Anthony V. Calcagno
Stephanie A. Laciny
Nidhi S. Lakhanpal
Staff Auditors

Robert H. Dean
Justin P. Vlahacos
Information Systems Staff Auditors