Audit Report

Department of Labor, Licensing and Regulation
Office of the Secretary
Division of Administration

November 2008

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

November 21, 2008

Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Department of Labor, Licensing and Regulation – Office of the Secretary and Division of Administration (DLLR) for the period beginning August 1, 2004 and ending August 31, 2007. 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.

Our audit disclosed that available security features were not fully used to enhance controls over information systems and DLLR's website, which is used to issue and renew occupational and professional licenses and collect the related fees. For example, DLLR's network security over the electronic licensing application process was not adequate, allowing unauthorized users the ability to view license applicants' confidential information.

We also noted that that DLLR did not timely recover approximately $540,000 in federal expenditures, resulting in lost interest income, and DLLR recorded $10.4 million in unsupported accrued federal revenue transactions at the close of fiscal years 2005 and 2006. Proper internal controls were not in place over purchasing and disbursement transactions, as well as cash receipts and equipment.

An executive summary of our findings can be found on page 5 and DLLR's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us by DLLR personnel during the course of this audit.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

Information Systems Security and Control

Purchases and Disbursements

Federal Funds

Cash Receipts

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

Executive Summary

Legislative Audit Report on the
Department of Labor, Licensing and Regulation
Office of the Secretary and Division of Administration (DLLR)
November 2008

- **DLLR did not establish adequate security over its computer network. For example, network level access was allowed from all internal network addresses and an insecure connection protocol was used for remote administrative access to two critical network devices.**

  DLLR should take the recommended actions to improve security over its computer network.

- **Sensitive information for initial unemployment insurance claims, processed by DLLR's Unemployment Insurance Division, was not adequately protected. For example, claim records sent over the Statewide Intranet and transferred over the Internet to and from commercial payroll service providers were not adequately encrypted.**

  DLLR should ensure that unemployment insurance claims records are adequately encrypted.

- **Security measures over the electronic licensing application administered by DLLR's Divisions of Occupational and Professional Licensing and Financial Regulation were inadequate. For example, controls over credit card service provider accounts were inadequate and certain licensee personal information on the web server was stored in plain text.**

  DLLR should take the recommended actions to improve security over the electronic licensing application.

- **Proper internal controls were not established over the processing of purchasing and disbursement transactions to ensure adequate approval of all transactions. As a result, DLLR employees could modify transactions after the related approvals were obtained.**

  DLLR should establish online approval requirements over all critical documents to ensure critical transactions are not modified after approvals are obtained.

- **DLLR’s procedures to ensure that all federal funds were recovered timely were inadequate. Approximately $540,000 in expenditures was not recovered timely resulting in approximately $18,000 of lost investment income. In addition, DLLR recorded accrued revenues totaling $10.4 million to eliminate federal fund deficits without ensuring that the related amounts were actually due from federal grants.**

  DLLR should ensure that all federal funds are recovered in a timely manner, and should ensure that all accrued revenue transactions are adequately supported.

- **DLLR did not establish adequate controls over cash receipts and equipment. For example, DLLR had not properly investigated and resolved missing sensitive equipment (such as computers) costing $614,538.**

  DLLR should establish the recommended controls in these areas, including investigating all missing equipment and taking appropriate corrective action.

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

The Office of the Secretary and the Division of Administration are included in the scope of this audit and, according to the State's records, had operating expenditures totaling approximately $28.2 million during fiscal year 2007. These two divisions provide executive oversight, general administration, public information, fiscal services, information technology support, and comprehensive planning for the other DLLR divisions. According to the State's records, total expenditures for these other divisions were $145.4 million during fiscal year 2007.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the 15 findings contained in our preceding audit report dated June 9, 2005. We determined that DLLR had satisfactorily resolved 14 of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

DLLR's Office of Information Technology operates and maintains various servers and applications to support all divisions, including certain file transfer responsibilities related to the Division of Unemployment Insurance and an agency website that provides online licensing services to the Divisions of Occupational and Professional Licensing and Financial Regulation. 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 un-trusted networks, including the Internet. According to DLLR's records, the Divisions of Occupational and Professional Licensing and Financial Regulation oversee more than 200,000 licensees. Fiscal year 2007 Office of Information Technology expenditures totaled approximately $6 million, according to the State's records.

Finding 1
Security over DLLR's computer network was not adequate.

Analysis

Security over DLLR's internal network, which hosts numerous critical servers, was not adequate. Specifically, we noted the following conditions:

- Network level access was allowed from all of DLLR's internal network addresses (including employee workstations) to many critical DLLR servers over all protocols and ports. As a result, these internal computer resources were exposed to risks of improper access and modification.

- An insecure connection protocol was used for administrative access to two of DLLR's critical network router devices. As a result, usernames and passwords used to obtain administrative access to these devices moved across the network in clear text.

- A management service used to maintain and monitor DLLR's core network router used widely known default values to connect to this device. Accordingly, there was increased risk that the device, which provided wide area network connectivity, could be compromised and network services disrupted.

Recommendation 1

We recommend that network level access to DLLR's critical servers be restricted to only those network addresses requiring such access over required protocols and ports. We further recommend that remote management services which access and monitor critical network devices use only secure communications protocols. Finally, we recommend that the default values used by a critical management service to connect to the core router be changed.

Finding 2

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

Analysis

Sensitive personal and financial information relating to initial unemployment insurance claims processed by DLLR's Unemployment Insurance Division was not adequately protected. Specifically, we noted the following conditions:

- On a daily basis, initial unemployment insurance claim records were retrieved from a mainframe computer, over the Statewide Intranet network, and 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.

- DLLR did not encrypt unemployment insurance claim records while the information was stored on its file transfer server.

- Records transferred over the Internet from DLLR's file transfer server to three commercial payroll service providers, and from these providers to the file transfer server (after the service providers had updated their records), were encrypted. However, the encryption level used was not adequate for critical information transmitted across the Internet, increasing the risk that the information could be converted into readable text. These records include sensitive personal and financial information (such as the claimants' names, social security numbers, and income amounts).

- DLLR did not properly restrict access to the unemployment insurance claim records stored on the DLLR file transfer server. Accordingly, each one of the three payroll service providers had unnecessary read access to the unemployment insurance claim records pertaining to the other two service providers.

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

Recommendation 2
We recommend that unemployment insurance claim records in transit or on the DLLR network be encrypted in compliance with the Department of Information Technology's *Acceptable Encryption Policy*. We also recommend that DLLR allow each payroll service provider access to only its unemployment insurance claimant information.

Finding 3
Security measures over the electronic licensing application were inadequate.

Analysis
Web server security measures over the electronic licensing application administered by the Divisions of Occupational and Professional Licensing and Financial Regulation were inadequate. Specifically, we noted the following conditions:

- Controls over the credit card service provider accounts used to process credit card payments for license fees were inadequate. We noted that a single credit card service provider account was used by the Division of Occupational and Professional Licensing to manage credit card verification and payment settings, and to process credit card payments. A similar account was used by the Division of Financial Regulation. Separate accounts should be established for credit card payment transaction processing and for service management to limit security risks. In addition, the use of these accounts was not limited to specific Internet addresses, which would enhance security over who could attempt to use these accounts. These service provider account names and passwords were also stored in plain text on the web server computer, exposing the names and passwords to anyone capable of accessing these files, and one of these accounts could still be used by a terminated employee. Finally, this account was also used by an employee who reconciled license information with bank and credit card service provider reports and, accordingly, improper refunds could be processed without detection.

- New occupational and professional licensee personal information, including names, addresses, dates of birth, and social security numbers, was unnecessarily stored in plain text on the DLLR web server that supported the licensing function. According to DLLR records, during fiscal year 2007, personal information for 26,401 individuals was recorded in this server's files. This information is commonly sought by criminals for use in identity theft.

- The licensing web server account was granted excessive modification access to critical files. Proper internal control requires that web server accounts be granted limited access to sensitive system resources to reduce security risks and attacks.

- There was no documentation to support DLLR's claim that the licensing web server logs were periodically reviewed by agency personnel to identify and investigate noteworthy security-related events.

Recommendation 3
We recommend that DLLR improve security over its electronic licensing application. Specifically, we made detailed recommendations, which if implemented, should provide for adequate security over the electronic licensing application.

Finding 4
DLLR did not adequately log security events, monitor security reports, and document security reviews and investigations.

Analysis
DLLR did not adequately log security events, monitor security reports and document security reviews and investigations. Specifically, we noted the following conditions:

- The occupational and professional licensing application server was not properly configured to log certain critical security events. For example, authorization failures and changes to user accounts were not logged. In addition, documentation frequently did not exist to support DLLR's review and investigation of security events that were recorded on security reports. Accordingly, significant system activities, such as unauthorized access attempts, changes to user accounts, and direct modifications of critical data files may not be detected.

- For a critical database containing personal information for job seekers, certain key system security and audit-related events 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, permitting unauthorized or inappropriate activities to adversely affect the integrity of the production database.

Best practices for security control and monitoring provide that agencies should ensure that information is accessed by the appropriate persons for authorized use only. This should be accomplished by establishing an audit trail process to ensure accountability of system and security-related events and a review process of security audit logs, incident reports, and online reports, at least one time per business day, using automated tools to facilitate the review where possible.

Recommendation 4
We recommend that DLLR log critical security server and database events, review all relevant security logs, investigate events where necessary, document these reviews and investigations, and retain this documentation for audit verification purposes.

Finding 5
Access controls, segregation of critical functions, and account and password controls were not adequate.

Analysis
Access controls, segregation of critical functions, and account and password controls were not adequate. Specifically, we noted the following conditions:

- A default administrative database account had full access to a critical database. Since this account, by default, includes local server administrators, all local administrators on the server hosting this database had full administrative access to this database. In addition, anyone able to achieve local administrator privileges would automatically have full administrative access to this database and could perform modifications to critical data.

- Security settings for the occupational and professional licensing application server gave 52 accounts (including programmer accounts) unrestricted access to a critical program library. As a result, these accounts could make undetected changes to programs before the programs were placed into production. Accordingly, erroneous or unauthorized changes to critical production programs could occur without management’s knowledge and approval.

- For the occupational and professional licensing application server, three individuals had conflicting duties regarding security functions, programming, and operations. As a result, these three individuals had complete system access and control over this server. Furthermore, we noted that two of these individuals shared a common userid, which removes individual accountability for any actions performed.

- Network account and password controls were not adequate. For example, the network security settings did not enforce account lockout, password length, password complexity, password history, and password aging. Accordingly, control settings for accounts and passwords did not provide adequate authentication and access controls.

Recommendation 5
We recommend that DLLR implement adequate access controls, segregation of critical functions and account and password controls. Specifically, we made detailed recommendations, which if implemented, should provide for adequate controls in these areas.

Purchases and Disbursements

Finding 6
Proper internal controls were not established over the processing of purchasing and disbursement transactions.

Analysis
Proper internal controls were not established over the automated processing of purchasing and disbursement transactions to ensure an adequate approval of all transactions. For example, DLLR established online approval rules over certain critical procurement and disbursement transactions, including purchase orders. However, these rules permitted the return of the documents to the employees initiating the transactions after the independent approvals were obtained. As a result, five employees who had the ability to initiate these transactions could modify the transactions after the related approvals were obtained without detection. During fiscal year 2007, DLLR used the State's accounting system to process disbursements totaling approximately $64 million.

Recommendation 6
We recommend that DLLR establish online approval requirements over all critical documents that ensure all critical transactions are subject to adequate supervisory review and approval, including ensuring that these transactions are not modified after approvals are obtained.

Federal Funds

Finding 7
DLLR did not have adequate procedures to ensure all federal expenditures were recovered timely, resulting in lost investment income of $18,000. In addition, $10.4 million in accrued federal fund revenues were not supported.

Analysis
DLLR did not have adequate procedures to ensure all federal fund expenditures were recovered timely, and certain federal fund revenues were accrued without being supported. According to the State's records, DLLR's fiscal year 2007 federal fund expenditures totaled approximately $116 million. Specifically, we noted the following conditions:

- DLLR did not have adequate procedures to ensure all federal expenditures were recovered in a timely manner. DLLR maintained an automated system to account for federal fund activity, which was used for reporting activity to the federal granting agencies and for processing related federal fund reimbursement requests. However, DLLR did not ensure that all federal fund expenditures, which serve as the basis for the reimbursement requests, were recorded in its automated system. As a result, as of March 2008, DLLR failed to identify approximately $540,000 in fiscal year 2007 federal fund expenditures that should have been submitted for reimbursement. The failure to request reimbursement of these funds on a timely basis resulted in a loss of investment income to the State of approximately $18,000. DLLR management advised us that these funds were recovered shortly after we brought this omission to its attention. State budget law provides that, to the extent consistent with federal requirements, federal funds should be used before State funds are charged.

- DLLR could not support accrued revenue transactions totaling $10.4 million. Specifically, our review of five year-end accrued revenue transactions processed during the close of fiscal years 2005 and 2006 disclosed that DLLR could not support the transactions. DLLR management advised us that it accrued these revenues to eliminate federal fund deficits without ensuring that the related amounts were actually due from federal grants. While DLLR ultimately recovered these funds from the respective grants, this practice violated the State's fiscal year-end closing instructions issued by the Comptroller of the Treasury's General Accounting Division. These instructions require that detailed documentation of accrued revenues be maintained by agencies to support their accounting transactions.

Recommendation 7
We recommend that DLLR establish procedures to ensure that all federal expenditures are properly identified and recovered in a timely manner. We also recommend that, in the future, DLLR ensure that all accrued revenue transactions are adequately supported.

Cash Receipts

Finding 8
DLLR did not independently investigate and resolve certain deposit adjustments and did not record certain collections in the State's accounting system in a timely manner.

Analysis
DLLR's Office of Budget and Fiscal Services (OBFS) did not independently investigate and resolve certain deposit adjustments and did not always record collections in the State's accounting system in a timely manner. Specifically, the employee who investigated and resolved deposit adjustments for collections received by mail (for example, for checks returned for insufficient funds) was involved in processing the related collections. Because of this lack of separation of duties, there was a lack of assurance that all recorded adjustments were proper, and misappropriation and other discrepancies could occur without detection. In addition, collections received by mail were not always recorded in the State's accounting system in a timely manner. Specifically, 13 of the 15 items tested, totaling approximately $10.2 million, including one $10.1 million check, were recorded in the State's accounting system from 4 to 43 days after the dates of deposit. The Comptroller of the Treasury's *Accounting Procedures Manual* requires that cash receipts be recorded within two business days of the deposit to facilitate the reconciliation of the State's bank accounts.

DLLR's collections totaled approximately $33.2 million during fiscal year 2007, consisting of $8 million collected via the DLLR lockbox account, $7.6 million receipts collected by other DLLR divisions and forwarded for deposit to OBFS,

$7.1 million in credit card receipts from electronic licensing activity, and $10.5 million in mail receipts. According to DLLR's records, deposit adjustments processed during fiscal year 2007 totaled approximately $175,000.

Recommendation 8
We recommend that DLLR independently investigate and resolve all deposit adjustments and ensure all collections are recorded on the State's accounting system in a timely manner. We advised DLLR on accomplishing the necessary separation of duties using existing personnel.

Equipment

Finding 9
DLLR did not adequately maintain equipment records and did not comply with various provisions of the Department of General Services' *Inventory Control Manual.*

Analysis
DLLR did not adequately maintain equipment records and did not comply with record keeping and physical inventory provisions of the Department of General Services' (DGS) *Inventory Control Manual.* Specifically, DLLR did not maintain an independent control account and, our test of ten acquisitions, totaling approximately $227,000, disclosed four items, totaling approximately $60,000, which were not properly recorded in the detail records. In addition, DLLR did not properly investigate and resolve missing items identified during physical inventories. Specifically, we reviewed the most recent physical inventories for four DLLR units that were completed during the period from July 2006 to April 2007; these four units had sensitive equipment (such as computers) totaling $4.3 million as of June 30, 2007. Our review disclosed that 413 sensitive items totaling $614,538 were not located during the physical inventories and, as of September 2007, these items had not been investigated and resolved. We were advised that, as of July 2008, many items had been located and that the investigation was continuing.

Similar conditions have been commented upon in our four preceding audit reports dating back to 1996. The DGS *Inventory Control Manual* requires that a control account and detailed records be maintained to properly reflect all transactions for all categories of property and that the detailed records be reconciled to the related control account balance. The *Manual* further requires that physical inventories be conducted and variances be investigated and resolved and such efforts be properly documented and retained for audit verification. The reported book value of DLLR's equipment at June 30, 2007 totaled approximately $19.3 million.

Recommendation 9
We again recommend that DLLR comply with the *Inventory Control Manual* requirements.

Audit Scope, Objectives, and Methodology

We have audited the Department of Labor, Licensing and Regulation – Office of the Secretary and Division of Administration (DLLR) for the period beginning August 1, 2004 and ending August 31, 2007. 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. 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.

Our audit scope was limited with respect to the DLLR's cash transactions because the Office of the State Treasurer was unable to reconcile the State's main bank accounts during a portion of the audit period. Due to this condition, we were unable to determine, with reasonable assurance, that all DLLR cash transactions prior to July 1, 2005 were accounted for and properly recorded on the related State accounting records as well as the banks' records.

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.

APPENDIX

DLLR
STATE OF MARYLAND
DEPARTMENT OF LABOR, LICENSING AND REGULATION

MARTIN O'MALLEY, Governor
ANTHONY G. BROWN, Lt. Governor
THOMAS E. PEREZ, Secretary

OFFICE OF THE SECRETARY

DLLR Home Page • http://www.dllr.state.md.us
DLLR E-mail • mddllr@dllr.state.md.us

November 20, 2008

Revised

Mr. Bruce A. Myers, CPA
Legislative Auditor
Department of Legislative Services
301 West Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Myers:

Attached is the response of the Department of Labor, Licensing and Regulation to the draft Legislative Audit Report on the Office of the Secretary and Division of Administration for October 2008.

We appreciate the professional and cooperative manner in which your team conducted the audit. Should you have any questions or concerns regarding our response, please contact Adam Ortiz, Director of Compliance and Audit at (410)230-6242 or aortiz@dllr.state.md.us.

Sincerely,

Thomas E. Perez
Secretary

Enclosure

cc: Leonard Howie, Deputy Secretary
Adam Ortiz, Director of Compliance and Audit
Richard Pragel, Director of Information Technology
David McGlone, Director of Budget and Finance

Response of DLLR-Office of the Secretary and Division of Administration to Audit Findings and Recommendations for the Legislative Audit of October 2008

Information Systems Security and Control

Finding 1
Security over DLLR's computer network was not adequate.

Agency Response:

DLLR Agrees with this finding.

- Under network security best practices recommends that these servers would be more fully segregated from the rest of the DLLR internal network. We are currently assessing the best way to provide the highest security for these servers while also not impacting their operation or the applications that require access to them.

- Best practice would include the use of a secure protocol to manage the DLLR Network core devices. However, the current devices and operating systems do not support the use of a secure protocol for management connections. DLLR is evaluating if software upgrades are available for these that will allow for secure management, or if the devices will have to be physically upgraded to gain this functionality.

- Due to a configuration error the internal core router did have default connection values. While this did not expose the internal network to any external threats, it is less than desirable from a security perspective. These default values have since been removed from the device removing any possible threat.

Finding 2
Sensitive information relating to initial unemployment insurance claims was not adequately protected.

Agency Response:

DLLR agrees with this finding.

- DLLR is discussing with ADC - the use of a secure transfer process.

- Response is included in next paragraph.

- The data can be handled in a more secure fashion, however, this issue will have to be addressed and negotiated between Unemployment Insurance and the companies that they are doing the transfers with. Under their original transfer agreement there was no plan made for the encryption of the data or method to be used, just an agreement that transfer encryption would be used for the passing of data across public networks. When a new agreement for data encryption is completed with the payroll companies, OIT has no issue with implementing it. The existing encryption level for the transfer was set because one of the payroll companies was unable to support higher encryption levels at the beginning of the project. All providers are now able to support strong encryption and that has now been set as the minimum standard.

- The ability to view file names of other provider's files was a rights error by OIT. The issue was corrected as soon as it was discovered during the audit. New server hardware and more restrictive server software account configurations t have been installed. OIT also reviewed the file access records since 2004, when the transfer was initiated, and found that there had been no unauthorized access by any of the three providers to another provider's files.

Finding 3
Security measures over the electronic licensing application were inadequate.

Agency Response:

DLLR agrees with this finding.

- DLLR will obtain and install a separate credit card service provider account for application processing and service management. The service management accounts will be restricted to access by DLLR IP addresses only. DLLR will store the credit card service provider accounts and passwords for application processing in a secure location. Access to credit card service provider accounts is being restricted immediately upon an employee's termination. Credit card service provider service management accounts are now being assigned only to individuals not responsible for reconciling the business licensing sales to the credit card service provider /Bank accounts.

- DLLR will remove the plain text log files from the associated web server and move the text log files to a different server.

- Modification access of the public use account has now been restricted to the application document root.

- As web server logs are periodically reviewed by agency personnel to identify and investigate security-related events documentation will be maintained.

Finding 4
DLLR did not adequately log security events, monitor security reports, and document security reviews and investigations.

Agency Response:

DLLR agrees with this finding.

- DLLR is now logging AF (Authority Failures), CP (User Profile Changes), and the direct creation and deletion of records to critical data files. DLLR is now documenting all investigations of questionable items on its security reports.

- In order to automate and log the events, log monitoring software was purchased and installed and a procedure has been put in place to review and document audit violations.

Finding 5
Access controls, segregation of critical functions, and account and password controls were not adequate.

Agency Response:

DLLR agrees with this finding.

- The Administrators Group was taken out from the authorized users.

- The critical program library has been changed to “Exclude” and library access has been restricted to authorized individuals.

- DLLR will segregate the functions of system administration and security administration to provide segregation of duties. The shared profile is no longer being shared. All users are now uniquely identified.

- Certain users had account lockout, password length, password complexity, password history, and password aging. We are in the process of migrating all users to a platform that will enable us to provide adequate password and account controls. After the migration is complete all restrictions will be in place for all users.

Purchases and Disbursements

Finding 6
Proper internal controls were not established over the processing of purchasing and disbursement transactions.

Agency Response:

The agency partly agrees with the finding. The agency FMIS administrator established approval paths to require the approval from a higher level which prevents anyone creating or releasing any two documents within a two or three way match requirement from acting independently to create, approve and release the documents. However there is a regulation of law that the last approver must be duly authorized to release the documents. The system was in compliance with regulation during the audit period including the most recent ADPICS and R*STARS Security Officer Audit Reports that indicate no security violations.

In May 2008, the agency FMIS administrator completed removal of interface security class 02 from users who have the ability to update procurement documents and completed removal of interface security class 05 from users with the ability to update vouchers. The agency believes separating the ability to post critical documents satisfies the auditor’s concern and also renders the use of approval paths as redundant controls. DLLR will provide this documentation to the auditors.

Federal Funds

Finding 7
DLLR did not have adequate procedures to ensure all federal expenditures were recovered timely, resulting in lost investment income of $18,000. In addition, $10.4 million in accrued federal fund revenues were not supported.

Agency Response:

The agency concurs with the need to strengthen procedures relating to accounting for federal funds on our Schedule G reconciliation. In this instance the initial expenditure report did not include the $540,000 for the period in question. This omission was discovered and a revised expenditure report was submitted to the Department of Labor within two weeks of the original submission date. The effect on Schedule G was corrected on the submission of the Fiscal Year 2008 Schedule G per instruction from the General Accounting Division (GAD). DLLR has initiated a follow up procedure to all revised expenditure reporting. The Chief of Accounting or the Director of Budget and Fiscal Services will review and initial all corrected reports to ensure that the drawdown and reporting of federal funds have been handled correctly.

DLLR also concurs with this finding regarding accrued revenue transactions and will ensure all accrued revenues will be supported with specific identification from a subsequent collection. During the closeout federal fund revenues were accrued in the aggregate to reflect federal fund balances due from the Schedule of federal grants receivable (schedule G). DLLR will change this method to specifically identify each grant receivable due and reconcile to a subsequent collection.

Cash Receipts

Finding 8
DLLR did not independently investigate and resolve certain deposit adjustments and did not record certain collections in the State's accounting system in a timely manner.

Agency Response:

We concur with the findings and recommendations noted above. DLLR has implemented corrective actions as noted below:

a) DLLR has restructured the process so that the employee who investigates chargebacks related to collections is no longer involved in the collection of revenue (deposit) process.
b) We agree with the recommendation that all deposits are recorded in R*STARS within (2) business days and will to adhere to the Comptroller's *Accounting Procedures Manual* requirement. A memo issued to the accounting staff dated June 3, 2008, changes the recording procedures to allow posting to R*STARS within the time frame designated.

Equipment

Finding 9
DLLR did not adequately maintain equipment records and did not comply with various provisions of the Department of General Services' *Inventory Control Manual*.

Agency Response:

We concur with the auditors' recommendation regarding compliance with the *Inventory Control Manual* and provide the following information in support of our continued reconciliation activity:

a) In June 2005, the Office of General Services (OGS) implemented a new fixed asset tracking system (A-Track) and has completed 3 physical inventories since. Since that time, we have located items that were not found in the initial 2005 inventory. To date, this includes items totaling $390,678 located since June 2007. We expect recoveries to continue to increase in the next few months. OGS will continue to work with our control agencies to clear up outstanding issues and follow procedures discussed in the inventory control manual.

b) The Office of Budget & Fiscal Services maintains a control account based on the fixed assets quarterly report of equipment purchases prepared from FMIS and compares it to the monthly additions and subtractions report prepared by OGS. OBFS then issues a quarterly variance report to OGS for reconciliation purposes. The beginning total inventory is based on a previously reconciled balance.

AUDIT TEAM

Brian S. Tanen, CPA, CFE
Audit Manager

Stephen P. Jersey, CPA, CISA
A. Jerome Sokol, CPA
Information Systems Audit Managers

David R. Fahnestock
Jonathan H. Finglass, CPA
Senior Auditors

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

Amin N. Berrah
LaTeasa R. Lomax
Ramin M. Niknava
Staff Auditors