Audit Report

Department of Human Resources
Office of the Secretary and Related Units

June 2014

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

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

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

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

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

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

June 24, 2014

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

Ladies and Gentlemen:

We have audited the Office of the Secretary and related units of the Department of Human Resources (DHR) for the period beginning November 17, 2009 and ending August 12, 2012. DHR provides intervention services to stabilize families and vulnerable adults, encourages financial independence by providing temporary support and transition services, and provides for the welfare of children at risk.

Our audit disclosed that DHR recorded unsupported special fund revenue transactions to offset deficit balances which resulted from expenditures exceeding revenues in one program. In addition, procedures had not been established to ensure that payments made to legal firms on behalf of indigent individuals were proper. Furthermore, DHR did not adequately monitor its grantees to ensure that funds were spent and services were performed in accordance with the grant agreements.

Our audit also disclosed that DHR could improve its information systems security and control. For example, the assignment of critical privileges and user access to mainframe systems were not sufficiently restricted to properly protect these systems.

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

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

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

Executive Summary

Legislative Audit Report on
Department of Human Resources (DHR) and Related Units
June 2014

- **DHR recorded unsupported special fund accrued revenues of approximately $11.5 million and $15.2 million at June 30, 2012 and June 30, 2013, respectively, for the Local Department Operations Assistance Payments program. These revenues were recorded to eliminate the deficit balances in the assistance program's special funds (Finding 1).**

  DHR should only record revenues in accordance with the General Accounting Division's closing instructions and take appropriate actions to eliminate the deficit balance.

- **Adequate procedures had not been established to ensure that payments made to legal firms on behalf of indigent individuals were proper and that the firms provided the related services. Such payments totaled $13.7 million during fiscal year 2012 (Finding 2).**

  DHR should ensure that payments made to legal firms are only for those individuals for whom DHR is responsible to provide legal services and should conduct on-site monitoring to ensure that the related services were provided.

- **DHR did not adequately monitor certain grantees to ensure that grant funds were spent as intended and services were performed in accordance with the grant agreements. For example, although the grantees were required to provide expenditure reports on a regular basis, DHR did not independently verify the accuracy of these reports (Findings 3).**

  DHR should adequately monitor its grantees to ensure that funds were spent and services were performed in accordance with grant agreements.

- **Numerous security and control issues were noted in regard to DHR's information systems. For example, the assignment of critical privileges and user access capabilities to mainframe systems were not sufficiently restricted to properly protect the systems (Findings 4 - 7).**

  DHR should take the recommended actions to improve security and controls over its information systems.

- **DHR's oversight of its electronic benefits transfer system and contractual services could be improved (Findings 8 and 9).**

  DHR should take the recommended actions to improve its oversight in these areas.

Background Information

Agency Responsibilities

The Department of Human Resources (DHR) provides intervention services to stabilize families and vulnerable adults, encourages financial independence by providing temporary support and transition services, and provides for the welfare of children at risk. To deliver these services, DHR is organized into seven budgetary units. This audit included the operations of the Office of the Secretary, which provides overall direction and coordination for all DHR programs and activities; the Operations Office, which provides core administrative services to DHR units; and the Office of Technology for Human Services, which is responsible for the overall management and direction of DHR's information systems. The remaining four units of DHR are audited and reported upon separately.

According to the State's records, during fiscal year 2013, expenditures for the three units included in this audit totaled approximately $142 million.

Reorganization

Chapter 356, Laws of Maryland 2011, effective July 1, 2011, transferred the Sexual Assault Crisis Programs and the Domestic Violence Programs from the Department of Human Resources - Office of the Secretary to the Governor's Office of Crime Control and Prevention. The scope of this audit included the activities of these programs through June 30, 2011. Activities subsequent to the transfer will be included in our audit of the Executive Department.

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 January 11, 2011. We determined that DHR satisfactorily addressed five of the findings. The remaining four findings are repeated in this report.

Findings and Recommendations

Special Fund Budgetary Closeout

Finding 1
The Department of Human Resources (DHR) recorded unsupported special fund revenue transactions to offset deficit balances which resulted from expenditures exceeding revenues in one program.

Analysis
DHR recorded unsupported special fund revenue transactions to offset deficit balances which resulted from expenditures exceeding revenues in one program. Specifically, during the fiscal year budgetary closeout process, DHR recorded special fund revenue transactions totaling approximately $11.5 million and $15.2 million to offset deficit balances that existed in the Local Department Operations Assistance Payments program as of June 30, 2012 and June 30, 2013, respectively. According to DHR records, these deficits resulted from special fund expenditures incurred which exceeded related revenues in each fiscal year dating back to 2010.

For example, according to the financial information provided by DHR, in fiscal year 2013 this program incurred special fund expenditures totaling approximately $18.7 million. During that year, the program received revenues of $15 million which was not sufficient to cover those expenditures. Furthermore, because of the deficit of $11.5 million that existed at June 30, 2012, revenues received during fiscal year 2013 were needed to cover the prior year's expenditures, leaving only $3.5 million available to fund fiscal year 2013 expenditures. The resulting $15.2 million deficit was offset by the unsupported revenue transactions recorded at June 30, 2013.

If special funds are not available for the recorded revenue transactions, general fund appropriations (or deficiency appropriations) may ultimately be needed to eliminate the resulting deficits. This issue has been commented upon in our budget closeout reviews for the last two years, most recently in our special report entitled *Statewide Review of Budget Closeout Transactions for Fiscal Year* 2013, dated January 13, 2014.

DHR management personnel advised us that the revenues recorded were proper, because it received sufficient revenue in subsequent years although these revenues were not received within 60 days of the fiscal year-end. However, closing instructions issued by the Comptroller of Maryland – General Accounting Division's (GAD) require that revenue should be recognized at year-end only

when revenues are available and measurable (collectible within 60 days of the end of the fiscal year). Additionally, we noted that GAD's *Accounting Procedures Manual* states that special fund appropriations can only be expended to the extent that an agency realized revenue sufficient to fund the appropriation.

The Local Department Operations Assistance program receives special funds from various sources. For example, the program pursues payment of child support for individuals receiving certain types of cash assistance. In these cases, a portion of child support collections may be owed back to the program. In other cases, DHR may provide assistance payments in advance of determining an individual's eligibility for federal funding, with the advanced payments being reimbursed once federal eligibility is approved and funding is received.

Recommendation 1
We recommend that DHR

a. ensure that all year-end revenue transactions are appropriately recorded in accordance with GAD's closing instructions,
b. implement corrective action to resolve the deficit balance, and
c. ensure that expenditures do not exceed the related revenue realized.

Maryland Legal Services Program

Finding 2
DHR did not ensure that payments to legal firms on behalf of indigent individuals were proper and did not perform site visits to ensure that required services were provided.

Analysis
DHR did not ensure that payments to legal firms on behalf of indigent individuals were proper, and it did not perform site visits to ensure that legal firms provided the required services. State regulations require DHR to contract with legal firms to represent indigent adults in Adult Protective Services proceedings, and to represent children in Children in Need of Assistance and Termination of Parental Rights cases. According to State records, payments to 12 legal firms during fiscal year 2012 totaled $13.7 million.

- Although the legal firms submitted invoices listing the individuals served, DHR paid the firms without verifying that it was responsible for providing legal services to these individuals. Such verifications could be done by reviewing a copy of the court order, appointing the legal firm as the representative, for the individuals. Generally, the legal firms are paid a flat

fee per case. A similar condition regarding not verifying the propriety of payments to legal firms was noted in our preceding audit report.

- DHR did not perform annual site visits (quality control reviews), as provided for in the contracts, for 8 of the 12 firms during fiscal years 2011 and 2012. In addition, for the 8 site visits performed, DHR did not maintain adequate documentation supporting what was reviewed and the conclusions reached. These site visits can be used to help ensure compliance with the contract terms and could help verify the propriety of the amounts billed. For example, these visits could help ensure legal firms were providing the required number of hours for each case, attorneys had a sufficient number of contacts with the client, the attorney/client ratio was reasonable, and that the overall quality of services performed was adequate, as provided for by the contract. A similar condition regarding not performing site visits has been commented upon in our two preceding audit reports.

- As of March 2013, DHR had not obtained the required annual reports for fiscal years 2011 and 2012 from 11 of the 12 firms. In addition, DHR did not take any follow-up actions (such as, contacting the firms) to obtain these reports. The contract requires the legal firms to submit annual reports with information such as caseload per attorney. These reports are to assist DHR in monitoring contractual requirements.

As a result of these conditions, there was a lack of assurance that amounts paid for legal services were proper and that the related services were provided in accordance with the contract terms.

Recommendation 2
We recommend that DHR

a. verify that payments made to legal firms are only for individuals for whom DHR is responsible to provide legal services (for example, require legal firms to submit copies of the court orders appointing the firm as the representative) (repeat);

b. conduct on-site monitoring to ensure that amounts invoiced were proper and services were provided in accordance with the contract terms (repeat) and maintain adequate documentation of the site visits; and

c. take appropriate follow-up actions to ensure the legal firms submit annual reports as required.

Grants Management

Finding 3
DHR lacked sufficient procedures and accountability over certain grants.

Analysis
DHR lacked sufficient procedures and accountability over certain grants. DHR's Office of Grants Management provides funding to a network of community and faith-based organizations, local departments of social services, and other state and local agencies.

- DHR did not independently verify that grant funds were spent as intended. Our test of 27 disbursements totaling approximately $1.5 million related to 15 grants (such as grants for the Maryland Emergency Food Program and for Emergency Transitional Housing Services) disclosed that DHR did not obtain sufficient supporting documentation for 24 disbursements totaling approximately $1.4 million. Although the grant agreements required grantees to provide expenditure reports on a regular basis, DHR did not independently verify the accuracy of the reports by obtaining supporting documentation. For example, DHR did not obtain appropriate documentation, such as food and hotel receipts, to support expenditures made by grantees for emergency and traditional housing services provided to the homeless.

- DHR did not ensure that assistance activity reports (such as the number of individuals served) required by the grant agreements, were submitted by the grantees. Additionally, DHR did not ensure that annual site visits, required by the grant agreements, were performed. Our test of 15 grants totaling approximately $11.3 million disclosed that, for 12 grants totaling approximately $10.8 million, 113 of the 119 activity reports required to be submitted in fiscal year 2012 were not on file. Additionally, site visits were not performed for 13 grants totaling $10.9 million during fiscal year 2012. Site visits are performed to ensure that services were provided in accordance with the terms of the grant agreements.

According to the State's records, during fiscal year 2012, expenditures to grantees totaled $14.4 million. Similar conditions were commented upon in our preceding audit report.

Recommendation 3
We recommend that DHR

a. independently verify, on a test basis, that grant funds are spent as intended (repeat);
b. ensure that all required reports are submitted, including the missing reports noted above (repeat); and
c. ensure that annual site visits are performed (repeat).

Information Systems Security and Control

Background

The DHR Office of Technology for Human Services (OTHS) is responsible for the overall management and direction of DHR's information systems. These systems include critical applications such as the mainframe-based Clients' Automated Resource and Eligibility System (CARES), the mainframe-based Child Support Enforcement System (CSES), and the server-based Children's Electronic Social Services Information Exchange System (CHESSIE).

These systems are used to provide eligible persons public assistance, food stamps, child support payments, and foster care payments. Maintenance and operation of these information systems are provided by a combination of outsourced services and DHR personnel. OTHS operates both an internal network at DHR's headquarters and a wide area network which connects to DHR's locations throughout the state. Additionally, DHR obtains Internet and Statewide Government Intranet connectivity from networkMaryland.

In addition to these systems, DHR also uses the State's Financial Information Management System (FMIS) to process purchasing and disbursement transactions. FMIS has security features to establish independent online approvals for purchasing and disbursement transactions.

Finding 4
DHR had not established sufficient controls to ensure the propriety of actions taken by certain users in its automated payment systems.

Analysis

DHR had not established sufficient controls to ensure the propriety of actions taken by users with unrestricted access to the electronic benefit and payment menu screens in CARES. Additionally, DHR did not fully use the security features available on FMIS.

- Sixteen employees had been granted unrestricted access to critical CARES files. CARES is used to authorize public assistance and food stamp benefits and, therefore, a user with unrestricted access could both add and approve a case for benefits without independent supervisory review and approval. According to DHR's records, benefits and payments totaling approximately $1.3 billion were processed via CARES during fiscal year 2012. A similar condition was commented upon in our preceding audit report.

- DHR established online approval rules over certain critical procurement 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, 17 employees who had the ability to initiate these transactions could modify the transactions after the related approvals were obtained, without detection. During fiscal years 2010 through 2012, DHR used the State's accounting system to process purchase orders totaling approximately $96 million.

Recommendation 4
We recommend that

a. critical actions taken on CARES by users with unrestricted access be subject to independent supervisory review and approval, at least on a test basis (repeat); and

b. available FMIS security features be used to properly control purchasing transactions, including ensuring that these transactions cannot be modified by the initiator after the related approvals are obtained.

Finding 5
Assignment of critical privileges and user access and monitoring controls over mainframe systems were not sufficient to properly protect these systems.

Analysis
The assignment of critical privileges as well as user access and monitoring controls over mainframe systems were not sufficient to properly protect these systems.

- Numerous users were inappropriately assigned critical database roles in the CARES and CSES databases including the system administrator (two users) and system operator (nine users) roles. Furthermore, mainframe security software access rules allowed many users unnecessary direct modification access to certain critical production programs and files. As a result of these

conditions, these users could make unauthorized changes to critical production tables, files, and programs.

- Although direct modifications to numerous tables in the CARES and CSES databases were logged, the modifications were not included on security reports for subsequent review. For example, an important daily security report, which reflects direct changes to other critical database tables, was not reviewed for the 10-month period ending December 2012.

- Two users were inappropriately granted security software privileges that allowed them to make changes to critical mainframe files without being logged. In addition, six users were granted privileges which allowed them to change security software log settings without detection.

- Security software reports did not include the use of certain critical commands or commands issued by users with certain critical privileges. In addition, although a report of changes to security software settings was generated daily; there was no evidence that this report was reviewed for propriety. As a result of these conditions, changes to critical security software settings and user profiles were not subject to review for propriety.

The Department of Information Technology (DoIT) *Information Security Policy* states that each agency must establish an authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and "need-to-know." This policy further requires that information systems must generate audit records for all security-relevant events, and procedures must be developed to routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and findings must be reported to appropriate officials for prompt resolution.

Recommendation 5

We recommend that DHR

a. grant critical database roles and restrict access to critical mainframe production programs and files to only those individuals who require such roles/access for their job responsibilities,

b. ensure that direct modifications to critical database tables are included on security reports for subsequent managerial review,

c. perform regular documented reviews of the security reports of direct changes to critical database tables and of changes to security software settings and retain these reviews for future reference,

d. grant security software privileges in a manner that ensures that all changes to critical files and log settings are logged for subsequent review, and

e. ensure that security software reports include the use of all critical commands and commands issued by users with critical privileges.

Finding 6
CHESSIE database controls were not sufficient to properly protect critical data.

Analysis
CHESSIE database controls were not sufficient to properly protect critical data.

- Direct modifications to all CHESSIE database tables were not logged. As a result of this condition, direct changes to critical data would not be readily detectable by DHR management.

- Database level auditing (for example, changes to audit settings and grants of authority) was not enabled except for critical event failures. In addition, reports of events that were logged were not generated. Therefore, unauthorized activities affecting the integrity of the production database could go undetected by management.

- Numerous users were inappropriately assigned critical database roles including the system administrator (six users) and database administrator (four users). As a result of this condition, these users could make unauthorized changes to critical production files.

- Numerous users were inappropriately assigned critical database table privileges (for example delete, update, and insert). As a result, many of these users could make unauthorized changes to tables related to payments, rates, and eligibility.

Recommendation 6
We recommend that DHR

a. log all direct modifications to critical CHESSIE database tables, generate periodic reports of these modifications, perform documented reviews of these reports, and retain these reviews for future reference;

b. enable database level auditing for all critical security events, generate periodic reports of these events, perform documented reviews of these reports, and retain these reviews for future reference; and

c. grant critical database roles and table privileges to only those individuals who require such capabilities for their job responsibilities.

Finding 7
DHR's internal network and the vendor network that contained the mainframe and servers which hosted critical DHR systems were not adequately secured.

Analysis
DHR's internal network and the vendor network that contained the mainframe and servers which hosted critical DHR systems were not adequately secured. DHR operated firewalls at its network interfaces and several virtual private network connections. In addition, DHR was responsible for the configuration of the vendor maintained firewall that protected the vendor network that contained the mainframe and servers that hosted the CARES, CSES, and CHESSIE systems.

- Firewall rules allowed insecure and unnecessary connections to the DHR internal network. Specifically, we noted that multiple county government Internet Protocol (IP) addresses could access the DHR mainframe and numerous DHR IP addresses over all ports. Most of this access was not necessary. Similar conditions were commented upon in our preceding audit report.

- DHR allowed unnecessary virtual private network connections from several untrusted parties to the DHR internal network. For example, as of the time of our review on December 18, 2012, a contractor could access the entire DHR internal network over all ports via a virtual private network to setup and maintain DHR network equipment. However, the contract with this vendor had expired on December 31, 2011. Therefore, this connection gave this vendor unauthorized and unnecessary network-level access to the entire DHR internal network for almost a year.

- Firewall rules were not configured to adequately secure the connections into the vendor's network that hosted CARES, CSES, and CHESSIE. For example, a third-party vendor which required limited access to the mainframe that hosted these systems could access the mainframe over all ports. A similar condition was commented upon in our preceding audit report.

As a result, these areas were susceptible to attacks which could result in a loss of data integrity, the destruction of critical files, and the interruption of critical network services.

Recommendation 7
We recommend that DHR

a. configure its firewalls and virtual private networks to achieve a "least privilege" security strategy giving individuals and devices only those privileges needed to perform assigned tasks (repeat); and

b. require the vendor that hosts CARES, CSES, and CHESSIE to configure the aforementioned firewall to properly protect the critical devices on the network hosting these systems (repeat).

Electronic Benefits Transfer System

Background

DHR contracted with a vendor to implement, operate, and maintain a web-based Electronic Benefits Transfer System (EBTS) for the State of Maryland Public Assistance and Food Stamp Benefit Programs. The contract between DHR and the vendor for the EBTS service covered an initial period from May 2007 to February 2011, plus two optional renewal periods (of two years each), that extended the contract through February 2015, with a cost of approximately $24.6 million through February 2015. The vendor procured an independent review over its EBTS service to be performed in accordance with the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagement 16 and received a Service Organization Controls (SOC) report for the period July 1, 2011 through June 30, 2012. The report was issued on August 14, 2012.

Finding 8
The SOC report on the DHR EBTS provider did not address several key security controls.

Analysis

The SOC report on the DHR EBTS vendor did not address several key security controls necessary for the EBTS service. For example, we noted that the report did not state that vulnerability scanning and patch management policies and procedures existed and had been implemented or that intrusion detection, malware prevention, and antivirus protection had been implemented. Furthermore, the report did not stipulate that disaster recovery and business continuity policies, processes, and procedures existed and had been regularly tested. Finally, we noted that the SOC report did not provide test results evidencing that reports of privileged user access activities, authorized and unauthorized access attempts, and information security events were actually generated and retained.

The aforementioned security controls not addressed by the SOC report are required either by DHR's contract with the EBTS vendor or DoIT's *IT Security Policy.*

We were advised by DHR personnel that they had not examined the SOC report to assess whether the scope of the work performed included a review and appropriate tests of all necessary controls that should exist within the EBTS vendor's environment to properly secure DHR data. Without a detailed examination of the report, DHR lacked assurance that adequate controls existed over the EBTS vendor's system and processes.

Recommendation 8
We recommend that, for future SOC reviews of the EBTS vendor's service, DHR obtain and review the vendor's SOC reports, determine if the related reviews adequately addressed the aforementioned EBTS security concerns, and ensure that the vendor implements all critical recommendations made in the reports.

Contractual Services

Finding 9
DHR did not document its rationale for not assessing liquidated damages.

Analysis
DHR did not document its rationale for not assessing liquidated damages against a vendor for qualifying conditions, as stipulated in the related contracts. This vendor is responsible for hosting the EBTS as well as for application maintenance and enhancement services. Specifically, we were advised by DHR management that there were five instances between July 2010 and August 2012 in which DHR notified the vendor that it was responsible for computer failures (such as, systems being inaccessible). The notifications further stated that DHR may impose liquidated damages totaling $373,500, unless the vendor could demonstrate that it was not responsible for the failures.

Our review of the aforementioned five notifications disclosed that, for three notifications, DHR did not have any documentation explaining why liquidated damages totaling $341,000 were not assessed. For example, on July 8, 2011, DHR notified the vendor that it may impose liquidated damages totaling $50,000 because the food stamp benefit system was inaccessible. In this case, liquidated damages were not assessed, and DHR could not provide us with documentation explaining this decision. We were advised by DHR management that it did not ultimately impose liquidated damages related to these three notifications because

the failures were eventually resolved. For the remaining two notifications, DHR assessed liquidating damages totaling $7,500 for one instance and had adequate supporting documentation to explain why damages were not assessed for the other instance.

Recommendation 9

We recommend that DHR formally document its reasons when liquidated damages are not assessed against vendors when qualifying conditions occur.

Audit Scope, Objectives, and Methodology

We have audited the Department of Human Resources and related units (DHR) for the period beginning November 17, 2009 and ending August 12, 2012. 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 DHR'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 included 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 electronic benefit transfers, grants, legal services, purchases and disbursements, information systems security and control, equipment, and payroll.

To accomplish our objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of DHR's operations and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. Finally, we performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

Our audit included various support services (such as payroll, purchasing, maintenance of accounting records, and related fiscal functions) provided by DHR's Office of the Secretary and related units to the other units of DHR.

Our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of DHR'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 DHR.

DHR'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 that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect DHR'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 DHR that did not warrant inclusion in this report.

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

APPENDIX

Maryland's Human Services Agency
Department of Human Resources
Martin O'Malley, Governor | Anthony G. Brown, Lt. Governor | Theodore Dallas, Secretary

May 30, 2014

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

Dear Mr. Barnickel:

Please find enclosed the Department of Human Resources' (DHR) responses of the Office of the Secretary for the Office of Legislative Audits draft report, covering the period of November 17, 2009 to August 12, 2012.

If there are any questions regarding these responses, please contact the Acting Inspector General, Marva M. Sutherland of my staff at 443-378-4008 or Marva.Sutherland@maryland.gov.

Sincerely,

Theodore Dallas

Enclosures

c: Carnitra White
William E. Johnson Jr.
Stafford Chipungu
Kenyatta Powers
Marva Sutherland
Rosemary Malone

Findings and Recommendations

Special Fund Budgetary Closeout

Finding 1
The Department of Human Resources (DHR) recorded unsupported special fund revenue transactions to offset deficit balances which resulted from expenditures exceeding revenues in one program.

Recommendation 1
We recommend that DHR

- **a. ensure that all year-end revenue transactions are appropriately recorded in accordance with GAD's closing instructions,**
- **b. implement corrective action to resolve the deficit balance, and**
- **c. ensure that expenditures do not exceed the related revenue realized.**

Department's Response

Recommendations (a), (b), and (c): The Department believed that the closing was conducted properly and that it complied with GAD closing instructions. The Department will review GAD policy regarding year-end closings for all future closings with particular attention to the issues raised in the audit and make sure that accrued revenue and related expenditures are recorded in compliance with the GAD's closing instructions.

Maryland Legal Services Program

Finding 2
DHR did not ensure that payments to legal firms on behalf of indigent individuals were proper and did not perform site visits to ensure that required services were provided.

Recommendation 2
We recommend that DHR

- **a. verify that payments made to legal firms are only for individuals for whom DHR is responsible to provide legal services (for example, require legal firms to submit copies of the court orders appointing the firm as the representative) (repeat);**
- **b. conduct on-site monitoring to ensure that amounts invoiced were proper and services were provided in accordance with the contract terms (repeat) and maintain adequate documentation of the site visits; and**

c. take appropriate follow-up actions to ensure the legal firms submit annual reports as required.

Department's Response

Recommendation a: The Department agrees with this recommendation and had made this change prior to the draft audit finding. The Department regularly reviews every invoice that is submitted by the vendor for billing proficiency as a standard practice. In addition, DHR has always required all attorneys in the Court Appointed Attorneys Program (CAAP) responsible for handling Children in Need of Assistance (CINA) to submit court orders with each invoice, indicating that they have been appointed by the Judiciary for representation. Now DHR requires all CAAP attorneys in CINA and Adult Protective Services to follow the same procedure. DHR will audit the invoices submitted by the vendors for comprehensive evaluation using DHR approved methodology.

Recommendation b: The Department agrees with this recommendation and had made this change prior to the draft audit finding. A contract monitoring plan was developed and implemented. The contract monitoring plan requires annual monitoring of the providers files and attorney performance in court. DHR revised the contract monitoring form to be completed by the contract compliance monitors to document the performance of the providers and the sufficiency of the provider's files. The contract monitors produce a contract monitoring report that documents the monitoring information, identifies any deficiencies and requests corrective action plans.

Recommendation c: The Department agrees with this recommendation and had made this change prior to the draft audit finding. DHR implemented a process that requires that an annual notification is sent to the providers to request the annual reports. Additional notifications are generated to notify the providers when the annual reports have not been submitted in a timely fashion. DHR followed the new process and requested that the providers submit the annual reports for FY2012. As of April 2013, DHR had received the annual reports from all of the contracted providers for FY2012.

Grants Management

Finding 3
DHR lacked sufficient procedures and accountability over certain grants.

Recommendation 3
We recommend that DHR

a. independently verify, on a test basis, that grant funds are spent as intended (repeat);

b. ensure that all required reports are submitted, including the missing reports noted above (repeat); and
c. ensure that annual site visits are performed (repeat).

Department's Response

Prior to responding to the individual recommendations in the audit, DHR would like to acknowledge that it became aware of insufficient and inadequate monitoring of grants in the Office of Grants Management during the time period of the audit. As a result, the Department made several personnel changes in the Office including removing the director of the Office and some members of the staff in February 2012. The Department also moved the Office under the Family Investment Administration to ensure that the Administration could more closely monitor the programs.

Recommendation a: The Department agrees with this recommendation and had implemented controls to improve accountability and streamline the delivery of service in July 2012 prior to the audit. Specifically:

- All vendors were reminded of the receipting process, timeframes and deliverables;
- The Program Administrator now reviews all receipts that are submitted to ensure that they meet standards of accountability and all vendors have been required to submit any missing monthly expenditure and activity reports. Through these reports and site visits, one vendor in each jurisdiction was identified as a sample to verify that grant funds were spent as intended;
- Records of these verifications are being kept on file in the Bureau of Grants Management office and the results of the reviews are documented in the case records of the vendors;
- In the event the vendor fails to provide the receipts or submits questionable receipts, they are contacted immediately to resolve the problem. Failure to meet receipt compliance will result in ineligibility for future funding; and
- The Department has created a schedule of site visits for the entire fiscal year. Expenditure reports were submitted by all grantees for the fiscal year 2013.

Recommendation b: The Department agrees with this recommendation and had made this change prior to the audit. In December 2012, Program Administrators for all programs began reviewing and assessing all reports that are submitted for accuracy, and notifying the organization when their report has not been submitted by the 15th of the month following the report month. All of the programs have

established due dates and any incidents of non-compliance result in the grantee's ineligibility for the following year. The paper reports are inserted into a binder and are logged on a spreadsheet in the office's shared drive noting the location of the binder. For FY 2013, 498 reports were received and inserted in binders.

Recommendation c: The Department agrees with this recommendation and had made this change prior to the audit. The site visit process was redeveloped in September 2013 to ensure that visits to each grantee are made at least once a year, with the schedule beginning in October and ending in March. The visits have been jurisdictionally distributed with the monitor being responsible for all programs within their assigned county. For example, the monitor who has been assigned to Allegany County must perform a site visit for all programs in that jurisdiction. Reports are completed and inserted within the grantee's case record. Assessments that are problematic are immediately addressed in writing with a time line for resolution.

Information Systems Security and Control

Finding 4
DHR had not established sufficient controls to ensure the propriety of actions taken by certain users in its automated payment systems.

Recommendation 4
We recommend that

a. **critical actions taken on CARES by users with unrestricted access be subject to independent supervisory review and approval, at least on a test basis (repeat); and**
b. **available FMIS security features be used to properly control purchasing transactions.**

Department's Response

Recommendations a: The Department agrees with this recommendation and will conduct a documented independent supervisory review and approval process focusing on changes that may affect recipient's benefits.

Recommendation b: The Department does not concur that proper internal controls were not established over the processing of purchasing transactions. No one in the Department can initiate and post a critical procurement document (purchase order, blanket purchase order, direct purchase order, and increasing change order) without the use of an approval path requiring authorization by a separate employee. In the cases where a requisition is used to create a purchase order or blanket purchase order, an on-line approval path is used for the requisition; direct purchase orders have an online approval path; and, increasing

change orders have a manual approval process requiring written requests. The Department would also like to note that neither the Department nor OLA auditors have found any instances of inappropriate modification to an approved direct PO under the current and long standing policy.[1]

Finding 5
Assignment of critical privileges and user access and monitoring controls over mainframe systems were not sufficient to properly protect these systems.

Recommendation 5
We recommend that DHR

a. grant critical database roles and restrict access to critical mainframe production programs and files to only those individuals who require such roles/access for their job responsibilities,
b. ensure that direct modifications to critical database tables are included on security reports for subsequent managerial review,
c. perform regular documented reviews of the security reports of direct changes to critical database tables and of changes to security software settings and retain these reviews for future reference,
d. grant security software privileges in a manner that ensures that all changes to critical files and log settings are logged for subsequent review, and
e. ensure that security software reports include the use of all critical commands and commands issued by users with critical privileges.

Department's Response

Recommendations (a), (b), (c), (d) and (e): The Department agrees with the finding and all recommendations were completed by July 18, 2013.

[1] **Auditor Comment:** The report noted that DHR had not established sufficient controls in FMIS since seventeen employees could initiate and approve purchasing transactions. In its response, DHR disagreed with the recommendation and stated that no individual could initiate and post purchase orders without an independent approval. We subsequently revised our report to clarify that the approval paths allowed the initiators to modify the purchase orders after they were approved. The revisions to our report were provided to the Department and it elected not to modify its response. The finding regarding the lack of controls over purchasing transactions is still valid.

Finding 6
CHESSIE database controls were not sufficient to properly protect critical data.

Recommendation 6
We recommend that DHR

a. log all direct modifications to critical CHESSIE database tables, generate periodic reports of these modifications, perform documented reviews of these reports, and retain these reviews for future reference;
b. enable database level auditing for all critical security events, generate periodic reports of these events, perform documented reviews of these reports, and retain these reviews for future reference; and
c. grant critical database roles and table privileges to only those individuals who require such capabilities for their job responsibilities.

Department's Response

Recommendation a: The Department agrees with the finding and the recommendation was completed by June 30th, 2013. Specifically, the Department logs all direct modifications to critical CHESSIE database tables, generate periodic reports of these modifications, perform documented reviews of these reports, and retain these reviews for future reference.

Recommendation b: The Department has attempted to enable this type of auditing in CHESSIE on two previous occasions and, in each instance, the enabling of this functionality caused the system to become unstable and inaccessible for users. The Department will again test the viability of this approach and expects to complete testing of this approach in July 2014. If successful, the Department will implement these changes to our production environment.

Recommendation c: The Department disagrees that it was inappropriately granting critical database roles – security reviews were conducted for those granted access. It is our understanding that the basis of this finding was instead that auditors believed the review should be conducted with more strict criteria. The Department will review its security procedures in this area and make any necessary changes to ensure that it grants critical database roles and table privileges only to employees who require such access. [2]

[2] **Auditor Comment:** DHR's response indicated disagreement with the finding. Specifically, DHR disagreed that it was inappropriately granting critical database roles and indicated that security reviews were conducted for those granted access. DHR further stated that it believed that the basis of our finding was that its security review should be conducted with more strict criteria. However, our assessment that numerous employees were assigned critical database roles and table privileges that were not needed to perform their job duties was based, in part, on representations of DHR personnel. Nevertheless, DHR's response specified the actions that will be taken which, if implemented, should fully address the audit recommendation.

Finding 7
DHR's internal network and the vendor network that contained the mainframe and servers which hosted critical DHR systems were not adequately secured.

Recommendation 7
We recommend that DHR

a. configure its firewalls and virtual private networks to achieve a "least privilege" security strategy giving individuals and devices only those privileges needed to perform assigned tasks (repeat); and
b. require the vendor that hosts CARES, CSES, and CHESSIE to configure the aforementioned firewall to properly protect the critical devices on the network hosting these systems (repeat).

Department's Response

Recommendations (a) and (b): While the Department believes that the audit narrative overstates the vulnerability to its systems relating to this finding, the Department has complied with the recommendations (a) and (b). In addition, as of July 30, 2013 the Department and the vendor that hosts CARES, CSES and CHESSIE have complied with the recommendations.

Electronic Benefits Transfer System

Finding 8
The SOC report on the DHR EBTS provider did not address several key security controls.

Recommendation 8
We recommend that, for future SOC reviews of the EBTS vendor's service, DHR obtain and review the vendor's SOC reports, determine if the related reviews adequately addressed the aforementioned EBTS security concerns, and ensure that the vendor implements all critical recommendations made in the reports.

Department's Response

Recommendation: The Department disagrees with this finding. There are no federal, state or DoIT requirements that require a SOC audit of this nature. In fact, the Department and the federal government currently require an annual

SSAE 16 audit and both the Department and its vendor comply with that requirement.

The Department will, however, assess the additional security requirements recommended by OLA and see if additional auditing is feasible within the existing contract. Future contracts for an EBT vendor will require the aforementioned type of SOC audit, as recommended by the auditor, in addition to the SSAE 16 audit.[3]

Finding 9
DHR did not document its rationale for not assessing liquidated damages.

Recommendation 9
We recommend that DHR formally document its reasons when liquidated damages are not assessed against the EBTS vendor when qualifying conditions occur.

Department's Response

The Department disagrees with the finding that it did not document its rationale for not assessing liquidated damages against the vendor.

The vendor's contract states that upon issuing a cure letter, the contractor bears the responsibility to provide evidence in response to the cure letters that the incidents were the results of excusable failure, a force majeure event, or a failure due to third party event, not just that the vendor had to demonstrate it was not responsible for the failures.

The contract also states that "DHR shall adopt a reasonable standard of review, which takes into consideration the totality of the circumstances". DHR is not obligated, to provide written documentation to the vendor of its disposition of liquidated damages post reviewing contractor response(s) to the initial cure letter. DHR is only obligated to review written vendor response(s) and consequent corrective action plans, remedial measures etcetera, and monitor them for execution or completion or simply decide to move forward with imposing the

[3] **Auditor Comment:** DHR's response indicates disagreement with the finding. Specifically, DHR's response stated there are no federal, state or DoIT requirements that require a SOC audit of this nature and that the Department and federal government require an annual SSAE 16 audit and both the Department and the vendor comply with the requirement. Our finding acknowledged that the DHR EBTS vendor had a SOC (SSAE) report, but noted that the report did not address whether the vendor had implemented several key security controls, which are required by either DHR's contract with the EBTS vendor or DoIT's *IT Security Policy* Nevertheless, DHR indicated that certain actions would be pursued for the existing contract and for future contracts for EBTS services.

liquidated damages. Upon receiving the vendor response, DHR carefully considers all facets of the issue to arrive at a decision of whether or not to impose liquidated damages.

In all instances where DHR issued a cure letter, the vendor has responded in writing to the Department's cure letter by either immediately remedying the situation, explaining that the failure was due to a third party action for which the vendor is not responsible, or by presenting or, planning to present in the near future, a detailed corrective action plan. In this case, the vendor's corrective action involved conducting a series of on-going executive level meetings as an effective and interactive method to find solutions in the State's best interest. These discussions with DHR resulted in the vendor investing $2.7 million in system upgrades – significantly more than the proposed liquidated damage of $341,000 and a greater value to the taxpayers.[4]

[4] **Auditor Comment:** The report noted that DHR did not document its rationale for not assessing liquidated damages against a vendor when there were qualifying conditions. In its response, DHR disagreed with the finding and indicated that the contractor bears responsibility for providing evidence as to why damages should not be assessed and DHR is not obligated to provide written documentation to the vendor of its decision. Our report does not recommend that DHR provide such documentation to the vendor. Rather, DHR should retain documentation on file that demonstrates, as required by the contract, that DHR adopted a reasonable standard of review, which takes into consideration the totality of the circumstances. Such documentation would indicate the factors considered and substantiate that the decision made was in the best interest of the State.

AUDIT TEAM

Joshua S. Adler, CPA, CFE
Audit Manager

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

Nichole M. Becker
Julia M. King
Howard A. Marzolf, III, CPA, CFE
Senior Auditors

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

Andrew S. Bien
Lisa M. DeCarlo
Samuel Hur
Jeneba R. Jalloh
Staff Auditors

J. Gregory Busch
Information Systems Staff Auditor