Audit Report

Maryland Longitudinal Data System Center

February 2016

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Warren G. Deschenaux
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

February 26, 2016

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

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Maryland Longitudinal Data System Center for the period beginning July 1, 2013 and ending December 31, 2014. The Center is responsible for overseeing and maintaining the Maryland Longitudinal Data System, a Statewide data system that contains individual-level student and workforce data from all levels of education and the State's workforce. The Center is tasked with managing and analyzing these data to determine how students are performing and the extent to which students are prepared for higher education and the workforce.

Our audit disclosed that the Center used an interagency agreement with a State university to procure information technology and training services rather than employing a competitive procurement process. In addition, the Center did not adequately protect sensitive personally identifiable information obtained from certain State agencies. Furthermore, the Center's information systems servers were not adequately secured.

The Center's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us by the Center during the course of this audit.

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

Background Information

Agency Responsibilities

Effective July 1, 2010, Chapter 190, Laws of Maryland 2010 established the Maryland Longitudinal Data System Center as an independent unit of State government under the direction of a 12-member governing board. In fiscal years 2011 through 2013, no appropriations were included in the State's budget for the Center, and activity relating to the Center was conducted on its behalf by the Maryland State Department of Education (MSDE). Beginning in fiscal year 2014, the Center received its own appropriation.

The Center is responsible for overseeing and maintaining the Maryland Longitudinal Data System, a statewide data system that contains individual-level student and workforce data from all levels of education and the State's workforce. The Center is tasked with managing and analyzing these data to help determine how students are performing and the extent to which students are prepared for higher education and the workforce. The Center conducts research to improve the State's education system and to guide decision-making by State and local governments, educational agencies, institutions, teachers, and other educational professionals.

The Center obtains and analyzes data through collaboration with five State entities: MSDE, the Maryland Higher Education Commission, the Department of Labor, Licensing and Regulation, and the University of Maryland's School of Social Work and College of Education. As of April 15, 2015, the Center had collected data for calendar years 2008 through 2013, and was continuing to collect data for subsequent periods. According to the State's records, during fiscal year 2014 the Center had seven authorized positions and expenditures totaling approximately $1.7 million.

Findings and Recommendations

Interagency Agreement

Finding 1
The Maryland Longitudinal Data System Center procured certain services through an existing interagency agreement rather than through a competitive procurement process.

Analysis
The Center used an existing interagency agreement with the University of Maryland, Baltimore (UMB) to procure certain services rather than using a competitive procurement process. The Center's interagency agreement with UMB was for research services and covered the period beginning July 1, 2013 and ending June 30, 2016. However, the Center directed UMB to procure different services from third-party vendors although the oversight of the vendors would remain under the control of the Center.

Specifically, through the interagency agreement, the Center directed UMB to contract with three companies, at a cost of approximately $475,000, for certain information technology services and database training. In particular, the Center directed UMB to contract with two companies for two specific individuals to provide information technology services at an aggregate cost of $350,000 for the period from June 2014 through June 2016. We were advised that these individuals were selected since they had previously worked in developing the Maryland Longitudinal Data System. The Center also directed UMB to contract with a third specific company for database training at a cost of $125,000 for the period from May 2014 through June 2016.

Furthermore, UMB did not exercise any contractual responsibilities other than procuring the three contracts and processing related payments to the companies. Specifically, the daily supervision and monitoring of the individuals and companies, including assigning tasks and ensuring that defined responsibilities were fulfilled, was performed by the Center.

Additionally, the interagency agreement with UMB included a facilities and administrative fee that ranged from 10 to 15 percent added onto the UMB billings even though, as previously noted, UMB's responsibilities were very limited and the Center performed the supervisory and monitoring responsibilities over these individuals and companies.

Since these services were obtained under an interagency agreement between State agencies, the Center avoided using a competitive procurement process, and obtaining control agency approval for the procurements as required by State procurement regulations. Accordingly, assurance was lacking that these services were obtained at the most advantageous cost to the State. We confirmed with staff at the Board of Public Works that the use of an interagency agreement to procure these contractual services was not appropriate.

Recommendation 1
We recommend that the Center discontinue the practice of using interagency agreements as a mechanism to avoid a competitive procurement process to obtain contractual services.

Information Systems Security and Control

Background
The Center collects data from sources including the Maryland State Department of Education (MSDE), the Department of Labor, Licensing and Regulation (DLLR) and the Maryland Higher Education Commission (MHEC). This data includes MSDE enrollment data for students attending Maryland public schools from pre-K to grade 12, earnings data for individuals employed by any entity required to submit earnings data to DLLR and MHEC enrollment data for students attending Maryland public colleges and universities. Data from DLLR and MHEC includes sensitive personally identifiable information such as full names, related social security numbers, and dates of birth. The Center processes the collected data and stores the data in two databases.

During our audit fieldwork, the Department of Public Safety and Correctional Services (DPSCS) provided support services to the Center by hosting the Center's servers. DPSCS also maintained the physical and network infrastructure which supported the hosted Center computer devices. However, the Center is ultimately responsible for all controls over the hosted devices and related data. We were advised that effective June 10, 2015 all critical Center servers and data have been transferred from DPSCS to MSDE. In addition, the Center's Data Security and Safeguarding Plan dated December 13, 2013 specifies that the Center shall provide data security and perform regular audits for compliance with privacy and security standards.

Center staff advised us that as of April 15, 2015 the Center had collected six years of data (calendar years 2008 through 2013) from MSDE, DLLR and MHEC and had completed processing most of the data it had obtained during calendar year 2014. The Center is continuing to collect data for subsequent periods of time.

Finding 2
Sensitive personally identifiable information (PII) obtained from MHEC and DLLR was not properly protected.

Analysis
Sensitive PII obtained from MHEC and DLLR was not properly protected.

- We identified two clear text files containing sensitive PII that were improperly stored on the Center's server used to host two databases. Encrypted versions of these two files had been received from DLLR, decrypted, and processed by the Center. However, after processing, these decrypted files were stored on the Center's server rather than being immediately deleted in accordance with the Center's procedures. According to the Center's records, these two files contained 882,598 unique records and, as of April 15, 2015, had been improperly retained on this server for 42 and 2 weeks.

- Social security numbers (SSNs) included with data received from MHEC were retained in one of the aforementioned databases and were not encrypted. Although the database software was capable of encrypting data that contained PII, this feature was not enabled for the aforementioned SSNs. Per our request, Center staff determined that, as of April 2015, this database contained 2,237,976 records with unique individual names and SSNs in clear text.

- The Center did not employ any substantial mitigating controls (such as the use of data loss prevention software) to protect this unencrypted sensitive PII.

This sensitive PII, which is commonly sought by criminals for use in identity theft, should be protected by appropriate information system security controls. The State of Maryland *Information Security Policy* specifies that agencies must protect confidential data using encryption technologies and/or other substantial mitigating controls.

Recommendation 2
We recommend that the Center
a. in accordance with its procedures, delete all decrypted files containing sensitive PII, immediately after processing; and
b. enable encryption for all databases tables containing sensitive PII.

Finding 3
The Center's servers, hosted by DPSCS, were not adequately secured.

Analysis
The Center's servers, hosted by DPSCS, were not adequately secured.

- The Center had not updated any of its 14 servers' operating systems for any updates released by the operating system's vendor. We determined that, as of our testing dates, the operating system vendor had issued 202 updates to the version of the operating system used on these servers and these updates addressed 229 known vulnerabilities associated with this version of the operating system. The *Information Security Policy* states that network devices should be patched and updated for all security-related updates/patches.

- Anti-malware software had not been installed on any of the Center's servers. The *Information Security Policy* states that agencies must protect against malicious code by implementing anti-malware solutions that, to the extent possible, include a capability for automatic updates.

- Three of four servers tested had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, the Center had not updated its servers for these patches.

- The firewall used by DPSCS to protect the Center's servers allowed the entire MSDE's network unnecessary network level access to these servers over numerous ports. The *Information Security Policy* states that information systems shall be configured to monitor and control communications at the external boundaries of these systems and at key internal boundaries within these systems.

As a result of these conditions, these servers were susceptible to unnecessary access and compromise and potential disclosure of critical and sensitive data. Although the Center's servers are no longer hosted by DPSCS, the Center still needs to ensure the servers are adequately secured regardless of who maintains the equipment.

Recommendation 3

We recommend that, as required by the *Information Security Policy*, the Center

a. continually update all of its servers with the latest operating system security patches issued by the operating system vendors;

b. install anti-malware software on all of its servers and continually maintain this software at current version levels with up-to-date anti-malware signatures;

c. keep its servers up-to-date for all critical security-related updates to potentially vulnerable installed software; and

d. ensure network-level access to its servers is limited to only those individuals/devices requiring such access over required ports.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Maryland Longitudinal Data System Center for the period beginning July 1, 2013 and ending December 31, 2014. 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 the Center's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included the procurement of interagency agreements with institutions of higher education and related disbursements, and information technology systems.

Our audit did not include support services provided to the Center by the Maryland State Department of Education (MSDE). These support services (including payroll processing, purchasing, maintenance of accounting records, and related fiscal functions) are included within the scope of our audit of MSDE.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of the Center's operations, and tests of transactions. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected. We also performed 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.

The Center'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 related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect the Center'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. Another less significant finding was communicated to the Center that did not warrant inclusion in this report.

The Center'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 the Center regarding the results of our review of its response.

APPENDIX

MLDS Center
Maryland Longitudinal Data System

Address 550 West Baltimore Street
Baltimore, MD 21201
Phone 410-706-2085
Email mlds.center@maryland.gov
Website www.MLDSCenter.org

February 24, 2016

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

Dear Mr. Barnickel,

Enclosed are the Maryland Longitudinal Data System Center's responses to the Legislative Auditor's current audit of the MLDSC for the period beginning July 1, 2013 and ending December 31, 2014.

An electronic version was forwarded by email. If you have any questions or need additional information please feel contact me at 410-706-2085 or Ms. Tejal Cherry, MLDS Center Chief Information Officer at 410-767-7089.

Sincerely,

Ross Goldstein
Executive Director

Finding 1
The Maryland Longitudinal Data System Center procured certain services through an existing interagency agreement rather than through a competitive procurement.

Recommendation
We recommend that the Center discontinue the practice of using interagency agreements as a mechanism to avoid a competitive procurement process to obtain contractual services.

Agency Response
The Center concurs with the auditor's recommendation. The Center will discontinue the practice of using an interagency agreement to procure vendor services.

In audit reports of other agencies, the auditor has noted similar findings regarding the improper use of interagency agreements to hire contractors in prior audits. While the Center does not dispute the finding or proposed recommendation, it is worth noting that the situation in this instance is different. First, the purpose of the interagency agreement between UMB and the Center was to establish a Research Branch for the Center that would utilize UMB's faculty and expertise to deliver high quality research and analysis to help inform Maryland policy makers. In fact, procuring vendor services was not even contemplated at the time of initiating the interagency agreement. When the need for vendor services arose, it was the understanding of both parties that UMB could procure the needed services since the services were directly related to the underlying purpose of the interagency agreement. Second, while the Center directly supervises and monitors the contractors, UMB researchers meet regularly with the contractors and work in conjunction with the contractors to develop the functionality of the system to fit the researchers' needs. It is a collaborative process.

One of the two vendor contracts ended on December 31, 2015. Additional funds were added to that contract prior to its conclusion to support work through the end of the year. The other vendor contract was entered into in June of 2015, prior to the receipt of the auditor's discussion notes. That contract will end on June 30, 2016.

Finding 2
Sensitive personally identifiable information (PII) obtained from MHEC and DLLR was not properly protected.

Recommendation 2
We recommend that the Center:

a. *in accordance with its procedures, delete all decrypted files containing sensitive PII, immediately after processing; and*
b. *enable encryption for all databases tables containing sensitive PII.*

Agency Response
The Center concurs with the recommendations and notes that the recommended actions have been fully implemented as of February 2015, when the hosting location was changed from the Department of Public Safety and Correctional Services (DPSCS) data center to the MSDE data center.

The audit was conducted on the Center's system as hosted by DPSCS. At the time of the audit, the Center was in the process of migrating from the DPSCS facility in order to ensure greater access and control over Center equipment and procedures. When the new MLDS Center IT capability was relocated to reside within the MSDE Data Center, a new automated process was put in place to handle all data files for processing. This automated process checks every hour for new files. When a file is discovered, it is unencrypted, read into the Staging Database and placed into encrypted tables using database encryption. Once the data loading process is complete, the file is deleted from the file folder, in which it was originally placed and the data provider is notified. This entire process is usually completed within two to three minutes.

A subsequent step in this automated process deconstructs the PII data into separate tables within the database, where the SSN column data is encrypted for storage and replaced with a tokenized representation of the SSN. This de-identifiable value is then associated with data for that person and written into the database, which contains no PII data.

Finally, the MLDS Center was not granted administrative level access to data center servers at DPSCS so that it could know that the unencrypted file folders existed. Immediately upon learning of this, the MLDS Center established a secure server within the MSDE Data Center and applied appropriate encryption to the files stored within the new server. The old server, located within the DPSCS data center has been deactivated and all files that resided in that server were destroyed.

Finding 3
The Center's servers, hosted by DPSCS, were not adequately stored.

Recommendation 3
We recommend that, as required by the Information Security Policy, the Center:

- *a. continually update all of its servers with the latest operating system security patches issued by the operating system vendors;*
- *b. install anti-malware software on all of its servers and continually maintain this software at current version levels with up-to-date anti-malware signatures;*
- *c. keep its servers up-to-date for all critical security-related updates to potentially vulnerable installed software; and*
- *d. ensure network-level access to its servers is limited to only those individuals/devices requiring such access over required ports.*

The Center concurs with the recommendations and notes that the recommended actions have been fully implemented as of June 2015, when the hosting location was fully transitioned from the Department of Public Safety and Correctional Services (DPSCS) data center to the MSDE data center.

The MLDS Center did not have adequate authority over its system at the DPSCS data center. Once the system resources were relocated to the MSDE data center, the physical servers were rebuilt with the latest version of the operating system, where updates are reviewed monthly and applied as approved through a formal change management process. Only upgrades that would cause disruption to the complex and integrated MLDS Center environment are not implemented. All application and database servers are now virtual servers using virtual storage, and placed behind the MSDE Data Center DMZ and firewalls. Additionally, PII data has been deconstructed; restricted to the appropriate database; secured behind its own firewall; and PII data is encrypted. Anti-Virus software has been installed on all MLDS Center servers and workstations, with the MSDE Data Center providing updated versions of the software. Least privileged access has been established behind the MSDE Data Center firewalls. Over the coming months, the entire firewall will be substantially upgraded by replacing the current firewall with the managed firewall protection through the Department of Information Technology.

AUDIT TEAM

Brian S. Tanen, CPA, CFE
Audit Manager

Stephen P. Jersey, CPA, CISA
Information Systems Audit Manager

Sandra C. Medeiros
Senior Auditor

R. Brendan Coffey, CPA, CISA
Information Systems Senior Auditor

James J. Podhorniak, CFE
Staff Auditor

Edward O. Kendall
Information Systems Staff Auditor