Nicole R. Galloway, CPA
Missouri State Auditor

ELEMENTARY AND SECONDARY EDUCATION

Missouri Student Information System Data Governance

October 2015

Report No. 2015-093

http://auditor.mo.gov

October 2015

Nicole R. Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Missouri Student Information System Data Governance

Background

The Department of Elementary and Secondary Education (DESE) Office of Data System Management is responsible for the Missouri Comprehensive Data System, which includes the Missouri Student Information System (MOSIS), the student-level record system. MOSIS is the main student information reporting system used by DESE to collect student-level data from school districts. The scope of our audit included DESE management's approach to data governance, including information security, privacy, and other relevant internal controls, policies and procedures, and other management functions and compliance issues.

User Account Management

DESE management has not fully established and documented user account management policies and procedures. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges. Multiple DESE users are allowed access to the MOSIS system via shared accounts; however, DESE management does not regularly monitor these accounts to ensure actions taken by account holders are appropriate.

Data Collection

Certain MOSIS system data submissions from school districts to DESE include an optional field to collect social security numbers, even when there is no business purpose to include that information. Maintaining personally identifiable information that is not necessary for business functions places students at risk should a data breach occur. By limiting this information to the least amount necessary, DESE may limit potential negative consequences in the event of a data breach.

Breach Response Policy

DESE management has not established a comprehensive data breach response policy, as recommended by the U.S. Department of Education. Without a comprehensive data breach response policy, management may not be sufficiently equipped to respond quickly and effectively in the event of a breach, increasing the risk of potential harm to affected individuals.

Business Continuity Plan

DESE established a comprehensive business continuity plan in 2004; however, the plan has not been updated or tested, increasing the risk the plan may not be adequate to support the timely recovery of business functions after the occurrence of a disaster or other significant incident. Without an up-to-date or tested business continuity plan, management has limited assurance the organization's business functions can be sustained during or promptly resumed after a disruptive incident.

In the areas audited, the overall performance of this entity was Good.*

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

All reports are available on our Web site: auditor.mo.gov

Missouri Student Information System Data Governance
Table of Contents

State Auditor's Report 2

Introduction

Background 4
Scope and Methodology 6

Management Advisory Report - State Auditor's Findings

1. User Account Management 8
2. Data Collection 9
3. Breach Response Policy 10
4. Business Continuity Plan 11

NICOLE R. GALLOWAY, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Dr. Margie Vandeven, Commissioner
Department of Elementary and Secondary Education
Jefferson City, Missouri

We have audited the Department of Elementary and Secondary Education, Missouri Student Information System (MOSIS) data governance in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted to evaluate the effectiveness of the data governance approach, including security and privacy controls designed to secure student data and as a result of increasing concerns regarding security of information maintained in state databases. The objectives of our audit were to:

1. Evaluate internal controls over significant management and financial functions.

2. Evaluate compliance with certain legal provisions.

3. Evaluate the economy and efficiency of certain management practices and information system control activities.

4. Evaluate the security and privacy controls designed to ensure the confidentiality, integrity, and availability of data and information maintained by the MOSIS system.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

For the areas audited, we identified (1) no deficiencies in internal controls, (2) no significant noncompliance with legal provisions, (3) the need for improvement in management policies and procedures, and (4) the need to fully establish certain security and privacy controls.

The accompanying Management Advisory Report presents our findings arising from our audit of the Department of Elementary and Secondary Education, Missouri Student Information System Data Governance.

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	John Luetkemeyer, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Patrick M. Pullins, M.Acct., CISA
Audit Staff:	Hussein A. Arwe

Missouri Student Information System Data Governance Introduction

Background

The Department of Elementary and Secondary Education (DESE) reports to the State Board of Education and is primarily a service agency working with educators, legislators, government agencies and citizens to maintain the state's public education system. According to the department's website, DESE strives to guarantee the superior preparation and performance of every child in school and in life through its statewide school-improvement initiatives and regulatory functions. To help carry out this mission, the DESE utilizes a series of information systems to collect, analyze, and report student-level information.

The DESE Office of Data System Management is responsible for the Missouri Comprehensive Data System, which includes the Missouri Student Information System (MOSIS), the student-level record system. The office coordinates school district data team training and certification regarding the use of data to improve classroom instruction. In addition, the office collects and generates data to meet federal reporting requirements and compliance, as well as providing data utilized in research and analysis that impacts policy decision-making.

The MOSIS is the main student information reporting system used by the DESE. The system is composed of two separate subsystems purchased from and supported by contractors. The MOSIS Identification (ID) component is used to assign students a unique, 10-digit number to allow schools to link an individual student's records from any district in the state. The MOSIS Data Collection component is used to collect student-level data from school districts and transmit the data to the state for processing and reporting. Data collection includes elements such as enrollment and attendance, demographics, performance information, and college and career data for evaluating the success and achievements of students.

The DESE employs a user access management system for granting and administering school district employees access rights to various DESE systems, including the MOSIS ID and MOSIS Data Collection components. Each local school district has a designated user manager or security administrator who is responsible for approving and administering employee access requests and for ensuring access remains appropriate. While the DESE has assigned responsibility for the day-to-day management of user accounts to local user managers, as system owners, DESE remains ultimately responsible for ensuring access rights are appropriate.

According to the U.S. Department of Education, Privacy Technical Assistance Center,[1] data governance is an organizational approach to data

[1] U.S. Department of Education, Privacy Technical Assistance Center, *Data Governance Checklist,* is available at <https://nces.ed.gov/programs/ptac/pdf/data-governance-checklist.pdf>.

and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. This includes establishing policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, data sharing and dissemination. Establishing a comprehensive data governance program helps ensure confidentiality, integrity, and availability of data and information by reducing data security risks due to unauthorized access or misuse of data.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting personally identifiable information (PII)[2] and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

In the 2015 High-Risk Series[3] update, the Government Accountability Office (GAO) expanded the scope of the information security high-risk area to include protecting the privacy of PII. The GAO expanded this risk area due to the challenges of ensuring the privacy of PII created by advances in technology. Technological advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional

[2] According to the Family Educational Rights and Privacy Act (FERPA), personally identifiable information (PII) includes, but is not limited to (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; and (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student.

[3] Report GAO-15-290, *Report to Congressional Committees, High-Risk Series An Update*, February 2015, is available at <http://www.gao.gov/assets/670/668415.pdf>.

threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, state agencies are increasingly reliant on technology and information sharing to interact with citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

Various state and federal laws and regulations pertain to the protection of sensitive student data, including the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Protection of Pupil Rights Amendment (PPRA). Additionally, Section 161.096, RSMo, passed by the Missouri Legislature in 2014, required the State Board of Education to promulgate rules regarding "student data accessibility, transparency, and accountability."

Scope and Methodology

The scope of our audit included DESE management's approach to data governance, including information security, privacy, and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place for the MOSIS during the year ended June 30, 2015.

Our methodology included reviewing written policies and procedures, and interviewing various DESE personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained the employment records of all state employees for fiscal years 2001 to 2015 from the statewide accounting system for human resources. We matched these records to the MOSIS user account records to determine if any terminated employees had active accounts. No terminated state employees with active accounts were identified. Although we used computer-processed data from the human resources system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We obtained a listing of the MOSIS user account records from the user access management system for two school districts the State Auditor's office was currently auditing. We asked the selected districts to verify whether employees on the list of authorized users were current employees and whether the user access was appropriate. No employees with inappropriate access were identified. Although we used computer-processed data from the student records system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We obtained certain records from the MOSIS for testing. These records were modified and resubmitted to the system to test the functionality and accuracy of certain system data edits.[4] We found one insignificant issue with a numeric validity edit, which we discussed with DESE management who promptly had the edit corrected. Although we used computer-processed data from the MOSIS, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We based our evaluation on accepted state, federal, and international standards; policies and procedures; and best practices related to information technology security and privacy controls from the following sources:

- Office of Administration (OA) - Information Technology Services Division (ITSD)[5]
- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)
- U.S. Department of Education

[4] An edit, also known as a data validity check, is program code that tests the input for correct and reasonable conditions; such as account numbers falling within a range; numeric data being all digits; and dates having a valid day, month, and year; etc.

[5] The OA-ITSD established the Missouri Adaptive Enterprise Architecture (MAEA) to guide information technology decisions. The MAEA includes standards, policies, and guidelines and is made up of several information technology domains, including domains dedicated to security and information. The domains define the principles needed to help ensure the appropriate level of protection for the state's information and technology assets.

Missouri Student Information System Data Governance
Management Advisory Report
State Auditor's Findings

1. User Account Management

Department of Elementary and Secondary Education (DESE) management has not fully established and documented user account management policies and procedures. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. User account management policies and procedures should be established for all user accounts, including system administrators.

1.1 Periodic review of user accounts

DESE management has not fully established policies and procedures for administering and reviewing user access to data to ensure access rights remain appropriate and are commensurate with job responsibilities.

DESE management has provided training and issued administrative memos to local user managers emphasizing the need to ensure user account access rights remain appropriate. However, DESE management has not established a formal policy or procedures requiring local security administrators to perform a documented review of user accounts to ensure users are still employed and access rights commensurate with job responsibilities, and to verify to the DESE that user accounts have been reviewed.

Requiring a periodic review of all accounts ensures the right type and level of access has been provided. Otherwise, user accounts and access rights can be granted to or maintained for users who should not have access, according to accepted standards.

Without requiring a periodic review of user access rights, there is an increased risk of inappropriate access, that unauthorized alterations of these rights would go undetected, or that access rights would not be aligned with current job duties.

1.2 Shared accounts

Multiple DESE users are allowed access to the MOSIS system via shared accounts. However, DESE management does not regularly monitor these accounts to ensure actions taken by account holders are appropriate.

Since the access management system only allows a user account access to a single school district, DESE employees use a separate method to gain access to student data. This method allows the use of two accounts for each of the over 500 school districts in the state. Each account allows either view-only or full access to student records for a specific district. View-only accounts are used primarily for support and technical assistance purposes, while the full access accounts are typically used to upload data to the MOSIS system prior to asking the district to review and verify the information. While the rights granted a full access account allow for uploading data to the MOSIS system, only in rare circumstances would a shared account be needed to submit data to the MOSIS for processing, according to a DESE official. For example if a district ceased operations, DESE staff might need to upload and submit that district's records.

Fifteen DESE users (8 with full access and 7 with view-only access) share the passwords for these accounts. While the sharing of accounts greatly decreases the administrative burden of creating and maintaining fifteen accounts at each of the over 500 school districts (over 7,500 accounts total), this process has the potential to limit accountability for changes made in the system. If the DESE determines the continued use of shared accounts is necessary, increasing account monitoring controls would reduce risk and help to increase accountability.

Accepted standards require all users to have uniquely identifiable user accounts. Allowing multiple users to share the same account, without establishing compensating controls, makes it difficult, if not impossible, to identify the user responsible for making changes to student records.

Recommendations

The DESE:

1.1 Periodically require school district officials perform documented reviews of user access to the MOSIS to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

1.2 Eliminate the use of shared accounts, or establish compensating monitoring controls over shared accounts to mitigate the risk of lack of individual accountability for system activity.

Auditee's Response

1.1 The Department concurs with the recommendation and will put in place a process for access rights by June 30, 2016.

1.2 The Department concurs with the recommendation and has eliminated the shared accounts as of September 25, 2015.

2. Data Collection

Certain MOSIS student data submissions collect personally identifiable information (PII) that is not used by the system. Maintaining PII that is not necessary for business functions places students at risk should a data breach occur.

Local school districts upload a "Student Core" data submission to the DESE through the MOSIS Data Collection component five times throughout the year. Each of these submissions has an identical file layout, with certain fields changing status between "Required," "Optional," "Conditional,"[6] or "Not allowed" for each submission. Other data collections are submitted by school districts to the MOSIS Data Collection component throughout the year as well.

One of the optional fields collected by the DESE during the MOSIS "Student Core" submission is a student's Social Security Number (SSN). According to DESE staff, the number was required for students participating in the A+ Scholarship program since the number was used as a key field to link records between DESE and the Department of Higher Education systems, but the SSN is no longer used in this capacity. However, the SSN needs to be maintained as a data element in certain records that are not used on a daily basis because of the importance of using the data when linkages are needed to other record systems, such as across education levels within a state.

Accepted standards state minimization of the use, collection, and retention of PII is a basic privacy principle. By limiting PII collections to the least amount necessary to conduct its mission, the DESE may limit potential negative consequences in the event of a data breach involving PII. In addition, organizations should regularly review holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting their business purpose and mission.

Recommendation

The DESE discontinue the collection and maintenance of optional SSN data in the MOSIS Data Collection component and securely remove the data already collected that is no longer needed for business purposes. Additionally, the DESE should periodically review PII collected to ensure the collection of sensitive data remains necessary for business purposes.

Auditee's Response

The Department concurs with the recommendation and will remove the SSN collected in the MOSIS Data Collection component by June 30, 2016. In addition, the Department will ensure that the PII collected is needed for business purposes.

3. Breach Response Policy

DESE management has not established a comprehensive data breach response policy. Implementing a data breach response policy is an essential step in protecting the privacy of student data.

While the Family Educational Rights and Privacy Act (FERPA) does not contain specific breach notification requirements, the law requires recording of each data disclosure incident in the applicable record. However, the U.S.

[6] Conditional fields may or may not be required based on the status of a second field. For example, a field indicating the student's participation in the A+ Scholarship program is conditional on the student being enrolled in grades 9 - 12.

Department of Education recommends all educational organizations create a data breach response policy, approved by the organization's leadership, that is germane to its environment. The policy should establish goals for the response process and include the definition of a breach, staff roles and responsibilities, as well as reporting, remediation, and feedback mechanisms. The policy should be well publicized and made easily available to all personnel whose duties involve data privacy and security protection. While DESE staff provided us a document with steps to take in the event of a breach, this document had not been formally presented to or approved by DESE management and did not contain all key elements required for an effective breach response.

Documenting and formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure operations will be performed correctly and efficiently, according to accepted standards.

Without a comprehensive data breach response policy, management may not be sufficiently equipped to respond quickly and effectively in the event of a breach, increasing the risk of potential harm to affected individuals.

Recommendation

The DESE should formally document and adopt a comprehensive data breach response policy to promote an appropriate response in the event of a breach of protected student data.

Auditee's Response

The Department concurs with the recommendation, and will be adopting a formal breach response policy by December 31, 2015, and will publish the policy in the Department administrative manual.

4. Business Continuity Plan

The DESE has established a comprehensive business continuity plan; however, the plan has not been updated or tested, increasing the risk the plan may not be adequate to support the timely recovery of business functions after the occurrence of a disaster or other significant incident.

The DESE adopted a business continuity plan in May 2004; however, the plan has not been updated since that time. The maintenance section of the plan indicates the document should be reviewed annually in December. DESE staff said the plan has not been updated since that time due to staff turnover and changes in the DESE operating environment, including the Office of Administration (OA), Information Technology Services Division (ITSD) taking over responsibility for information technology services and consolidation of facilities services within the OA - Division of Facilities Management, Design, and Construction.

DESE staff said the plan has not been tested, primarily because critical functions of the plan (specifically the recovery of information systems and facilities) are no longer the responsibility of the DESE, but rather the OA divisions providing those services. While OA divisions do play a significant role, the business continuity plan also covers non-infrastructure issues, such as recovery team organization, communication plans, and DESE preparedness and response efforts needed to ensure critical DESE business functions could continue.

Continuity planning provides an efficient approach for agencies to develop policies and procedures for the timely recovery and restoration of critical processes and services vital to citizens, according to accepted standards. Continuity planning also provides a structured approach for developing cost-effective solutions that accurately reflect business requirements and integrate continuity planning principles into all aspects of information technology operations.

Without an up-to-date or tested business continuity plan, management has limited assurance the organization's business functions can be sustained during or promptly resumed after a disruptive incident.

Recommendation

The DESE maintain and test a comprehensive business continuity plan that reflects the current business environment.

Auditee's Response

The Department concurs with the recommendation and will update its current business continuity plan by June 30, 2016.