A Report
to the
Montana
Legislature

Performance Audit

Senate Joint Resolution 10: School Data Collection Systems and Processes

Office of Public Instruction

May 2016

Legislative Audit
Division

16P-01

Fraud Hotline
(Statewide)
1-800-222-4446
(in Helena)
444-4446
ladhotline@mt.gov

Performance Audits

Performance audits conducted by the Legislative Audit Division are designed to assess state government operations. From the audit work, a determination is made as to whether agencies and programs are accomplishing their purposes, and whether they can do so with greater efficiency and economy.

We conducted this performance audit 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. Members of the performance audit staff hold degrees in disciplines appropriate to the audit process.

Performance audits are performed at the request of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Aubrey J. Curtis
Joe Murray
Orry Hatcher
William Soller

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angus Maciver

May 2016

The Legislative Audit Committee
of the Montana State Legislature:

This is our performance audit of the Office of Public Instruction's (OPI) school data collection systems and processes, completed in accordance with Senate Joint Resolution 10 enacted by the 2015 Legislature. This report provides information to the legislature on OPI data collection processes. It addresses legislative questions regarding the burden on local school districts of adhering to OPI data collection requirements and whether OPI maintains the privacy of students and their families. Overall, our work identified a need for OPI to strengthen the management of data collections and the maintenance of student privacy. This report includes recommendations for complying with state law in regards to a K-12 Data Task Force, strengthening data governance activities to manage school district data collections, and improving risk assessment and mitigation regarding the individual privacy of students and their families. A written response from OPI is included at the end of the report.

We wish to express our appreciation to the superintendent and her staff for their cooperation and assistance throughout the audit

Respectfully submitted,

/s/ Tori Hunhausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Figures and Tables

Figures

Tables

Elected, Appointed, and Administrative Officials

Office of Public Instruction

Denise Juneau, Superintendent

Dennis Parman, Deputy Superintendent

Madalyn Quinlan, Chief of Staff

Ken Bailey, Assistant Superintendent of Operations

Montana Legislative Audit Division

Performance Audit
Senate Joint Resolution 10: School Data Collection Systems and Processes
Office of Public Instruction

May 2016 16P-01 Report Summary

The Office of Public Instruction collects thousands of data elements from local school districts in Montana; however, some data elements currently collected are not required by state or federal mandates and place additional reporting requirements on local school districts. In addition, there are weaknesses in how OPI secures and maintains the individual privacy of students and their families.

Context

Per state law, the Superintendent of Public Instruction is responsible for the general supervision and welfare of K-12 public schools and districts in Montana. The Superintendent serves as the chief executive officer for the Office of Public Instruction (OPI) and administers the affairs of the agency, which provides education-based services to school-aged children and teachers in over 400 local school districts across the state. Administering these services generally requires that OPI collect program and student data from local school districts to comply with both state and federal requirements. According to OPI management, school districts respond to nearly 200 different data collections administered by OPI, several of which include personally identifiable information (PII) for students and their families. In response to Senate Joint Resolution 10 passed by the 2015 Legislature, we conducted an audit of OPI data collection systems and procedures.

Audit work examined OPI's data governance structure to determine if it is an effective mechanism to manage data collection activities and how OPI maintains the individual privacy of students and their families. As part of our work, we identified unnecessary data elements collected by OPI that are not required by any state or federal mandates, contributing to the burden of data collections on local school districts. For example, of 37 data collections we reviewed, we identified two collections containing data elements not currently required, including examples related to special education and salary information for school district staff. Audit work concluded that OPI's current data governance structure is not an effective forum to manage its data collections. We also noted that OPI currently does not convene the statutory K-12 Data Task Force.

In regard to PII, we concluded that deficient controls within OPI have compromised the confidentiality of student data. We identified concerns regarding the confidentiality of student data in the areas of system account access, email, physical security, security training, mobile device management, and research agreements. For example, we observed instances where OPI staff transported student information via unsecure email, with several emails pertaining to students with disabilities, including name, birthdate, and disability-related diagnosis and evaluation information. Ultimately, our work concluded that OPI needs to implement procedures to mitigate data security risk factors and assess risks to student data security on a regular basis.

(continued on back)

Results

Audit recommendations address the need for OPI to comply with statutory requirements, strengthen data governance activities, and mitigate and assess risks to student data privacy. Recommendations include:

- Strengthen data governance by incorporating the periodic review of OPI data collections for duplication, legal requirements, and potential information technology system consolidations,
- Update and clarify agency policies and procedures for staff data governance requirements, including training staff on those requirements,
- Include structured input from key stakeholders and develop a sustainability plan for maintaining data governance,
- Continually work in consultation with the statutory K-12 Data Task Force,
- Monitor and evaluate employee compliance with OPI's Student Record's Confidentiality Policy and implement procedures to mitigate data security risk factors, and
- Prioritize and implement measures to assess and document risks and potential threats to information student data security on a regular basis.

Recommendation Concurrence	
Concur	6
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (16P-01) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **ladhotline@mt.gov**.

Chapter I – Introduction

Introduction

Per state law, the Superintendent of Public Instruction is responsible for the general supervision and welfare of K-12 public schools and districts in Montana. The Superintendent serves as the chief executive officer for the Office of Public Instruction (OPI) and administers the affairs of the agency, which provides education-based services to school-aged children and teachers in over 400 local school districts across the state. OPI administers a wide variety of education-based services for K-12 schools and districts, including programming and technical assistance in the areas of student enrollment, school accreditation, school curriculum development, academic achievement, educator licensure, school nutrition, special education services, standardized testing, and state entitlement funding. Administering these services generally requires that OPI collect program and student data from local school districts to comply with both state and federal program requirements and enable OPI to evaluate and monitor these activities.

According to OPI management, school districts respond to nearly 200 different data collections administered by OPI, several of which include personally identifiable information (PII) on students and their families. Based on concerns over burdensome data collection requirements and how OPI maintains the individual privacy of students and their families, the 2015 Legislature passed Senate Joint Resolution (SJR) 10 requesting a performance audit of OPI school data collection systems and procedures. Consequently, the Legislative Audit Committee prioritized a performance audit of OPI data collection activities. This chapter further discusses the scope of our audit work and provides background information on data collections activities conducted by OPI, including areas where we conducted audit work.

Audit Scope and Objectives

OPI administers a wide variety of education-based services for K-12 schools and districts. This includes collecting program and student data from local school districts to comply with both state and federal program requirements, which enables OPI to evaluate and monitor these activities. While §20-7-104, MCA, references a statewide data system used by OPI to manage K-12 data collections from local school districts, there is no single statewide data collection system. Data collections range across numerous areas such as school nutrition, student enrollment and program participation, and special education. Considering the scale and diversity of data collections, we assessed the landscape of these various collections in an effort to determine where to best focus audit work. Based on this assessment work, we determined that OPI's data governance structure used to collectively manage its data collections and the controls OPI maintains over the privacy of student information merited audit examination. Based

on audit assessment work, we developed the following two objectives for examining OPI data collection activities:

1. Has OPI implemented a data governance structure to effectively manage data collections and reduce unnecessary duplication?
2. Does OPI ensure its data collection activities and sharing methods and practices maintain a level of individual privacy for students and their families by reducing unnecessary disclosure of personally identifiable information?

The following paragraphs discuss scoping considerations regarding those areas of OPI data collections in which we conducted audit work.

Data Governance

Data governance is commonly defined as an organizational approach to data and information management that encompasses the full life cycle of data. Data governance within OPI was established in approximately 2011, in response to a federal grant OPI received to develop a statewide longitudinal data system. As part of this federal grant, OPI indicated that it intended to create a data governance structure, as it was struggling as an agency with data collections due to the lack of a formal data governance policy to guide data coordination. However, during audit assessment work, we determined that while OPI developed several policy documents outlining the data governance structure within OPI, these documents were never completed, with current policies and procedures at OPI not accurately reflecting how data governance functions within the agency. Consequently, we examined OPI's data governance structure to determine if it is an effective mechanism to manage data collection activities.

Student Data Security

In a world increasingly defined by the use of large data sets to analyze everything from consumer spending habits to individual health care to school improvement, the risk of data privacy breaches has become a common concern for both public and private organizations. As part of its numerous data collections, OPI routinely gathers PII for students and their families. PII is any data that could potentially identify a specific individual. Since the legislature identified student privacy as a concern in SJR10, we examined how OPI maintains the individual privacy of students and their families in accordance with applicable state and federal laws, administrative rules, and office polices.

Audit Methodologies

To accomplish our objectives, we completed the following methodologies:

- Obtained and reviewed applicable state and federal laws, administrative rules, and office policies for how OPI manages its various data collection activities, including data governance and student privacy requirements.

- Obtained and reviewed the 37 data governance request reviews from fiscal year 2014 and fiscal year 2015 to determine if OPI consistently reviews and approves new or revised data collection items.
- Obtained and reviewed the legal authorities for the 37 data collections OPI identified as completed by all school districts in Montana for potential duplication and to determine if OPI is only collecting data from school districts in response to legal requirements.
- Obtained and reviewed sources for criteria regarding data governance and student privacy for similar K-12 educational organizations in other states, including best practices developed by the federal government and national data quality organizations.
- Examined both electronic and physical methods used by OPI for transmitting and retaining student data, including system interfaces, email transport, physical security, user access, and mobile device management.
- Obtained and reviewed three active data sharing agreements from 2013 through 2015 to examine how OPI reviews and approves the release of student information within the requirements of state and federal law.
- Interviewed OPI staff to obtain their input on how data governance operates within OPI, including how OPI maintains the individual privacy of students and their families.
- Interviewed local educational stakeholders with whom OPI interacts to obtain their perspective regarding data governance and student privacy at OPI.
- Developed and conducted a survey of school district data stakeholders to obtain the perspective of school district staff on the consistency of data collection activities, including perceptions of the data governance process, redundancy in data collections, and how districts secure student data.
- Conducted field visits to ten school districts to assess the involvement of local school districts in data governance and obtain their perspective on OPI data collection activities and student data privacy.

An Overview of OPI Data Collection Activities

As part of administering education-based services for K-12 schools and districts, OPI collects a variety of program and student data from local school districts to comply with both state and federal program requirements and enable OPI to evaluate and monitor these activities. According to OPI management, the office only requests and collects information from local school districts that is specifically required by the Montana Legislature or another governmental entity to fulfill either statutory or regulatory requirements. These other governmental entities include the federal Departments of Education and Agriculture, and the Montana Board of Public Education. Examples of state-required collections include student enrollments that allow for the calculation of entitlement payments to local school districts, school bus inspections, and the

various information collected for accreditation purposes, such as class size and teacher qualifications. Federally required data collections are generally comprised of reporting requirements related to federal funding sources, such as school nutrition, special education, or academic achievement programming. Many federally-required collections consist of periodic grant reporting requirements for Montana schools which have elected to participate in these programs, such as grants related to use of technology in classrooms, and resources to assist rural schools to improve the quality of instruction and academic achievement. So while school districts collectively respond to nearly 200 different data collections administered by OPI, not all data collections are required of all school districts, with many data collections related to federal funding sources in which individual school districts voluntarily participate that require periodic reporting as a condition of funding. According to an analysis conducted by OPI management for the 2015 Legislature, nearly 70 percent of data collections only apply to less than a third of school districts in Montana.

While OPI does collect a variety of program and student data from local school districts to comply with both state and federal program requirements, OPI collects this information through a network of many different information systems managed by many different programs within different divisions within the agency. There is no single statewide data collection system. Currently, OPI maintains five primary information collection systems, with approximately 20 additional data collection and reporting modules. OPI management estimates the total investments in OPI data collection systems at nearly $9 million, with ongoing costs including personal services and contracting of approximately $4 million annually. The following bullets describe the five primary data collection systems maintained by OPI, with descriptions of those systems:

- **Montana State Educator Information System (MSEIS)** collects information related to educator licensure. This system was developed by an outside contractor to meet OPI needs.
- **EGrants** is used by OPI to manage the various federal grants and programs in which Montana participates. The system is considered an "off-the-shelf" product, which OPI has customized to its needs.
- **Achievement in Montana (AIM)** represents the student information system used by OPI. AIM is also considered an "off-the-shelf" product, which OPI has customized to its needs. This system is used to collect student demographic, enrollment, and program participation data.
- **Terms of Employment, Accreditation, and Master Schedule (TEAMS)** is used by OPI to collect information on the employment status of school district employees. The system also is used to collect accreditation information related to district course offerings and teaching assignments. TEAMS was initially developed by a vendor, but later taken over by OPI staff for programming and customization.

- **Montana Automated Education Financial and Information Reporting System (MAEFAIRS)** is the in-house developed and supported school finance system used by OPI to calculate entitlement payments to local school districts.

Examples of the approximately 20 additional data collection and reporting modules include various in-house technical solutions for collecting information related to activities such as special education, school nutrition, transportation services, and continuous school improvement plans. Many of these various systems and modules interface with each other for the purposes of linking information collected by another system which is then used by the users of both systems. For example, MAEFAIRS obtains student enrollment information from AIM which is used to calculate entitlement payments. OPI management indicates that it is their goal to have all of these various systems "talk" to each other to provide integration across all systems. However, this is not always the case, with OPI staff needing to extract data from one system and upload the information into another system. Per OPI management, while not a true system interface, this eliminates the need for school districts to enter the same information more than once. At time of our audit work, OPI did not have a current diagram or comprehensive information available to describe the relationships between the various systems and related programming it uses to collect information from local school districts. Currently, OPI relies on data governance concepts to guide and coordinate data collections conducted across the agency. The following paragraphs describe in further detail the concept of data governance, including how it operates within OPI.

What Is Data Governance?

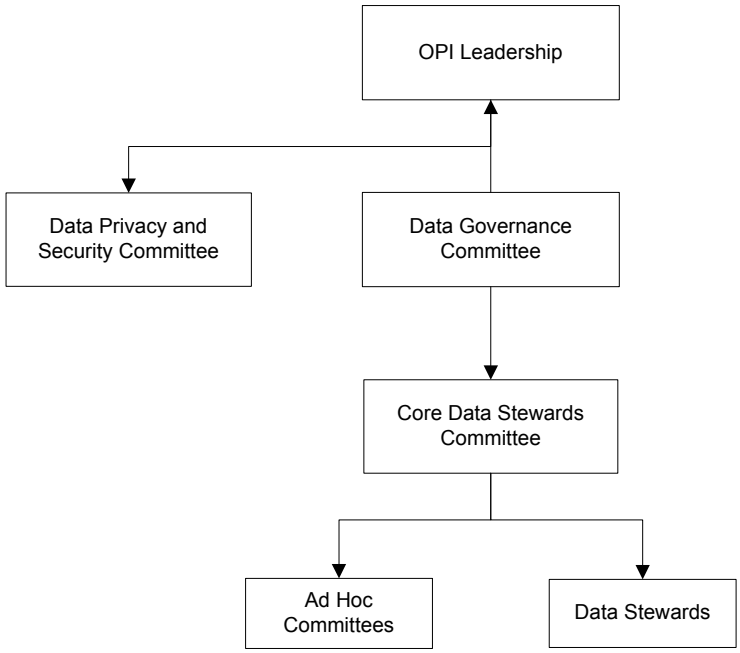
As noted above, data governance is commonly defined as an organizational approach to data and information management that encompasses the full life cycle of data. The concept of data governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. Data governance includes the practice of establishing and implementing policies, procedures, and standards for the effective use of an organization's data assets. Ultimately, data governance is the decision-making process used by an organization to prioritize and allocate resources, and measure results to ensure data is managed in support of an organization's business needs. As is the case with the general governance or oversight of any agency or activity, data governance could include the establishment of governing bodies, policies and procedures, membership rights, decision rights, and monitoring or enforcement expectations. In the case of data governance, these general governance concepts would all be related to the overall picture of how an organization approaches and manages the data it uses.

How Does Data Governance Operate Within OPI?

As part of the federal grant OPI received, it established several objectives for the development of a statewide longitudinal data system, including creating a data governance structure. After receipt of the grant, OPI hired a consultant in 2011 to create a framework to document data practices and develop new policies where needed. As a result of this work, OPI developed several policy documents defining a data governance structure within OPI, including organizational charters outlining the roles and responsibilities for several committees. These committees include a data governance committee, a data privacy and security committee, and a core data stewards committee.

Per these charters, data governance committee members are key management staff with OPI responsible for the development of policies needed to ensure effective implementation of data systems and collection methods, and ensuring awareness of data collection and reporting requirements. Data privacy and security committee members review and consider data requests for accessing data and research proposals related to requests for access to confidential student data. Core stewards represent content experts or skilled data analysts within OPI who are responsible for ensuring that data collections are coordinated, non-redundant and as simple as possible for school districts. These charters also establish a data governance facilitator within OPI who is responsible for oversight, coordination, and facilitation of data governance activities. There are also other participants in OPI's data governance structure, including data stewards or program level staff who work with program data on a daily basis, and the opportunity to form ad hoc committees when considering unique concerns within data governance. Figure 1 (see page 7) illustrates the current organizational structure of data governance within OPI.

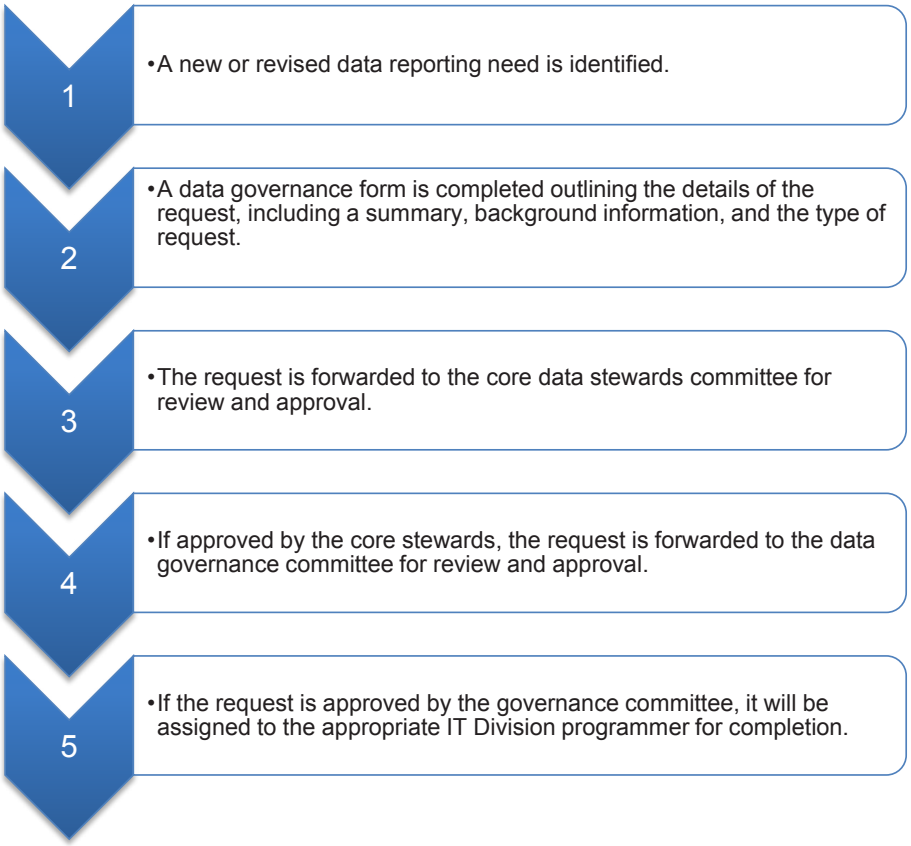
Figure 1
OPI Data Governance Structure



Source: Compiled by the Legislative Audit Division from OPI records.

While OPI data governance documents identify multiple duties and roles for how data governance operates within the agency, data governance at OPI is primary comprised of a request review process, whereby data governance-related issues such as the need for a new or revised data collection element is reviewed, considered, and approved. The primary purpose of this process is to ensure that when reviewing requests for new or revised data elements that the data is not currently being collected elsewhere within OPI and how to leverage existing data collections when considering new or revised collection requirements. Data governance will also review proposed formatting changes with existing data collections, such as adding or modifying data tables to an existing application to better manage and access data within the application. Figure 2 (see page 8) illustrates the data governance request review process.

Figure 2
OPI Data Governance Request Review Process



Source: Compiled by the Legislative Audit Division from OPI records.

An Overview of OPI Student Data Security

Recent growth in the amount of student records collected and stored electronically by educational agencies has increased the scrutiny of data management and protection practices they employ. Consequently, data security is an integral part of data governance and stewardship. The U.S. Census Bureau defines data stewardship as an "organizational commitment to ensure that identifiable information is collected, maintained, used, and disseminated in a way that respects privacy, ensures confidentiality and security, reduces reporting burden, and promotes access to statistical data for public policy." As part of implementing data governance, OPI has established several committees responsible for not only promoting data collection efficiency but also ensuring privacy. Per OPI policy, the data stewards committee is responsible for establishing rights and security levels for all data elements, queries, procedures, and tools to ensure that data are stored, managed, and reported in a secure manner. The data and privacy committee

is responsible for reviewing data requests for accessing data and research proposals related to requests for access to confidential student data.

As the state education agency in Montana, OPI is required to comply with the federal Family Educational Rights and Privacy Act (FERPA), which is the federal law that protects the privacy of student education records. FERPA was codified in 1974 to allow parental access to their student records, the ability to amend the records if deemed necessary and prudent, and a level of control over what information is disclosed from these records. Educational agencies and institutions may disclose student record information, without the consent of the parents, to agencies or organizations that are legally responsible for the care and protection of the student. Any student record policy or procedure at OPI must be in compliance with FERPA, especially those regarding confidentiality and data sharing. There is a viable concern from parents on keeping student data private, as it may include health and disciplinary information. Security breaches in the United States are more prevalent today than ever before, and according to recent history, the State of Montana is no exception. One such data breach occurred in December 2015 within the Missoula County Public Schools. A file, containing sensitive information of over 1,100 current and former students, was attached to an email sent to several families of student athletes. The file was reported to include information such as student disabilities, immunization requirements, academic standings, drug and alcohol use, as well as criminal records. While this breach did not involve OPI, this incident not only sheds light on the importance of data security controls, but also the magnitude of information collected by school districts and likely shared with state and federal agencies.

Local Control Frequently Impacts OPI Data Collection Activities

Within K-12 education, local control refers to the governing and management of public schools by elected or appointed representatives serving on governing bodies, such as school boards or school committees that are located in the communities served by the schools. The concept of local control is grounded in the belief that the individuals and institutions closest to the students and most knowledgeable about a school are best suited to making important decisions. This notion of governance is often contrasted with state or federal policies intended to influence the structure, operation, or academic programs in public schools. In Montana, OPI provides education-based services to school-aged children and teachers in over 400 local school districts across the state and enforces broad state and federal education mandates. However, local leaders and governing bodies can make independent decisions about the governance and operation of the public schools in their communities, including how to best meet those state and federal education mandates.

As a part of our audit work, we noted that local control frequently impacts data collection activities conducted by OPI in both how OPI effectively collects data and the manner in which student data is maintained by local school districts. For example, while school districts in Montana may use AIM as their local student information system, several larger districts have chosen to use student information systems offered by different vendors to better meet their local needs. Consequently, the process to collect data from these districts can frequently involve technical-based issues, with a local school information system not interfacing well with AIM. Likewise, while local school districts must comply with state and federal laws regarding student data privacy, those districts independently decide how to maintain student data privacy. OPI does not have the authority to direct local school districts on how to ensure the individual privacy of students and their families.

Report Contents

The remainder of this report includes chapters detailing our findings, conclusions, and recommendations in the following areas:

- Chapter II presents information on how OPI should prioritize and strengthen data governance activities, including consulting with a K-12 data task force as required by state law.
- Chapter III discusses the necessity for risk assessment related to data security, along with areas of concern that require immediate risk mitigation.

Chapter II – Data Governance

Introduction

As a result of the direction of Senate Joint Resolution 10 to examine the school data collection systems and procedures in place within the Office of Public Instruction (OPI), our first objective assessed the data governance structure in place at OPI used to manage data collections. We conducted this work in an effort to examine whether OPI has implemented a data governance structure to effectively manage data collections and reduce unnecessary duplications. Overall, we found that OPI does not comply with state law to work in consultation with a data task force to advise OPI on the best options for a statewide K-12 data system. We also found that the current data governance structure within OPI is not an effective forum to manage data collections, and does not identify and reduce unnecessary data collection burdens on local school districts. Our work identified the need for OPI to convene the statutory K-12 data task force and also strengthen its current data governance structure. This chapter presents our findings and recommendations in these areas.

School Districts Report That OPI Data Collections Detract From Other Work

In order to obtain a wide level of input from district stakeholders who interact with OPI data collection activities, as part of our work we visited ten local school districts to assess their involvement in and perspective regarding OPI data collection activities. In order to obtain a broad perspective regarding OPI data collections, we visited school districts in both urban and rural areas. Table 1 (see page 12) represents the ten school districts we visited, including the student enrollment in those school districts in the 2014-15 school year.

Table 1
School Districts Visited as Part of Audit Work With Enrollment

School District Name	City	Student Enrollment
Billings Public Schools*	Billings	16,418
Great Falls Public Schools*	Great Falls	10,336
Missoula Public Schools*	Missoula	8,791
Kalispell Public Schools*	Kalispell	5,839
Miles City Public Schools*	Miles City	1,586
Glasgow K-12 Schools	Glasgow	813
Townsend K-12 Schools	Townsend	654
West Glacier Elementary	West Glacier	51
Trail Creek Elementary	Miles City	13
Pine Grove Elementary	Brusett	9

Source: Compiled by the Legislative Audit Division from OPI records.

*Represents a consolidated school district.

We also conducted a survey of local school district staff that routinely provides data to OPI as part of standard data reporting collections. We conducted this survey in an effort to obtain and review information on the consistency of data collections, including perceptions of local school districts on the data governance process, and redundancy or duplication in OPI data collections. Based on information provided by OPI management, we determined that, in the 2014-15 school year, there were 408 school districts in Montana, with a total enrollment of 144,532 students. Student enrollment in individual school districts ranged from 1 student to 11,348 students. Several school districts in the state have consolidated for administrative purposes. We surveyed school district authorized representatives, county and district school superintendents, and school district business clerks. Overall, our survey produced a response rate of 58 percent. For the purposes of our work, we also established size factors to categorize school districts survey responses based on student enrollment. Table 2 (see page 13) represents the size factor, the total number of school districts categorized by that size, the total number of students enrolled in that size category in the 2014-15 school year, and the number of survey respondents in each of those size categories.

Table 2

Audit Survey School District Size Factors, Student Enrollment, and Survey Respondents

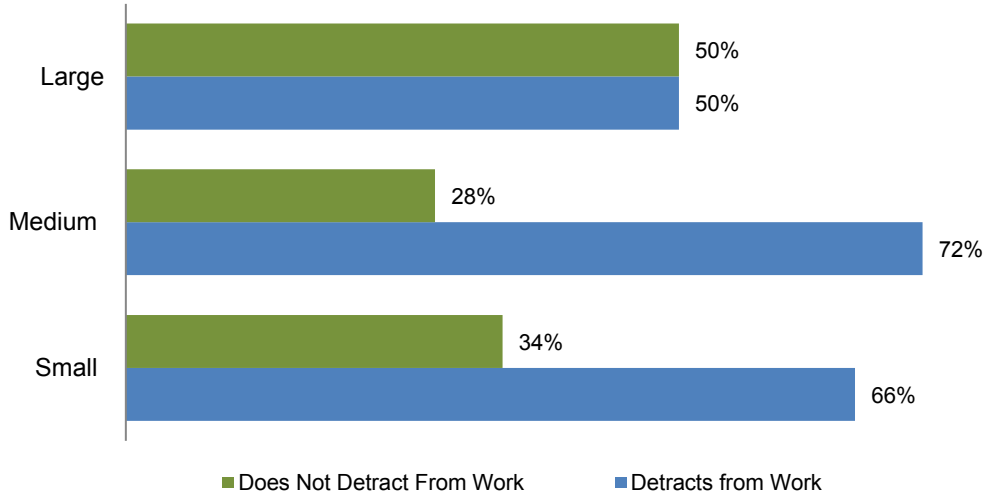
Size Factor	Number of School Districts	Total Student Enrollment	Number of Survey Respondents
Large (greater than 2,500 students)	12	56,743	32
Medium (501 to 2,500 students)	47	45,110	97
Small (500 or fewer students)	349	42,679	303
Total	**408**	**144,532**	**432**

Source: Compiled by the Legislative Audit Division from OPI records and survey results.

Overall, 66 percent of respondents reported that OPI data collections detract them from their ability to conduct other work, rating the average burden of OPI collections as approximately 3 on a scale of 1 to 5, with 5 being the most burdensome and 1 being the least burdensome. However, when considering responses based on size factors, our survey indicated that small- and medium-sized school districts more frequently report that OPI data collections are a burden and detract from their ability to conduct other work. However, when rating the burden of data collections, districts of all sizes most frequently rated the burden of OPI data collections as either a 3 or a 4 on the scale of 1 to 5. Collectively, respondents from school districts of all sizes reported they spend an average of 18 hours weekly on OPI data collections during peak collection periods. Figure 3 (see page 14) represents the percentage of districts by size factor which indicated that OPI data collections detract from their ability to conduct other work. Figure 4 (see page 14) represents how school districts rated the burden of OPI data collections on a scale of 1 to 5 by size factor.

Figure 3

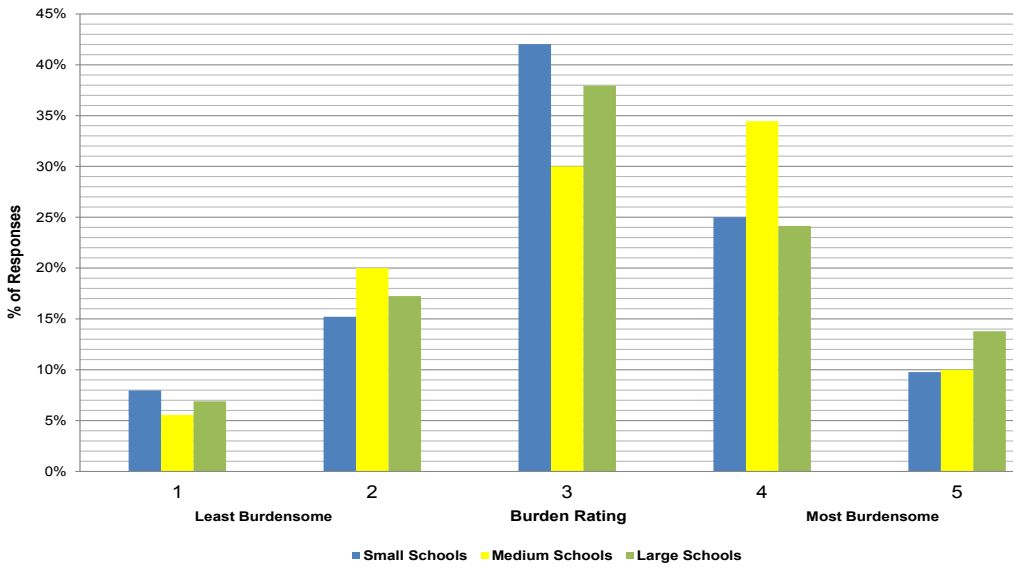
Percentage of Survey Respondents Who Report OPI Data Collections Detract From Their Work



Source: Compiled by the Legislative Audit Division from survey results.

Figure 4

OPI Data Collections Burdens as Rated by Local School Districts



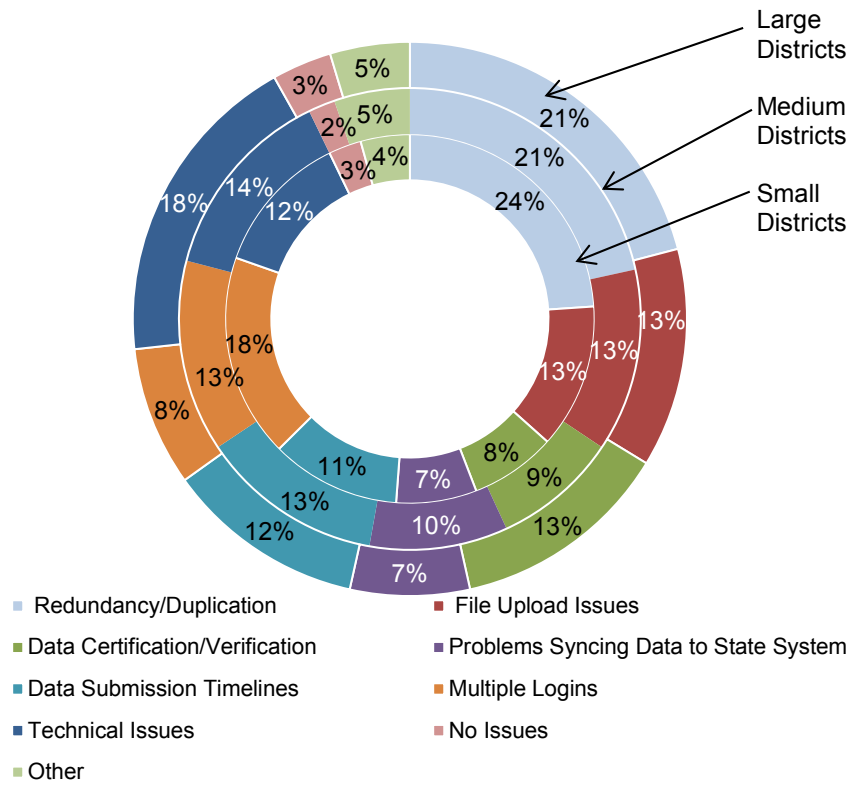
Source: Compiled by the Legislative Audit Division from survey results.

As part of our survey work, we also assessed the types of issues school districts have encountered with OPI data collections. Our work noted that there were few differences

between differently-sized schools and the types of issues they commonly encountered. For example, concern over redundancy and duplication was the most frequent issue reported by school districts of all sizes. Figure 5 represents the types of issues reported by school districts as a percentage of total responses for each sized district. The inner ring represents small school districts, the center ring medium districts, and the outer ring larger districts:

Figure 5

Types and Percentages of Data Collection Issues Reported by School Districts by Size



Source: Compiled by the Legislative Audit Division from survey records.

Overall, our survey work indicated that school district staff collectively reported several common concerns regarding the burden of data collections, regardless of the size of the district. School districts all expressed concerns about the Terms of Employment (TOE) school district staff compensation collection that is conducted by OPI. School districts widely expressed a frustration at how onerous the TOE data was to collect, with no real understanding of the purpose of the collection or how the information is used. They reported that district staff compensation information is also reported as part of other school trustee financial reporting. In regard to special education, school districts with established student information systems reported that not only do they report on

special education activities in their student information system, but they also report this information directly to special education staff within OPI, which they considered redundant and duplicative. While school district staff generally reported OPI staff as helpful when they experience data collection issues, district staff generally had the perception of OPI data collections activities being siloed, with little communication between the various divisions at OPI.

Industry Best Practices and Other States Exhibit More Comprehensive Data Governance

As part of our work, we reviewed best practices for data governance developed by the federal government, industry organizations, and other states regarding the effective use of data within education. Based on information obtained and reviewed from the U.S. Department of Education, data governance is an agency-wide approach to managing information from collection through use. Consequently, there should be distinct roles for and relationships among program areas, information technology, and leadership, as well as district representation and an agency-wide data governance coordinator. Industry best practices indicate that data governance provides state agencies a structure in which to define the roles and responsibilities needed to ensure clear processes for collecting and reporting education data and accountability for data quality and security. These industry best practices suggest focusing on six key areas when implementing data governance, including vision and mission; composition and membership; roles and responsibilities; data decisions; committee processes; and sustainability.

As is the case in Montana, education agencies in other states are also responsible for collecting and reporting data based on various state and federal requirements. The other states we reviewed report similar struggles when collecting education-based data from local school districts. For example, other states we reviewed also reported concerns with data duplication, redundancy, and the burden of data collection on local school districts. We noted that while other states may use a single student information system, they still collect considerable amounts of non-student data from local school districts through multiple data systems. While our work indicated that other states experience similar data collection challenges, we also noted that the data governance structure in the other states we reviewed is generally more comprehensive in comparison to Montana. These data governance structures included a more defined and proactive role in reviewing data collection activities. In addition to reviewing any new or revised data collection elements, data governance in other states also periodically reviews all state data collections directed at local school districts to assess collection requirements and take steps to avoid duplication. For example, in Idaho, the Data Management Council oversees the assessment and review of the underlying authority of data collections and

recently was responsible for a reduction in the number of data elements collected from local school districts. Staff with K-12 based education agencies in other states reported that periodic requests to review new or revised data collections needs are only a part of the role for data governance, with data governance also responsible for assessing and inventorying data collections in an effort to reduce data collection requirements imposed on local school districts. Our review of data governance activities in other states also highlighted that the lack of ongoing training or a strong commitment on the part of management had impacted the success of past data governance efforts. Organizational buy-in was specifically noted by staff in all of the other states we contacted as an essential component for a successful data governance structure within a state education agency. Overall, our review of best practices for data governance highlighted the need for OPI to strengthen data governance by periodically reviewing data collections, updating and clarifying policies and procedures, including structured input from key stakeholders, and developing a sustainability plan to maintain data governance.

The Effectiveness of OPI Data Governance Is Limited

As reported by OPI management, school districts respond to nearly 200 different data collections administered by multiple OPI divisions. However, not all data collections are required of all school districts. Throughout the course of our work, OPI management stressed they only collect data from local school districts that are specifically required by another governmental entity to fulfill either the statutory or regulatory requirements set by that entity. We reviewed the 37 data collections OPI said are currently submitted by all school districts in Montana to comply with a statutory or regulatory mandate. Our work compared these collections with its underlying legal authority. These 37 data collections were comprised of over 1,500 individual data elements. We completed this work to determine if OPI only collects data from local school districts in response to existing legal authorities and also to assess potential duplication. Data collections we reviewed are conducted by OPI for numerous reasons, including district budgetary reports, district staffing and compensation information, student enrollment counts, student assessment registration, school nutrition reimbursements, and students receiving special education services. Table 3 (see page 18) represents divisions within OPI in which we reviewed data collections, the number of data collections within each of those divisions we reviewed, and the number of data elements within those collections.

Table 3
OPI Data Collections Reviewed Including Data Elements by Division

OPI Division	Number of Collections Reviewed	Number of Data Elements Reviewed
Accreditation	2	43
Centralized Services	4	327
Health Enhancement and Safety	4	490
Measurement and Accountability	14	322
School Finance	9	272
Special Education	4	123
Total	**37**	**1,577**

Source: Compiled by the Legislative Audit Division from OPI records.

OPI Collects Unnecessary Data From Local School Districts

Overall, our work identified that OPI's current data governance structure is not an effective forum to manage its data collections. Our work found that the current data governance structure is ineffective in identifying and reducing unnecessary collections, duplication, and redundancy for school district data collections in Montana. For example, as part of our work to review the underlying legal authority for the 37 data collections, we noted a varied level of awareness on the part of OPI staff regarding the authority for their various collections. While the majority of data collections we reviewed were required by state or federal mandates, we identified collections that were not wholly required. Of the 37 data collections we reviewed, 35 of those data collections were wholly supported by state or federal requirements, with two collections containing six unnecessary data elements, including examples related to special education and salary information for school district staff. Our review also identified potential redundancies relative to data collections, including opportunities for potential system consolidation regarding special education collections and questions regarding the frequency of student program participation collections. The following bullets summarize the unnecessary data elements and potential redundancies we identified as part of our work:

- Within OPI's Special Education Division, we identified two unnecessary data elements related to a special education data collection for students who have been removed from the classroom to an alternative setting as a result of disciplinary action. While OPI is required by the federal government to collect disciplinary data for special education students, OPI also collects

information on the number and type of victim involved in the disciplinary action, such as if the victim was another student or school personnel. OPI staff believe that the collection of this information is a historical oversight and a holdover of a past data collection which is no longer required, but has not been removed from the current special education disciplinary data collection.

- The OPI School Finance Division collects compensation information for school district staff in what is commonly referred to as the TOE data collection. Section 20-7-104(3)(b)(i), MCA, requires that OPI collect the total amount of compensation paid to the employee by each district. However, our work identified four unnecessary data elements collected by OPI related to employment days, employment hours, employment status code, and base salary. While state law does reference base salary, OPI currently collects this information within another collection. OPI management reported that these unnecessary data elements are gathered as contextual information that could be used when conducting comparative analysis of school district compensation. They indicated they have provided this type of information to education stakeholders in the past, but OPI does not currently conduct any type of analysis with the unnecessary elements we identified.
- As for potential system consolidation, our work identified that OPI's Achievement in Montana (AIM) student information system currently appears to have the capability to collect data of special education students, but OPI has developed an in-house data module to collect this information due to historic perceptions regarding the lack of functionality for AIM. OPI management reported that there are some concerns on the part of special education staff to consolidate, as the in-house data module currently meets their needs. However, OPI management acknowledged that OPI data collections should be more holistically viewed and not driven by one group within the office.
- There are numerous educational services and programs in which students participate, such as free and reduced meals, gifted and talented, special education, or job corps. Our work identified that the frequency of these program participation collections is not tied to a specific legal requirement. OPI staff collect this information multiple times annually since the individual timing requirements are unknown to current OPI staff.

While our findings in this area were isolated in nature, the unnecessary data elements we identified do not align with OPI representation that the agency only collects information in response to the requirements of external legal authorities. It should be noted that there are approximately 150 additional data collections which audit work did not review, where there may be additional unnecessary data elements. Our work raises reasonable questions regarding the extent of unnecessary data collections conducted by OPI which contributes to the burden felt by local school districts. This highlights the need for OPI to periodically and systematically assess all of its data collections to ensure the office is only collecting information that is required by state or federal law. While the circumstances of unnecessary data elements we identified varied

in cause, the outcome remains the same, with OPI collecting unrequired information and contributing to the perceived burden of data collection on school districts. As part of review work of collections authorities, we also reviewed over 1,500 data elements for potential redundancy. However, an analysis of the various data elements was challenging as OPI does not maintain an agency-wide data dictionary that defines the various data elements it collects. Currently, the different divisions responsible for administering the various collections maintain individual data dictionaries, with similarly named data elements named differently across different data collections. Therefore, identically named data elements may mean different things across different systems. Since OPI does not maintain an agency-wide data dictionary defining these data elements, we were unable to identify any clear examples of data duplication. However, OPI staff who work with data as part of their duties stated it is likely data duplication exists across the different data collections administered by various divisions within OPI, meaning it is also likely school districts are being required to submit duplicate information to OPI.

OPI Has Made Efforts to Improve Data Collections

While OPI has conducted some analyses in the past to improve data collection processes and mechanisms for OPI local school districts which have led to improvements, these analyses have been isolated and reactive in nature. These analyses have been in response to external sources such as federal grants or legislative interest and do not represent periodic or ongoing efforts proposed by OPI to continually assess OPI data collections. For example, as part of the federal grant OPI received to develop a statewide longitudinal data system, the office conducted a survey and analysis of its various data collections in an effort to evaluate and improve the various methods used by OPI to collection information from school districts. As part of effort, OPI conducted an inventory of data collections with the intention of identifying and resolving redundancies; however, the work slowed at some point and was not an ongoing effort. OPI management indicate that these efforts are currently evolving, with similar data collection review activities having not historically occurred within data governance. However, these activities are now coordinated with data governance. Overall, as a result of OPI not periodically assessing its data collections, there continue to be unnecessary burdens on local school districts regarding OPI data collections.

Recommendation #1

We recommend the Office of Public Instruction prioritize and strengthen its current data governance structure to incorporate the periodic review of data collections for duplication, legal requirements, and potential information technology system consolidation.

The Request Review Process Lacks Uniformity

As part of our review of 37 request reviews from fiscal year 2014 and fiscal year 2015, we evaluated whether OPI conducts these review activities consistently and within established policies and procedures. Our work consisted of reviewing available data governance request review forms and committee minutes from the core data stewards and data governance committees. Overall, we noted that request reviews is a reactive process which relies on OPI staff to independently bring forth requests for new or revised data collection needs for review and approval. The fact that OPI staff independently brings forth new or revised data collection needs is not an issue. Rather, our work found that data governance within OPI is not clearly defined for or understood by staff, with program and IT staff inconsistently participating in the data governance structure. Our work noted OPI staff do not clearly understand what types of issues should be submitted for review as part of the request review process or what the expectations are for the documentation and completion of requests. OPI does not train staff periodically on data governance requirements and responsibilities. OPI management and staff also do not consistently agree upon what constitutes a data collection. Our audit work noted that the request review process was not uniformly conducted, with a general lack of consensus among OPI staff regarding the role of data governance. The following bullets represent audit observations regarding the data governance request review process:

- One hundred percent (37/37) of data governance request review forms were incomplete, including referral or assignment information.
- Fifty-four percent (20/37) of data governance request reviews lack documentation of approval from core data stewards.
- Twenty-four percent (9/37) of data governance request reviews were missing documentation of approval from the data governance committee.

Regarding referral and completion of the request, it was unclear if all issues brought forth as part of the request review process were always addressed. For example, our work noted one request regarding establishing AIM system access for Montana State Prison staff to report data for inmates with disabilities under the age of 21 who are still eligible for disability-related educational services. Our review noted that this request was submitted twice as a data governance request review. However, based on available documentation, it appeared the request was delayed due to OPI staff absence, with the resolution and completion of the issue not clearly documented. Our audit work identified a need for OPI to more clearly define what office expectations are for data governance, including what types of data collection issues must be reviewed within the context of data governance and how those issues are resolved.

Recommendation #2

We recommend the Office of Public Instruction:

A. *Update agency policies and procedures for data governance requirements,*

B. *Clarify the roles responsibilities of program and information technology staff regarding the current data governance request review process, and*

C. *Provide training to staff on data governance requirements.*

Local School District Observations Support Need for More Robust Data Governance

Overall, our visits and survey work with local school districts highlighted the need for a more formal and robust means for districts to communicate data collection concerns with OPI on an ongoing basis. Larger school districts with established school information systems often reported the extract and upload process by which they provide student information from their system to OPI does not always work well, expressing concerns over the frequent need to verify information with OPI. They questioned why the interface could not be configured for automatic updates, rather than periodic uploads. Smaller districts manually entered the information or used the same system as OPI, with little in the way of concerns to report. Larger districts acknowledged that while they generally have dedicated staff who perform data collections, these activities are resource intensive and take time that could be directed elsewhere. Staff at smaller school districts reported they generally wear many hats, with OPI data collections detracting from the many other duties they are required to perform. However, staff at smaller school districts acknowledged they do not have the same level of enrollment as larger districts. Larger districts with established student information systems reported they are generally not receptive to a single statewide student information system, citing concerns over local control, statewide access to local student data, and the time and resources which have been spent on developing technology platforms which meet the needs of individual districts. Smaller districts with no student information system also did not see the need for a statewide system, expressing similar concerns of local control. School districts of all sizes collectively reported they had little if any knowledge of data governance or the K-12 data task force enacted by the Legislature. Audit survey work indicated that nearly 90 percent of respondents currently have no awareness of the data governance structure within OPI. School district staff frequently reported they did not always understand exactly why OPI collects certain data or how it is used. They indicate that school districts have a lot of experience and perspective that could be of value to OPI.

When discussing our observations, OPI management indicated they were unsurprised by how school districts generally responded. They expressed frustration at the fact that school districts of all sizes routinely rank the issue of redundancy and duplication as their largest concern, without districts providing specific examples. However, OPI management acknowledged that the TOE collection is often cited as school districts of all sizes as redundant, with compensation information also collected as part of school trustees financial reporting, as a specific example of redundancy. They indicated the TOE collection currently requires school districts to provide some information that is not required in state law, with OPI not currently using the information to conduct any sort of analysis on the compensation for school district staff. OPI management indicated that our district observations generally aligned with past survey work and observations of their own. They noted that smaller schools reported OPI collections detracting from their work at a higher rate, which is likely attributable to the fact that larger districts have dedicated staff who perform data collection activities rather than staff within smaller districts who have many duties for which they are responsible. OPI staff also indicated that data verification activities may be confused by districts as data collections, which is not accurate.

OPI Management Views Data Governance as Internal and Voluntary

The concept of data governance within OPI was primarily driven by the application of a federal grant to develop a statewide longitudinal data system. As part of this federal grant, OPI committed to developing a data governance structure, with an emphasis on developing common practices for all data systems at OPI. Consequently, OPI management and staff frequently describe data governance as an internal and voluntary effort and have not imbedded data governance into OPI's organizational structure. Data governance currently is a limited effort where expectations for staff participation are not clearly defined or understood within the agency. OPI management and staff frequently indicate that there is no specific requirement for data governance to exist within the office. However, they stress the current state of data management within OPI is likely a better environment for managing data collections than prior to the establishment of data governance. OPI staff also report they do not know if there is value in including local school districts within data governance, as the structure is currently implemented as an internal administrative function. They report they receive frequent solicited and unsolicited feedback regarding data collections from local school districts. Presently, data governance is not prioritized within OPI, with current policies and procedures out-of-date and not accurately reflecting the activities of data governance. There is a lack of ongoing education and training within OPI regarding what is types of activities staff should bring to data governance, including what constitutes a data collection. Without the involvement of local school districts

in data governance, OPI is not taking the opportunity to leverage the expertise and experience of education stakeholders when managing OPI data collections. In addition, as a result of its grant-based origins, OPI has not developed a sustainability plan for maintaining data governance beyond federal resources, with OPI management and staff indicating that the future of data governance is uncertain, with limited resources to conduct, strengthen, or even continue current efforts in the future. According to OPI management, they requested and received three FTE from the 2015 Legislature to continue, in part, data governance practices. However, our work did not identify any current practices in place to support data governance beyond federal funding. OPI management acknowledge that our audit observations indicated that OPI needed to do a better job of communicating the importance of data governance, including clarifying expectations and educating staff regarding the purpose of data governance with the agency. They reported that, based on our audit work, it is likely time to assess the current state of data governance in an effort to better define its role within OPI.

Other States Frequently Include External Stakeholders as Part of Data Governance

As part of our audit work, we reviewed data governance activities in other states, including Colorado, Idaho, and Kentucky. We noted the other states we reviewed typically provide structured input from key stakeholders, such as local school districts, as part of their data governance structures. While data governance in Montana is best described as an OPI internal administrative structure, data governance in other states is commonly comprised of both internal and external functions, including the participation of local school districts. For example, in Colorado, an internal Data Management Committee comprised of state program staff is responsible for reoccurring tasks such as reviewing requests for data. An external group known as the Education Data Advisory Council is comprised of both state and district staff and periodically reviews every state data collection in an effort to avoid duplicate collections. This external group is defined in state law and charged with making certain that collections are necessary and monitoring collections from a district or stakeholder perspective.

RECOMMENDATION #3

We recommend the Office of Public Instruction strengthen its current data governance structure by including structured input from key stakeholders such as school districts and developing a sustainability plan for maintaining data governance beyond federal resources.

State Law Establishes a K-12 Data Task Force

The prior sections discuss the need for OPI to include district stakeholders to aid in the daily administration of data collections. However, our review of OPI data collection activities also highlighted the need for OPI to comply with state law regarding the involvement of statewide policy-makers in analyzing the best options for a statewide data system. State law indicates that a K-12 data task force shall serve in an advisory capacity to OPI. The task force shall review, monitor, and provide input and guidance in enhancing a statewide K-12 data system. While §20-7-104, MCA, references a statewide data system used by OPI to manage K-12 data collections from local school districts, there is no single statewide data collection system. Rather data collections within OPI are diverse and managed by project leadership teams within many different divisions using a variety of different information systems which collectively can be considered OPI's statewide data system. State law indicates that the superintendent of public instruction shall continually work in consultation with the K-12 data task force to analyze the best options for a statewide data system. Section 20-7-104(6), MCA, requires that the office of public instruction and the K-12 data task force shall collaborate to enhance the statewide data system to support:

- The needs of school districts in using data to improve instruction and student performance;
- The collection of data from schools through a process that provides for automated conversion of data from systems already in use by school districts or the office of public instruction and that resolves the repetition of data entry and redundancy of data requested that has been characteristic of the data system in the past and that otherwise reduces the diversion of district staff time away from instruction and supervision;
- Increased use of data from the centralized system by various functions within the office of public instruction; and
- Transparency in reporting to schools, school districts, communities, and the public.

Per state law, the task force is comprised of numerous stakeholders within the education community, including legislators, school board trustees, school administrators, teachers, school technology staff, and parents. Presently, OPI does not convene the statutory K-12 data task force to be used in an advisory capacity to analyze the best options for a statewide K-12 data system.

OPI Management Does Not See a Clear Purpose for the K-12 Task Force

At the time of our audit work, the K-12 task force had only met once, in January 2014, since being established by OPI. Available meeting materials indicated there was

a general lack of understanding regarding the purpose of the task force. Meeting minutes from the task force indicated that stakeholders voiced concerns about student data in several areas, such as data privacy, student performance, data duplication, and the appropriate use of student data. The task force wanted to obtain input from a wide variety of education stakeholders on how to effectively use data related to student achievement. However, despite stakeholders seeing the task force as an opportunity for improving data collections, OPI management said that the purpose of the task force has never been clearly defined, having not developed any specific goals, objectives, or deliverables. Without what they perceive as a clear purpose, OPI management has not proactively taken the opportunity to define a role for the task force and do not see value in assembling the group on a periodic basis. As a result, OPI management has not prioritized convening the K-12 data task force. However, state law specifically outlines the areas in which OPI is required to collaborate with the task force.

Education Stakeholder Dissatisfaction Has Increased

The topic of data collections has been an ongoing concern for local school districts. However, as a result of OPI not convening the K-12 task force as required by state law, there has been an amplified level of dissatisfaction among the various K-12 education stakeholders across Montana, including local school district staff and state legislators, regarding the perceived burden of OPI data collections on local school districts. Without the forum of the task force to provide an opportunity for an ongoing dialogue regarding how OPI collects data from local school districts and the development of a statewide K-12 data system, OPI is not only in noncompliance with state law but also not taking the opportunity to leverage the expertise of K-12 education stakeholders. Audit survey work indicated that nearly 70 percent of respondents were generally unaware of the purpose or role of the task force. However, those who were aware of the task force expressed frustration regarding OPI's commitment to the task force, characterizing OPI as not interested in the ideas or solutions generated by the task force. While the topic of the burden of OPI data collections is an issue that has been discussed for several years in the education community, the failure of OPI to proactively convene the K-12 task force has only increased education stakeholder frustrations.

RECOMMENDATION #4

We recommend the Office of Public Instruction prioritize and continually work in consultation with the K-12 data task force to analyze statewide school data collections, including addressing and resolving school district concerns regarding data entry repetition, redundancy, and duplication.

Chapter III – Student Data Security

Introduction

State law requires that each department head is responsible for ensuring security for all data within that department. It also requires the designation of an information security manager to administer the agency security program, implementation of safeguards to reduce identified threats, and internal evaluations of the security program. The Office of Public Instruction (OPI) has addressed these statutory directives by establishing a Student Record Confidentiality Policy for the agency in 2008, with updates completed in 2013. The purpose of this policy, as stated, is to "establish procedures and responsibilities governing the access, use and dissemination of confidential, sensitive and/or restricted student information by the [OPI]." The scope of the policy applies to all contractors and employees of OPI, in addition to all other parties requesting access to confidential, sensitive, or restricted information. The basis for this policy can be found in the federal Family Educational and Privacy Rights Act (FERPA), with added detail specific to OPI processes and procedures. Overall, information technology is comprised of three main facets, namely access, use, and dissemination. Consequently, our audit work also references OPI's Plan for Development of the Information Systems Security Plan (ISSP) and the 2014 OPI IT Strategic Plan.

Our work examined both electronic and physical security of student data collected, stored, and distributed by OPI along with any associated risks. This work included an inspection of the general security controls around the OPI's student information system. In addition, we examined controls around business processes (manual or automated) that dealt with student data, and whether they comply with federal law, statute and/or OPI policy. Our work did not review local school district controls for retaining and transmitting student data. Per OPI management, they do not have the legal authority to direct local school districts on how to maintain the individual privacy of students and their families. Our audit work identified a need for OPI to strengthen the manner in which it currently maintains the individual privacy of students and their families and also assess data security risks regarding student data. This chapter presents our findings and recommendations in these areas.

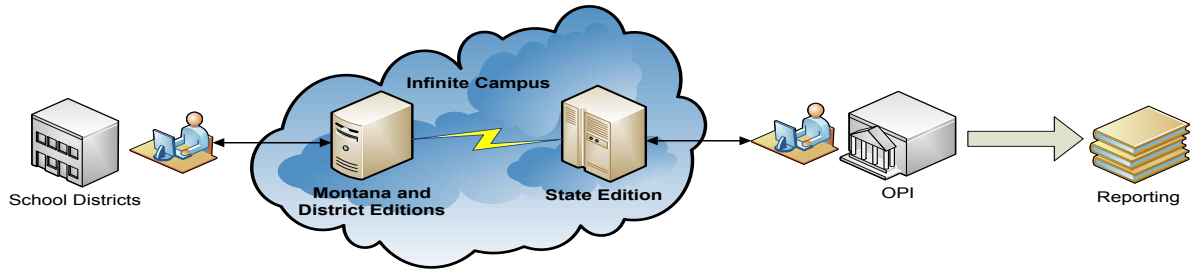
OPI Student Information System

The Achievement in Montana (AIM) system is the primary student information system (SIS) where OPI collects personally identifiable information (PII) on students and their families. PII is any data that could potentially identify a specific individual. We primarily focused our security-related audit work on the AIM system. There are essentially three different versions of AIM, with varying levels of functionality. These versions are the following:

- The State Edition of AIM is used by OPI staff and contains all the Montana districts' enrollment, demographic, programs and special education data.
- The District Edition of AIM is the edition that can be used by the districts as their main local SIS and contains a complete package of student data and features. OPI indicates that approximately a third of Montana school districts use this edition.
- The Montana Edition of AIM is the edition generally used by smaller school districts as their main local SIS. It is also used by districts with an established SIS from another vendor to transfer information to the State Edition. The Montana Edition has less functionality than the District Edition, but contains the same basic set of enrollment, demographic, programs and special education data.

Recently, AIM has moved from internal system administration (OPI servers and databases) to a cloud solution at the vendor location. As a result, a significant level of security responsibility has been outsourced. However, the AIM vendor gets audited by a third-party firm on an annual basis, which involves an examination of data security. While OPI still has a vested interest in the security procedures of the vendor, its primary role is now to manage the access to the State Edition of AIM. The following figure illustrates the flow of student information reported by local districts to OPI via the AIM system.

Figure 6
The Achievement in Montana Student Information System



Source: Compiled by the Legislative Audit Division from OPI records.

OPI Business Processes And Student Data Confidentiality

As described above, the decision to move the AIM IT infrastructure from a local presence to a cloud-based solution managed by a third-party vendor lessened the burden of maintaining general controls on the primary student information system for OPI. However, student data confidentiality must be addressed through examination of business process controls around that system. Business process controls can be automated or manual and typically cover structure, policies, and procedures that

operate across processes within the office. These controls support the completeness, accuracy, validity, and confidentiality of data. As part of our audit work, we evaluated the various processes affecting the security of student data within OPI. Overall, we concluded that deficient business process controls within OPI have compromised the confidentiality of student data. The following sections outline the various business processes where we identified concerns regarding the confidentiality of student data, including AIM account access, email, physical security, security training, mobile device management, and research agreements.

Review of AIM Account Access

Both the Montana Edition and the District Edition are managed by local school districts – i.e. user accounts and role-based user rights. The State Edition user accounts are managed by staff at OPI. As part of audit work, we requested a current list of the users with access to the State Edition of AIM. Of the 33 access accounts within the State Edition, we identified 8 generic accounts created for certain school districts. We contacted the vendor for AIM, which indicated that in 2012 there was a push to move all districts with access to the State Edition of AIM over to the Montana Edition. According to the vendor, there could be selective instances where a district would need the access, but the goal was to have all districts on the Montana Edition, since the state would no longer need to manage the accounts of users at the district. The vendor confirmed that generic accounts would pose a certain degree of security risk to the data within the State Edition; however, they were also able to determine that user roles were built into these accounts to allow these districts to only view information pertinent to their individual district.

In an effort to evaluate the use of these generic accounts, we also contacted districts with access to the State Edition of AIM. The majority of district contacts for these accounts said that the primary purpose of the account was to be able to verify that the information entered into either the Montana Edition or the District Edition was uploaded properly into the State Edition. OPI staff reviewed all the accounts in question and disabled some in response. Regardless of the roles that have been assigned to the accounts, it is in the best interest of OPI to either restrict the districts from having access to the State Edition, or at least implement tighter controls on these accounts. For example, eliminate the generic user accounts and specify usernames that identify the actual user of the account (moderately restrictive) or disable the account after a limited amount of time (least restrictive). The moderately restrictive solution would allow access to the information throughout the year, but would isolate access to a single user versus a generic account. It is possible for the district to share account credentials among personnel; however, the onus is on the district and not on OPI. The least restrictive solution would assume a level of risk with the generic account, but only

allows access during a short window throughout the year. This would also mitigate the burden of account management that comes with changing personnel at the district. A third option, besides eliminating access to the districts altogether, would be to apply both individual accounts with a window of time for access (most restrictive).

Electronic Mail (email)

The email we use as part of our daily work lives is not secure. It was not designed with privacy or security in mind. The best way to protect email communications is to encrypt them, where information is scrambled and only accessible using a key or other credentials. As part of our audit work, we obtained access to OPI staff email accounts and reviewed email correspondence for individuals within OPI with direct access to student data. We limited our review to periods of high data collections when student counts from local school districts are collected by OPI and focused on emails with attachments. Audit work identified eight emails that violated student data confidentiality. Several emails we identified pertained to students with disabilities, including name, birthdate, and disability-related diagnosis and evaluation information. The subject emails were sent between OPI employees, as well as from the school districts to the OPI. Upon review, OPI management confirmed that the emails we found contained sensitive and identifiable student information and were in violation of the OPI policy that directs personnel to not send any student data over unencrypted email. We also included questions in our survey of school districts addressing information security. Specifically, we asked school district staff which methods they used to transfer student data to or from OPI. While the majority identified transfer methods that would protect student privacy, some respondents (6 percent) indicated they have transmitted student information via email to OPI. Although this is a relatively small proportion of respondents, the sensitivity of some student data and the risks involved in email transfers still make this a concern.

Physical Security

Our audit work included a review of physical security of hardcopy documents at OPI. To do this, audit staff performed an after-hours walk-through of one of OPIs buildings that primarily houses employees dealing with student data on a routine basis. OPI buildings have single entry open and public access points, with no security requirements to enter. During the course of the walk-through, we inspected only documents that were in plain sight on individual desks; we did not sort through documents that were stored on employee's desks. We also examined documents in waste/recycling baskets, along with unlocked filing cabinets that were located in the work area. We identified one document with sensitive student information on an OPI staff member's desk. This document was a case management report for students with disabilities containing the names, birthdays, and a disability-related diagnosis for those students. We did not

identify student data in any of the unlocked filing cabinets or in the waste/recycling bins. According to OPI policy, all office employees are responsible for protecting data by "prevent[ing] disclosure of data by protecting visibility of reports and computer monitor when displaying and working with confidential information." In addition, "physical data (including hard copies of reports, storage media, notes, backups) should be protected from unauthorized persons, or locked when not in use." While the results of our inspection were not alarming, it is sufficient to say that the office could have reasonable cause for concern that sensitive information is not being properly secured overnight, and individuals without a need to know could potentially gain access to sensitive student data. For example, at the time of our review, janitorial staff were also in the building performing routine cleaning activities.

OPI Security Training

In a letter to all Cabinet Members and Heads of Agencies dated September 2013, the Governor's office stressed that "maintaining the security of information is a shared responsibility in which each of us has a critical role, and awareness of computer security essentials is key to the security of State of Montana's computer systems." The correspondence goes on to require all executive branch State of Montana employees to take cyber security training on an annual basis beginning that same month. The training is provided by the State Information Technology Services Division (SITSD). Based on audit work, OPI has not implemented any requirement for annual security awareness refresher training at this time. Internal policy at OPI does include information security training, but does not indicate how often training should occur. For new employees at OPI, security training is accomplished once during the onboarding process.

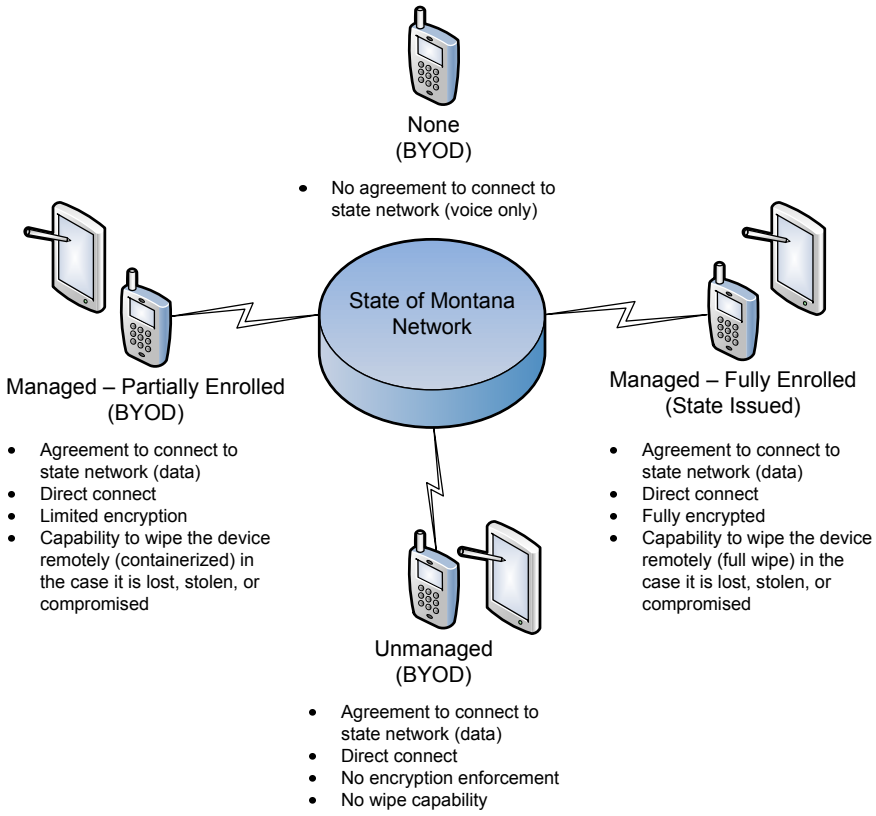
Currently, OPI is exploring the possibility of receiving assistance from the SITSD with providing on-site security training to program managers. SITSD staff confirmed that discussions with OPI have been ongoing and there are plans to "roll-out" an agency-wide requirement for annual security awareness training in the near future. Within the Plan for Developing the OPI ISSP, awareness and training (AT) is included as a baseline control family from the National Institute of Standards and Technology (NIST) – a required standard to follow based on state policy. AT controls are described in the ISSP as operational controls which will "enable all users across an organization to make informed, safe decisions." Based on the sensitivity of the information collected by OPI, combined with the criticality of these controls for agency personnel to make informed and safe decisions, information security training should be provided immediately for all OPI employees and required on an annual basis. The ISSP states that the presence of threats from both external (malicious) and internal (nonmalicious) sources may indicate a need for mitigation efforts as soon as reasonably possible, possibly sooner

than the time needed to develop and implement the OPI ISSP. Audit work, along with the OPI ISSP, would indicate that security training should be a prioritization prior to the suggested timeline of AT controls being implemented April of 2017. As noted above, our audit survey work identified inappropriate methods of transmitting student information between OPI staff and from local school districts to OPI, highlighting the need for additional training and education for OPI staff regarding how to best ensure student data privacy.

Mobile Device Management

OPI policy on the use of mobile devices for business purposes was created to align with the state mobile device management (MDM) policy. As part of our work, we obtained a list of the employees within OPI who are currently under agreement for either unmanaged or managed mobile devices. Unmanaged devices are "bring your own devices" (or BYOD) and can have direct access to state email and calendaring. However, security of these devices rests solely on the individual user and OPI has no capability to wipe any data remotely in the case it is lost, stolen or compromised. Managed mobile devices can either be fully-enrolled or partially-enrolled. Fully-enrolled devices in the state's MDM policy are typically agency-owned devices with direct access to the state network, and have the ability to detect if the device has been compromised, along with the capability to remotely wipe (i.e. remove) all data from the device if a problem is detected. Partially-enrolled devices can be BYOD and will also have direct access to the state network, and will have "containerized storage" which separates state data from personal files, pictures, music, etc. Information in containerized storage is what will be wiped remotely in the event the device is lost, stolen, or compromised. Figure 7 (see page 33) illustrates the difference between the devices under MDM.

Figure 7
State Mobile Device Management



Source: Compiled by the Legislative Audit Division from OPI records.

At the time the audit was conducted, there were 62 mobile devices assigned to OPI staff, with approximately half of these devices registered as unmanaged. We also determined that some of the unmanaged accounts had additional devices (such as tablets) listed, which conflicts with OPI internal policy. This policy limits registration to one device per account. A possible explanation provided by OPI for the additional devices was the inability to limit how many devices may be able to be registered. The following table outlines the total number of mobile device accounts currently registered for OPI staff, including the number of managed, partially managed, and unmanaged devices.

Table 4
OPI Mobile Device Management Accounts

Managed	Managed–Partially Enrolled	Unmanaged	Total Mobile Devices
21	12	29	**62**

Source: Compiled by the Legislative Audit Division from OPI records.

The risk involved with allowing unmanaged devices to access state resources, such as email, is that authentication happens once when registering. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information. There is no requirement to re-authenticate, and individuals with possession of the device can directly access state email. The only layer of security would be a passcode on the phone or tablet, which realistically cannot be enforced on BYOD devices. Recently, SITSD modified the MDM policy to require all mobile devices accessing the state network to be managed devices. The initial compliance date for the state was April 1, 2016. However, according to SITSD staff, the date has been pushed to July 1, 2016, in order to allow additional time for agencies to budget for and move devices to a fully managed MDM solution. While OPI currently is in a similar position as all other state agencies to comply with the state policy regarding mobile device management, our work identified OPI staff with unmanaged mobile devices with routine access to student data. Considering our audit findings in regard to OPI staff transmitting student data via unsecure email, mobile device management is an area of concern regarding student privacy within OPI.

Research Agreements

As part of our work, we also obtained and reviewed active research agreements that are currently in place with OPI. Research agreements represent requests from outside parties for confidential student data to conduct research. Within OPI's data governance structure, the Data Privacy and Security Committee is responsible for reviewing and approving any research agreement data requests. Since 2013, the committee has received five requests, with three research agreements currently active. For the purposes of audit work, we reviewed the three active research agreements. We contacted the research leads for the current agreements. Two of the research agreements originated from students either in Masters or Doctoral programs at the University of Montana (UM). One of those studies was conducted by an administrator at a local school district. After this study was completed, the researcher sent his doctoral dissertation to OPI for its records (as required through the agreement). Attached to the documentation sent, he included email correspondence regarding the processes for obtaining and handling the data provided by OPI. The liaison from OPI that sent the email indicated how the data would be transported (through secure e-Pass) and when the information needed to be destroyed. In a conversation with the researcher, it was confirmed that the OPI liaison did reach out after the expiration of the agreement to determine whether the data was destroyed as required. In addition to this correspondence, there is another layer of oversight from UM–the Institutional Review Board (IRB). An IRB is a university-level committee established to review and approve research involving human subjects. While FERPA does not specifically require IRB approval for agreements, OPI's Guidance for Reasonable Methods and Written Agreements, states that "research proposals involving

human subjects may have to be reviewed and approved by IRBs…" and recommends IRB review and approval as a best practice. However, there is no location to document IRB approval on OPI's research proposal agreement form.

Our review of IRB approval showed that one of the two research agreements coming from UM had approval letter from the IRB. When we contacted UM, it was confirmed that IRB approval had occurred only for the one study identified. From our review of both research agreements from UM, student data is requested in both and there is no indication of why one would require IRB approval, while the other would not. The third current research project is from a university outside of Montana, and is requesting student data from OPI. Based on audit work, there is no supporting documentation regarding IRB approval included with this request form. After contacting the lead researcher, it was discovered that the data has not yet been provided by OPI. Overall, regarding requests for student data, the research request process generally complies with FERPA requirements. The request form stipulates the responsibilities of the researcher and those of OPI representative or liaison. However, when applicable, OPI could improve its ability to assess and monitor student data used for research purposes by requiring IRB approval with the research agreement form before releasing requested student data. This would provide another layer of oversight through university IRBs, and would help mitigate some of the risk inherent in providing sensitive data to third parties.

Monitoring Compliance of Student Data Confidentiality

Over the course of our work, we identified areas of concern that are the result of a lack of monitoring by management at OPI to ensure its employees are correctly performing business processes and procedures while also complying with OPI's Student Data Confidentiality Policy and FERPA. Section 2-15-114, MCA, requires the necessity for internal evaluations of data security, which is echoed with the requirement for a "continuous monitoring strategy" found in state policy regarding information security. While it is impossible for an agency to eliminate all data security risk within their organization, it is reasonable to expect an agency to mitigate risk by effectively identifying and assessing threats, implementing appropriate policies and procedures, and monitoring staff and business processes to ensure policy is followed and identified risks are mitigated as quickly as possible. This risk is elevated for agencies which handle sensitive student information.

Recommendation #5

We recommend the Office of Public Instruction monitor and evaluate employee compliance with its Student Record's Confidentiality Policy and implement procedures to mitigate data security risk factors in the following areas:

A. *Generic access accounts issued to districts for State Edition of the Achievement in Montana System,*

B. *Emailing student personally identifiable information,*

C. *Confidential documents left unsecure in workspaces,*

D. *Requirements for annual information security awareness training,*

E. *Unmanaged personal devices accessing the state network, and*

F. *Requirements for Institutional Review Board approval for applicable research agreements from universities.*

Assessing Risk Is a Basic Information Security Practice

Proper risk management, according to industry standards, encompasses three processes: risk assessment, risk mitigation, and evaluation. Organizations will never eliminate data security risk; however, proper management of risk is necessary for administrators to prioritize resources and ensure confidentiality of data to the best of their ability. This discussion of risk leads to the question of how to determine which option is the best for the organization, or in other words, what level of risk is acceptable. Assessing risk is an inherent responsibility of information security specialists. Due to the ever-increasing reliance on electronic data, agencies need to incorporate periodic assessments of current and potential risk to information security into their business processes. This not only supports a level of assurance that information is accurate and confidential, but also provides management the basis to determine whether policies are appropriate and whether resources are allocated efficiently. Audit work identified several data security risks involving AIM access, email, physical security, security training, mobile device management, and research agreements.

Recently, OPI developed an ISSP which incorporates state policy requiring agencies to implement baseline security controls based on the NIST framework. Included within those security controls is risk and security assessment. According to the ISSP, risk assessment will not include security assessment and will take eight months to accomplish. According to the ISSP timeline, estimated date of completion for risk assessment procedures is April/May of 2017. Security assessment is scheduled for implementation four months after, in approximately August/September of 2017. While

it is positive that OPI has developed an ISSP and has placed a level of importance on information security, the various data security risks identified during audit work indicate that it is important for OPI to assess the security of the data it manages, including student data as a higher priority. Given the sensitivity of much of the student data collected and maintained by OPI and the nature of the risks faced by this office, we believe security of student data is of primary importance and should be addressed at a higher level of priority than is currently the case. Past audit work has also identified concerns regarding security management, with limited progress developing policies and procedures for a security program. It is essential that OPI make data security a priority. Measures must be taken, in conjunction with plan development, to identify, assess, and mitigate information security risk in the area of student data.

RECOMMENDATION #6

We recommend the Office of Public Instruction prioritize and implement measures to assess and document risks and potential threats to student data security on a regular basis.

Office Response

Montana
Office of Public Instruction
Denise Juneau, State Superintendent

opi.mt.gov

Office of Public Instruction
P.O. Box 202501
Helena, MT, 59620-2501
(406) 444-3095
(888) 231-9393
(406) 444-0169 (TTY)
opi.mt.gov

May 23, 2016

Tori Hunthausen, Legislative Auditor
Legislative Audit Division
Room 135, State Capitol
P.O. Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen,

Following is our response to the recommendations contained in the Senate Joint Resolution 10: School Data Collections Systems and Processes performance audit:

Recommendation #1
We recommend the Office of Public Instruction prioritize and strengthen its current data governance structure to incorporate the periodic review of data collections for duplication, legal requirements, and potential information technology system consolidation.

We concur. The following item will be added to the Data Governance Committee charter:

"Annually prepare an analysis of data collections for OPI Leadership that
- Confirms the statutory basis for all data elements;
- Identifies any duplicate data elements collected by OPI;
- Identifies any system consolidations that would reduce the reporting burden on schools; and
- Includes plans to resolve any of the above items."

In addition, OPI will institute changes in OPI leadership roles to clarify responsibility for data governance outside of the data governance committee and facilitate communication between the data governance committee and OPI leadership.

The recommendation does not specifically address the issue of reducing burden on school districts and the related finding of six data elements that are collected but are not required by statute, rule, or federal regulation. The two special education data elements will be removed before this collection occurs again. For the four data elements relating to school district salary information, the OPI will advise the organizations that have requested this information that the OPI plans to discontinue gathering this information and allow those organizations time to respond to this notice. The OPI notes that eliminating these data elements will not eliminate an entire data collection for the schools.

Also, the OPI believes the burden on school districts will only be reduced by eliminating some data collections. A portion of the reporting burden on the schools is solely required by 20-7-104 MCA (attached) which was passed during the 2011 legislative session. The legislature may want to revisit this statute and consider repealing some of the data requirements.

Recommendation #2
We recommend the Office of Public Instruction:

A. **Update agency policies and procedures for data governance requirements.**

B. **Clarify the roles and responsibilities of program and information technology staff regarding the current data governance request review process, and**

C. **Provide training to staff on data governance requirements**

We concur. By October 1, 2016, OPI will determine which policies and procedures should be changed or created. The resulting policies will include clear role definitions for program and information technology staff. The revised policies and data governance training for all OPI employees associated with data collections will be completed by January 31, 2017.

Recommendation #3
We recommend the Office of Public Instruction strengthen its current data governance structure by including structured input from key stakeholders such as school districts and developing a sustainability plan for maintaining data governance beyond federal resources.

We concur though the audit does not include a sufficient discussion of the efforts that OPI has made in the past to solicit input from school districts on data governance concerns. By October 1, 2016, OPI will study and create the data governance structure that formalizes the regular input of stakeholders to data governance management.

Regarding sustainability of data governance post federal funding, the audit states that the OPI obtained an appropriation in 2015 for three FTE that will, in part, replace the federally funded FTE supporting data governance. The sustainability of data governance is not in question, but the transition from federal funding is still in progress.

Recommendation #4
We recommend the Office of Public Instruction prioritize and continually work in consultation with the K-12 data task force to analyze the best options for a statewide data system, including opportunities to resolve data repetition and redundancy with school data collections.

We concur. OPI will reconvene the K-12 data task force no later than December 1, 2016. OPI will request an appropriation from the legislature to support this activity.

In the sections leading up to this recommendation and the preceding two recommendations, several statements are made that suggest the OPI conducts duplicate data collections and does not obtain or respond to school district input on the issue of data duplication. While the OPI concurs with the specific recommendations, the OPI does not agree with this finding.

The auditors heard statements from school and OPI staff that duplicate data collection is likely, but were not able to produce any examples despite their review of all of the data elements in the 27 data collections. In 2012 the OPI formed the Data Access Research Access Task Force (DART) that solicited input from school districts on duplications in data collections. The findings of this task force resulted in the elimination of the identified duplications. Since that work was completed, the OPI has been very deliberate to eliminate all duplicate reporting requests and have responded to every report where it has been found to occur in the

field. It has been about year since the last report of a specific example of duplicate reporting has been brought to the attention of OPI by anyone.

The OPI will continue to respond to any school district complaints of duplicate data being collected.

Recommendation #5

We recommend the Office of Public Instruction monitor and evaluate employee compliance with OPI's Student Record Confidentiality Policy and implement procedures to mitigate data security risk factors in the following areas:

A. Generic access accounts issued to districts for State Edition of AIM

B. Emailing student personally identifiable information (PII)

C. Confidential Documents left unsecure in workspaces.

D. Requirements for annual information security awareness training.

E. Unmanaged personal devices accessing the state network, and

F. Requirements for Institutional Review Board approval for applicable research agreements from universities.

We concur.

A. All generic access accounts will be terminated by July 1, 2016.
B. Employees that were discovered to have violated OPI policy for emailing student PII have been counseled. OPI will add to its policy a requirement that OPI employees must permanently delete emails received containing PII and inform the sender to send via a secure method. OPI employees with access to student PII data will receive refresher training on the OPI student confidentiality policy by September 1, 2016.
C. The employee that was discovered to have violated OPI policy for leaving PII unattended has been counseled. OPI employees with access to student PII data will receive refresher training on the OPI student confidentiality policy by September 1, 2016.
D. OPI will determine appropriate annual security awareness training in consultation with ITSD and conduct that training by December 31, 2016.
E. The new Mobile Device Management technology being implemented by SITSD will eliminate unmanaged personal devices by August 1, 2016
F. IRB approval is now required for research agreements.

Recommendation #6

We recommend the Office of Public Instruction prioritize and implement measures to assess and document risks and potential threats to information student data security on a regular basis.

We concur. In line with state policy, the OPI is following the NIST methodology for assessing the security risk. As risks are clarified, the OPI will institute mitigating actions. Progress has been delayed by the recent loss of the individual that prepared OPI's security plan.

Sincerely,

Denise Juneau
Superintendent of Public Instruction

Montana Code Annotated 2015

20-7-104. Transparency and public availability of public school performance data -- reporting -- availability for timely use to improve instruction. (1) The office of public instruction's statewide data system must, at a minimum:

(a) include data entry and intuitive reporting options that school districts can use to make timely decisions that improve instruction and impact student performance while creating a collaborative environment for parents, teachers, and students to work together in improving student performance. Options that the office of public instruction shall incorporate and make available for each school district must include data linkages to provide for automated conversion of data from systems already in use by school districts or by the office of public instruction that allow districts to collect, manage, and present local classroom assessment scores, grades, attendance, and other data to assist in instructional intervention alongside the existing school accountability and statewide student achievement results. The office of public instruction shall ensure that the design of the system is enhanced to prioritize collaborative support of each student's needs by classroom educators, administrators, and parents.

(b) display a publicly available educational data profile for each school district that protects each student's education records in compliance with the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, as amended, and its implementing regulations at 34 CFR, part 99.

(2) Subject to subsection (1)(b), each school district's educational profile must include, at a minimum, the following elements:

(a) school district contact information and links to district websites, when available;

(b) state criterion-referenced testing results;

(c) program and course offerings;

(d) student enrollment and demographics by grade level; and

(e) graduation rates.

(3) Each school district shall annually report to the office of public instruction and publish and post on the school district's internet website the following district data for the preceding school year:

(a) the number and type of employee positions, including administrators;

(b) for the current employee in each position:

(i) the total amount of compensation paid to the employee by the district. The total amount of compensation includes but is not limited to the employee's base wage or salary, overtime pay, and other income from school-sanctioned extracurricular activities, including coaching and similar activities; and

(ii) the certification held by and required of the employee;

(c) the student-teacher ratio by grade;

(d) (i) the amount, by category, spent by the district for operation and maintenance, stated in total cost and cost per square foot; and

(ii) the amount of principal and interest paid on bonds;

(e) the total district expenditures per student;

(f) the total budget for all funds;

(g) the total number of students enrolled and the average daily attendance;

(h) the total amount spent by the district on extracurricular activities and the total number of students that participated in extracurricular activities; and

(i) the number of students that entered the 9th grade in the school district but did not graduate from a high school in that district and for which the school district did not receive a transfer request. For reporting purposes, the students identified under this subsection (3)(i) are considered to have dropped out of school.

(4) Each school district shall also post on the school district's internet website a copy of every working agreement the district has with any organized labor organization and the district's costs, if any, associated with employee union representation, collective bargaining, and union grievance procedures and litigation resulting from union employee grievances.

(5) If a school district does not have an internet website, the school district shall publish the information required under subsections (2) and (3) in printed form and provide a copy of the information upon request at the cost incurred by the school district for printing only.

(6) The superintendent of public instruction shall continually work in consultation with the K-12 data task force provided for in 20-7-105 to analyze the best options for a statewide data system that will best enhance the ability of school districts to use data for the purposes identified in this section. Emphasis must be placed on developing or purchasing and customizing a statewide data system that promotes and preserves community ownership and local control and that incorporates innovative technologies available in the marketplace that may be in use and that are successfully working in other states. The office of public instruction and the K-12 data task force shall collaborate to enhance the statewide data system to support:

(a) the needs of school districts in using data to improve instruction and student performance;

(b) the collection of data from schools through a process that provides for automated conversion of data from systems already in use by school districts or the office of public instruction and that resolves the repetition of data entry and redundancy of data requested that has been characteristic of the data system in the past and that otherwise reduces the diversion of district staff time away from instruction and supervision;

(c) increased use of data from the centralized system by various functions within the office of public instruction; and

(d) transparency in reporting to schools, school districts, communities, and the public.

(7) The superintendent of public instruction shall gather, maintain, and distribute longitudinal, actionable data in the following areas:

(a) statewide student identifier;

(b) student-level enrollment data, including average daily attendance;

(c) student-level statewide assessment data;

(d) information on untested students;

(e) student-level graduation and dropout data;

(f) ability to match student-level K-12 and higher education data;

(g) a statewide data audit system;

(h) a system to track student achievement with a direct teacher-to-student match to help track, report, and create opportunities for improved individual student performance;

(i) student-level course completion data, including transcripts, to assess career and college readiness; and

(j) student-level ACT results, scholastic achievement test results, and advanced placement exam data.

(8) The superintendent of public instruction shall emphasize the creation of and distribution of individual diagnostic data for each student in a manner that is timely and protects the privacy rights of students and families as they relate to education so that school districts may use the data to support timely academic intervention as needed and to otherwise improve the academic achievement of the students of each school district.

(9) In addition to the data privacy protections in subsection (1)(b), the superintendent of public

instruction may provide personally identifiable information gathered, maintained, and distributed pursuant to subsection (7) and any other personally identifiable data only to the office of public instruction, the school district where the student is or has been enrolled, the parent, and the student. The superintendent of public instruction may not share, sell, or otherwise release personally identifiable information to any for-profit business, nonprofit organization, public-private partnership, governmental unit, or other entity unless the student's parent has provided written consent specifying the data to be released, the reason for the release, and the recipient to whom the data may be released.

(10) On or before June 30, 2013, the superintendent of public instruction shall begin presenting longitudinal data on academic achievement and shall develop plans for a measurement of growth for the statewide student assessment required by the board of public education.

History: En. Sec. 4, Ch. 418, L. 2011; amd. Sec. 4, Ch. 400, L. 2013.