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**.