

LEGISLATIVE AUDIT DIVISION

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



Deputy Legislative Auditors:
Cindy Jorgenson
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members
FROM: Angie Grove, Deputy Legislative Auditor
CC: Denise Juneau, Superintendent, Office of Public Instruction
Dennis Parman, Deputy Superintendent
DATE: October 2011
RE: Follow-up IS Audit (11SP-19): Achievement in Montana: Security of Student Information (09DP-10) Office of Public Instruction

Introduction

We presented our Information Systems audit on Achievement in Montana (AIM): Security of Student Information to the Legislative Audit Committee in February 2010. The report contains one recommendation relating to establishing procedures for district user account management in the State Edition of AIM.

We requested and received information from Office of Public Instruction (OPI) personnel regarding progress toward implementation of the report recommendation. This memorandum summarizes the offices' responses and our follow-up work.

Background

OPI implemented AIM to administer education information and support accountability at the local school districts and state level. The State Edition of AIM collects student data needed for OPI to meet state and federal reporting requirements. AIM is designed to track a wide variety of student data including enrollment and demographics information. Montana school districts collect and store information on students in accordance with federal regulations. There are also state requirements for data reporting, including calculation of average number belonging for school funding, registration for student assessment, and graduate and dropout rates. In AIM, local school district personnel enter each student's primary data just once. The data is then uploaded to the State Edition for reporting. A student's record contains the student's legal name, gender, birth date, race/ethnicity, and types of educational services received. Additional information includes scores on statewide assessments, dropout information, and information on students with disabilities.

Follow-up Discussion

The following sections summarize the report recommendation and the progress towards implementing the recommendation.

District User Access

According to the federal Family Educational Rights and Privacy Act, only authorized individuals with a legitimate educational interest should be allowed to view student data. During the audit, we noted district users have access to the State Edition of AIM via an account assigned to a district authorized representative. Practices for assignment of district accounts at the time of the audit did not include ongoing account management as suggested by industry standards. OPI has policies regarding acceptable use; however, these policies were not being followed. Users were sharing accounts, not updating passwords, and current account assignments were not up to date, resulting in a lack of individual accountability. As such, OPI could not ensure only appropriate individuals accessed student information in the State Edition of AIM. In addition, some district users indicated they were not aware of the need for conducting data confirmation activities. As a result, our findings indicated a need for improved district account management.

Recommendation #1

We recommend the Office of Public Instruction:

- A. Establish procedures to require unique accounts for all district users.
- B. Establish account management procedures to ensure district account user information is up-to-date and all users comply with applicable policies.
- C. Ensure district users receive appropriate training regarding security of student data and use of the system.

Implementation Status: Pending

According to OPI, in May 2010 they purchased the Oracle Identity and Access Management (OIAM) Suite. This suite was purchased to provide capabilities such as establishing unique accounts and the ability for authorized representatives to validate and confirm employee access. The software was also to provide for a Single Sign On ability. In March 2011 at the time of our initial follow-up request, OPI was still working on deploying the OIAM suite. For this reason, we chose to delay our follow-up until after their August 31, 2011, estimated completion date. However, OPI was unable to implement the Single Sign On capability. OPI reevaluated its initial decision and determined a different solution was needed to address its needs. As such, the OIAM suite was discontinued, and operations reverted back to original account management.

OPI is now in the process of evaluating identity management options for a separate data warehouse application. This identity management component (Forefront Identity Manager (FIM)) would then be deployed for AIM. The current estimation for deployment is June 30, 2012. According to OPI, FIM should be able to establish unique accounts for all district users as well as provide capabilities for authorized representatives of each district to validate and confirm district users and access levels. FIM will also be used to manage user accounts. Once the identity management system is deployed for AIM, OPI plans to update its confidentiality training. This training is required for all OPI employees, and promoted to school personnel and anyone else interested in understanding OPI's student records confidentiality policies and practices.