

# Secretary of State Audit Report

Jeanne P. Atkins, Secretary of State

Mary Wenger, Interim Director, Audits Division



---

## Oregon Department of Education: Computer Systems Ensure Integrity of Data, But Other Processes Need Improvement

---

### Executive Summary

The Oregon Department of Education (department) oversees the education of over 560,000 students in Oregon's public K-12 education system. The annual distribution of the State School Fund of \$3 billion and federal funding of about \$750 million help fund Oregon's public education.

The department's computer systems reasonably ensure the integrity of data used to distribute the State School Fund and appropriately process school district claims for federal funding. However, improvements are needed to provide better security for computer systems and student data, manage changes to computer systems, and ensure systems can be restored in the event of a disaster.

### Computer systems ensure integrity of student and school data

Department staff use the Consolidated Collection System to analyze and aggregate school and student data. They use information from this system to allocate monies to Oregon's schools and education service districts. Computer systems reasonably ensured the integrity of student and school information through automated processes that accurately identify students and detect potential data errors. In addition, department analysts use system information to validate student and school data.

### Computer systems appropriately receive and process school district claims for federal funding

The department uses the Electronic Grant Management System and the Federal Cash Ordering System to receive and process requests for federal program expenditure reimbursements. We found that computer controls reasonably ensure that these systems could appropriately receive and process school district claims for federal funding. These systems ensure

grant claims do not exceed available balances and reject claims that otherwise would be ineligible for reimbursement.

### **Security measures for computer systems were insufficient**

Although the department provides important protection measures for security, improvements are needed to better secure their computer systems and data. Weaknesses we identified relate to the department's processes for planning, configuring, managing, and monitoring information technology security components. As such, the department does not provide an appropriate layered defense to protect agency computer applications. Thus, confidential student level information is at increased risk of disclosure or compromise.

### **Management of changes to computer systems needs improvement**

The department has formal processes and tools for managing changes to their systems, but staff do not always fully utilize them. Independent and technical reviews of computer code changes did not always occur and processes were not in place to ensure only approved code could be placed in production. These weaknesses increase the risk that developers could introduce unauthorized or untested changes to the systems.

### **System files and data are appropriately backed up but procedures for timely restoration after a disaster are absent**

The department has processes in place to back up critical data and can restore individual files as needed. However, department management and staff have not fully developed and tested a comprehensive disaster recovery plan capable of restoring critical systems and data in the event of a disaster or major disruption. Without a disaster recovery plan, the department cannot ensure it can timely restore operations in the event of a disaster.

### **Recommendations**

We recommend that Department of Education management ensure resolution of identified security weaknesses, improve processes for changing computer code, and fully develop and test processes for restoring computer systems after a disaster.

### **Agency Response**

The full agency response can be found at the end of the report.

---

## Background

The Oregon Department of Education (department) functions under the control and operation of the Oregon State Board of Education, with the Superintendent of Public Instruction serving as the administrative officer. The mission of the department is to foster excellence for every learner through innovation, collaboration, leadership, and service to its education partners.

The Oregon Constitution directs the Legislature to “provide by law for the establishment of a uniform and general system of common schools.” The State Board of Education and the State Superintendent of Public Instruction are responsible for adopting rules for the general governance of public schools; implementing statewide standards for public schools; and making distributions from the State School Fund to districts that meet all legal requirements.

The department serves 197 school districts and 19 education service districts and oversees the education of over 560,000 students in Oregon’s public K-12 education system. The agency is also in charge of public preschool programs, the Oregon School for the Deaf, regional programs for children with disabilities, and education programs in Oregon youth correctional facilities.

### ***Department computer systems and processes***

To support its mission, the department uses various computer applications and maintains over 120 databases. The department currently hosts the majority of its computer servers, applications, and databases at Oregon State University’s data center.

Department staff use the Consolidated Collection System to control data inputs from school districts and other entities in order to populate over 70 databases. Information included in these databases often contain confidential student level data subject to requirements of the federal Family Educational Rights and Privacy Act (FERPA).

Consolidated Collection System data is critical because it supports the department’s key business processes. Department staff use information from this system to distribute the State School Fund and measure the efficacy of education programs through statistical analysis.

In addition, the department uses several other computer applications to manage payments that reimburse schools for federal program expenditures they incur. These applications include the Electronic Grant Management System, and the Federal Cash Ordering System.

Management of student data collections and storage is a dynamic process. As federal and state programs for education change, computer systems must be equally nimble to ensure stakeholders receive the information they need. In addition, because much of the information the department

handles is sensitive, the department must exercise great care to protect this information.

***Funding for education programs***

Money to support public education in grades K–12 comes from the state income taxes, Lottery funds, property taxes, and federal funding. Federal revenue sources include the Individuals with Disabilities Education Act, the National School Lunch Program, No Child Left Behind assessment funds, Child Care related funds, and various other education programs.

Allocations to school districts include transportation and general-purpose grants. The general-purpose grants follow a legislatively prescribed distribution formula based on number of students, with additional weighting reflecting specific education costs (e.g., poverty, special education, and remote schools), teacher experience, and local tax resources.

While distribution of the State School Fund totals approximately \$3 billion annually, the department also distributes over \$750 million of federal and state funding through the grant-in-aid programs for purposes such as child nutrition, special education, specialized education initiatives, professional development, and compensatory education.

---

## Audit Results

The purpose of this audit was to evaluate the effectiveness of Oregon Department of Education (department) controls over its information technology computing environment. Specifically, we evaluated the department's information technology processes, procedures and key computer applications. Based on the results of this work, we found that:

- Computer systems ensure integrity of student and school data.
- Computer systems appropriately receive and process school district claims for federal funding.
- Security measures for computer systems were insufficient.
- Management of changes to computer systems needs improvement.
- System files and data are appropriately backed up but procedures for timely restoration after a disaster are absent.

### **Computer systems ensure integrity of school and student data**

Calculating distributions from the State School Fund requires the department to collect statistical information from schools and school districts regarding student enrollment and other metrics as prescribed in law. Department staff use this information to allocate the State School Fund to the individual schools, districts, and education service districts located throughout Oregon. Federal agencies also require the department to capture, aggregate and regularly report certain student data in order to qualify for federal program funding.

Department staff use the Consolidated Collection System (CCS) to analyze and aggregate school and student data. This system relies on Microsoft Access and other databases. In addition, staff use Microsoft Excel spreadsheets to calculate individual payments they make to schools and districts. Processes department staff use to ensure CCS accurately measures the effectiveness of education programs and equitably distributes the State School Fund include:

- Electronic edits ensure that each student has a unique identification number and can only be counted once. If a student is reported by more than one institution, funding for that student is suspended until staff resolve the difference.
- System controls alert staff when data may contain errors or when data may have been inappropriately uploaded into the system. These processes also identify inputs that do not appear reasonable according to prior entries, allowing staff to verify and approve these amounts.
- System processes ensure publically viewed data does not include detail that could be attributable to individual students.

- Analysts use computer logic to independently validate student and school data. They then communicate these results to schools and school districts through a web portal to allow them to again verify the data.
- Logical access controls ensure that only users with a business need have access to systems.
- The system automatically logs changes users make to data.

We evaluated these controls and found they were functioning as intended. Based on this work, we concluded that system controls reasonably ensure the integrity of student and school data the department uses to distribute the State School Fund.

### **Computer systems appropriately receive and process school district claims for federal funding**

The department is responsible for managing school districts' federal grant claims. This task includes ensuring school districts' claims for federal reimbursements comply with specified grant requirements. The department assigns staff to monitor school districts' compliance with federal requirements for reimbursement. These grant managers rely on computer systems to provide the data they need to carry out their duties.

The department's Electronic Grant Management System (EGMS) is a web-based computer application school districts and educational service districts use to report their expenditures to the department for reimbursement. In addition, staff use the Cash Ordering System (COS) to obtain federal reimbursements for qualifying expenditures. These computer systems have electronic and manual processes to ensure proper reimbursements of federal grants, including:

- system edits to prevent grant claims from exceeding the available balance of the grants;
- processes to ensure all approved reimbursement claims are transferred to the COS;
- electronic processes to stop claims that are no longer eligible for reimbursement;
- controls to ensure reimbursement claims entered into EGMS are not paid twice by the COS; and
- logical access controls to ensure claims are only entered by authorized personnel.

We evaluated these controls and found they provided reasonable assurance that department systems could appropriately receive and process school district claims for federal funding.

## **Security measures for computer systems were insufficient**

In September 2016, Governor Kate Brown issued Executive Order 16-13 (directive) outlining a process to unify IT security functions to protect and secure information entrusted to the State of Oregon. The directive instructs state agencies to consolidate security functions and staffing into the Office of the State Chief Information Officer (OSCIO). In addition, it directs agencies to work with this new security group to develop and implement security plans, rules, policies, and standards adopted by the state Chief Information Officer.

Proper security requires the coordinated use of multiple security components to protect the integrity of computer systems and their data. The security industry refers to this methodology as defense in depth. The underlying principle is that it is more difficult to defeat a complex and multi-layered defense system than to penetrate a single barrier.

Department management has provided important protection measures for security, but improvements are needed to better secure their computer systems and data. Weaknesses we identified relate to the department's processes for planning, configuring, managing, and monitoring information technology security components.

Based on our evaluation, the department has not provided an appropriate layered defense to protect agency computer applications and data against internal and external threats. As a result, confidential student level information is at increased risk of unauthorized disclosure or compromise.

This is particularly noteworthy given federal requirements for protecting student data and the criticality of department information systems used to fund Oregon public schools. In addition, it is not yet clear how implementation of the Executive Order will impact the department's ability to timely resolve identified security weaknesses.

Because of the sensitive nature of IT security we communicated the details of weaknesses we identified in a confidential letter according to ORS 192.501 (23).

## **Management of changes to computer systems needs improvement**

Computer program code should be managed to ensure only tested and approved modifications are placed into production. To ensure this occurs, changes to computer code should be closely monitored, approved, and compared to the previously authorized versions.

Department management has established formal administrative procedures for approving proposed changes to their systems. Their Change

Review Board evaluates proposed changes to identify potential conflicts. After this initial review and approval, the department's technical team lead assigns staff to change the code.

The department has formal procedures and tools for developing, testing, and moving approved computer code changes into production. These procedures include limiting access to computer code, providing quality assurance testing and approval, and using automated version control tools. When followed, these processes provide adequate control over computer program changes.

However, department staff do not always follow established procedures or utilize available tools. Specifically, developers did not always perform independent reviews of computer code changes, perform code comparisons, or ensure only approved code could be placed in production.

In addition, important tools the department utilizes to limit developers' access to computer code or provide robust version control are not compatible with application code developed using Microsoft's Access Data Project (ADP). Department staff use this tool to maintain EGMS and COS. Therefore, these computer system cannot receive the benefit of important program change management tools.

Collectively, these weaknesses increase the risk that developers could introduce unauthorized or untested changes to the system. Should this occur, the department could experience delays in receiving and processing grant claims or incur disruptions to the distribution of the State School Fund.

### **System files and data are appropriately backed up but procedures for timely restoration after a disaster are absent**

Restoring operations after a disaster or other serious disruption requires significant advance planning and coordination. Generally accepted standards for information technology indicate that organizations should mitigate the risks associated with serious service disruptions by developing and testing disaster recovery plans. These plans should be based on agreed-upon requirements, and should be regularly updated to reflect changes to the computing environment.

The department has processes in place to back up critical data and can restore individual files as needed. However, management and staff have not fully developed and tested a comprehensive disaster recovery plan capable of timely restoring critical systems and data in the event of a disaster or major disruption.

Specifically, department staff have not clearly identified or defined critical recovery roles, responsibilities, or necessary infrastructure and configurations. In addition, they have not categorized and labeled

information assets or prioritized their order for restoration. Department staff also have not identified how quickly systems need to be restored.

Without these steps, the department cannot ensure it can timely restore operations and risks loss of educational data and delays in making monthly payments to schools from the State School Fund.

---

## Recommendations

We recommend that Department of Education management:

- Work with OSCIO management and staff to fully and timely resolve the security weaknesses we identified in our confidential management letter.
- Ensure independent reviews of all computer code changes are performed, including code comparisons, and establish procedures to ensure only approved computer code will be promoted to production.
- Fully develop and test a comprehensive disaster recovery plan for timely restoration of critical systems and data in the event of a disaster. This plan should clearly identify critical recovery roles, responsibilities, resources needed, and priorities for timely restoring systems.

---

## Objectives, Scope and Methodology

The purpose of our audit was to review and evaluate the effectiveness of key general and application controls over the computing environment at the Oregon Department of Education (Department). Our specific objectives were to determine whether information system controls governing the department's core applications provide reasonable assurance that:

- Inputs into the Consolidated Collection System remain complete, accurate, and electronic processes used to distribute the State School Fund are appropriately controlled.
- Transactions processed through the department's information systems reasonably ensure federal expenditures and revenues are complete and valid.
- The department's information systems are protected against unauthorized use, disclosure, modification, damage or loss.
- Changes to computer code are managed to ensure integrity of electronic systems and data.
- System files and data are appropriately backed up and can be timely restored.

The scope of our audit included the Electronic Grant Management System, the Federal Cash Ordering System, the Consolidated Collection System, and processes for State School Fund distribution. We evaluated controls for information system security, change management, and backup and recovery controls that were in effect during our audit, ending in October 2016.

We conducted interviews with department personnel, observed operations and procedures, and examined available computer system and security documentation. To fulfill our audit objectives, we evaluated processes for:

- receiving grant claims and requesting reimbursement for federal expenditures;
- collecting and reporting on statistical information from educational institutions;
- calculating and distributing the State School Fund;
- providing logical access to computer systems; and
- providing system and data backup and restoration.

We used the IT Governance Institute's publication "Control Objectives for Information and Related Technologies" (COBIT), and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM) to identify generally accepted control objectives and practices for information systems.

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 objective. We believe that the evidence obtained and reported provides a reasonable basis to achieve our audit objective.

Auditors from our office, who were not involved with the audit, reviewed our report for accuracy, checking facts and conclusions against our supporting evidence.



# Oregon Department of Education

Kate Brown, Governor

Office of the Deputy Superintendent  
255 Capitol St NE, Salem, OR 97310  
Voice: 503-947-5600  
Fax: 503-378-5156

December 6, 2016

Neal Weatherspoon  
Information Technology Audit Manager  
Audits Division, Office of the Secretary of State  
Public Service Building, Suite 500  
255 Capitol Street NE  
Salem, OR 97310

Dear Neal:

Thank you for the opportunity to respond to the December 8, 2016 audit of the Oregon Department of Education (ODE)'s computer systems. We consider the audit a very important review and safeguard to enhance the protection and management of ODE's computer systems. ODE is committed to protecting the data housed in our computer systems and takes all feedback and recommendations very seriously. ODE's response to the Oregon Secretary of State Audits Division (OAD) recommendation is outlined in this letter. We generally agree with OAD's recommendation for each specific finding; our associated responses follow.

**OAD Recommendation:**

We recommend that Department of Education management ensure resolution of identified security weaknesses, improve processes for changing computer code, and fully develop and test processes for restoring computer systems after a disaster.

**ODE response:**

**Management agrees with the recommendation. ODE has a demonstrated history of protecting the computer systems managed by the agency through supporting continuous improvement of the agency's computer systems and information security. Information systems evolve and change over time, as do the threats to those systems, and ODE continues to evolve the agency's information technology strategic and operational plans and information security strategy to meet those challenges.**

**OAD Finding:** Security measures for computer systems were insufficient.

**ODE Response:** ODE has a long history of practicing a defense-in-depth approach to information security and to protecting the agency's computing systems and resources. ODE has several efforts underway to address identified security weaknesses. Over the past year, ODE has completed a number of security projects that further enhance the agency's security stance. As of the release of this audit, ODE is reviewing the 2016 security plan and updating it for 2017 using the agency's participation in external audits and risk assessments to inform decision making and security project planning for 2017.

**OAD Finding:** Management of changes to computer systems needs improvement.

**ODE Response:** ODE has very strong control processes for changing computer code on the vast majority of our computing systems. OAD's concerns are specific to legacy systems that ODE is currently maintaining and has plans to upgrade, migrate or replace in the next biennium. The elimination of legacy systems will result in ODE comprehensively managing computer code changes across the agency's computing environment.

**OAD Finding:** System files and data are appropriately backed up but procedures for timely restoration after a disaster are absent.

**ODE Response:** ODE will fully develop and test processes for restoring computer systems after a disaster. While ODE is confident that the agency's data are protected and can be restored in the event of an emergency, the agency recognizes a need for a detailed and tested disaster recovery plan. ODE has already scheduled a project for developing and testing disaster recovery plans and processes in early 2017 with the expectation that this plan will be completed and tested by December 2017.

The Oregon Department of Education would like to thank the Oregon Secretary of State's Office, Audits Division for the opportunity to respond to this audit. We take these findings and recommendations very seriously. The findings align with the ongoing work ODE has been doing to continuously maintain and expand on our information security stance and computer systems management.

We appreciate your team's hard work and effort over the last year to identify concerns and highlight opportunities to strengthen ODE's computing system environment. Since the team completed its fieldwork in October 2016, we have moved forward with implementing its recommendations and will continue to progress as described above.

If you have any questions about this response, please contact Susie Strangfield, ODE Chief Information Officer at [susie.strangfield@ode.state.or.us](mailto:susie.strangfield@ode.state.or.us).

Thank you for the recommendations and the insights and feedback your audit has afforded us.

Sincerely,



Salam A. Noor, Ph.D.  
Deputy Superintendent of Public Instruction

---

## About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division is authorized to audit all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

---

### **Audit Team**

William Garber, CGFM, MPA, Deputy Director

Neal Weatherspoon, CPA, CISA, CISSP, Audit Manager

Matthew Owens, CISA, MBA, Senior Auditor

Sherry Kurk, Staff Auditor

---

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:

website: [sos.oregon.gov/audits](https://sos.oregon.gov/audits)

phone: 503-986-2255

mail: Oregon Audits Division  
255 Capitol Street NE, Suite 500  
Salem, Oregon 97310

The courtesies and cooperation extended by officials and employees of the Oregon Department of Education during the course of this audit were commendable and sincerely appreciated.