MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

SELECTED PAYMENT AND RELATED SYSTEMS

MICHIGAN DEPARTMENT OF EDUCATION AND
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

November 2008

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

313-0590-08

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Report Number:
313-0590-08

Selected Payment and Related Systems

Michigan Department of Education (MDE) and
Michigan Department of Information Technology (MDIT)

Released:
November 2008

MDE distributed $14.3 billion in federal and State grant payments in fiscal year 2006-07 through SAMS, MEGS, CMS, CNAP, and FNS-FRS. MDIT provides information system support services to these systems and the Michigan Education Information System (MEIS), including operating system configuration, database administration, and physical security. MDIT also provides application development and maintenance for SAMS and MEIS. Application project management, development, and maintenance are provided by contracted developers for MEGS, CMS, CNAP, and FNS-FRS.

Audit Objective:
To assess the effectiveness of MDE and MDIT's security and access controls over the selected information systems.

Audit Conclusion:
MDE and MDIT's security and access controls over the selected information systems were not effective. We noted two material conditions (Findings 1 and 2) and one reportable condition (Finding 3).

Material Conditions:
MDE had not established a comprehensive information systems security program and effective access controls over MDE information systems (Finding 1).

MDIT and MDE had not fully established security controls over the State Aid Management System (SAMS), Michigan Electronic Grants System (MEGS), Cash Management System (CMS), Child Nutrition Application Program (CNAP), and Food Nutrition System - Fiscal Reporting System (FNS-FRS) databases (Finding 2).

Reportable Condition:
MDIT had not established effective security controls over the server operating systems (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of system controls to ensure the integrity of data maintained by MDE and MDIT for use in the selected information systems.

Audit Conclusion:
MDE and MDIT were moderately effective in their efforts to ensure the integrity of data maintained by MDE and MDIT for use in the selected information systems. We noted one material condition (Finding 4) and three reportable conditions (Findings 5 through 7).

Material Condition:
MDE and MDIT had not developed a comprehensive change control process for SAMS, MEGS, CMS, CNAP, and FNS-FRS (Finding 4).

Reportable Conditions:
MDE did not fully ensure the completeness and accuracy of SAMS, MEGS, CMS, and CNAP data (Finding 5).

MDE and MDIT had not established complete backup and recovery controls (Finding 6).

MDE did not fully develop and monitor audit trails for SAMS, MEGS, and CMS (Finding 7).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of MDE and MDIT's efforts to ensure that the selected information systems accurately calculate federal and State payments.

Audit Conclusion:
MDE and MDIT were moderately effective in their efforts to ensure that the selected information systems accurately calculated federal and State payments. We noted one material condition (Finding 8) and four reportable conditions (Findings 9 through 12).

Material Condition:
MDE did not ensure the accurate processing of MEGS and CMS grant transactions (Finding 8).

Reportable Conditions:
MDE did not implement system controls to ensure the accurate calculation of education finance incentive grant Title I payments for the No Child Left Behind Act of 2001 (Finding 9).

MDE did not implement separate user roles for processing State aid payments in SAMS (Finding 10).

MDE and MDIT did not ensure that the vendor provided complete system documentation for MEGS and CMS as required by the vendor's contract (Finding 11).

MDE did not fully establish processing controls over meal claims calculated by FNS-FRS (Finding 12).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 12 findings and 12 corresponding recommendations. MDE's and MDIT's preliminary responses indicated that MDE and MDIT generally agree with 11 recommendations and disagree with 1.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

November 7, 2008

Mr. Michael P. Flanagan
Superintendent of Public Instruction
Michigan Department of Education
John A. Hannah Building
Lansing, Michigan
and
Mr. Kenneth D. Theis, Director
Michigan Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Flanagan and Mr. Theis:

This is our report on the performance audit of Selected Payment and Related Systems, Michigan Department of Education and Michigan Department of Information Technology. This report contains our report summary; description of agencies and systems; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

SELECTED PAYMENT AND RELATED SYSTEMS
MICHIGAN DEPARTMENT OF EDUCATION AND
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

GLOSSARY

Michigan Department of Education (MDE)

The mission* of MDE is to provide leadership and support for excellence and equity in education. MDE's Office of State Aid and School Finance is responsible for administering and distributing the State School Aid Act. MDE's Office of Grants Coordination and School Support and the MDE program offices aid in distributing grant funds provided by the U.S. Department of Education and are responsible for grant budgets, grant applications, and grant approvals. MDE's Office of Financial Management is responsible for MDE's accounting activities, including the cash disbursement of grant funds. MDE maintains and operates information systems critical to the processing of federal and State payments. MDE distributed $14.3 billion in federal and State grant payments in fiscal year 2006-07 through the following information systems:

1. State Aid Management System (SAMS)

   SAMS is an automated system used by the Office of State Aid and School Finance to calculate State school aid payments for distribution to the State's school districts and charter school recipients*. Funds are allocated to each recipient based on statutory formulas. The payments include a foundation allowance and funding for categorical programs, which are special program grants designated in the State School Aid Act of 1979. Examples of categorical programs include at-risk pupils, special education, vocational education, and adult education.

   SAMS obtains data for calculating State school aid payments from the Single Record Student Database (SRSD), the Taxable Value System, and the School Code Master. SRSD provides SAMS with pupil counts, and the Taxable Value System provides SAMS with aggregate nonhomestead property tax values by district. In fiscal year 2006-07, SAMS processed $12.7 billion in payments. MDE and MDIT are rewriting SAMS to replace the current SAMS. MDE and MDIT plan to implement the new system by 2009.

2. Michigan Electronic Grants System (MEGS)

   MEGS is an automated Web-based grant application system used to create, submit, approve, track, and amend grant applications. All school districts, local

** See glossary at end of report for definition.*

educational agencies, charter schools, and other education-related agencies use MEGS to apply for their federal formula grants and the majority of the MDE-sponsored competitive grants. MEGS manages the allocation of over 50 federally funded and State-funded grants. Some grant allocations are based on formulas calculated outside of MEGS and uploaded into MEGS. MEGS has approximately 10,400 users, including MDE staff, school districts, charter schools, colleges and universities, State agencies, and childcare centers. MEGS shares data with the Cash Management System, where grant payments are calculated and processed. MEGS was implemented in 2001.

3. Cash Management System (CMS)

CMS is an automated Web-based information system used to input, process, monitor, and control grant cash disbursements to recipients, including school districts, colleges and universities, day-care home sponsors, and summer camps. CMS processed $1.3 billion in recipient payments from MEGS from October 2006 through April 2008. CMS is used by recipients to request funds and submit expenditure reports. MDE uses CMS to calculate and monitor grant payments to recipients. MEGS and CMS are integrated and share data.

CMS replaced the Grants Cash Management Reporting System. CMS began processing some grant payments in fiscal year 2006-07. CMS was fully implemented and processed all grant payments beginning in April 2008. CMS has approximately 12,600 users, including MDE staff, school districts, charter schools, colleges and universities, and State agencies.

4. Child Nutrition Application Program (CNAP)

CNAP is an automated Web-based system used to apply for or renew participation in the School Meals Program, Child and Adult Care Food Program, Summer Food Service Program, and Summer Camp Special Milk Program. Participants enter application information, such as the type of meals served and facility locations, directly into CNAP using the Internet. The applications are approved and certified in CNAP by authorized MDE staff. Data from the applications is used to create claim forms used by the Food Nutrition System - Fiscal Reporting System for CNAP payment calculations. CNAP has approximately 2,900 users, including MDE staff, school districts, childcare centers, day-care home sponsors, residential childcare facilities, and summer camps and summer food service sponsors.

5. Food Nutrition System - Fiscal Reporting System (FNS-FRS)

FNS-FRS consists of 8 subsystems, including five claim collection systems, two data collection systems, and one batch payment processing system for the School Meals Program, Child and Adult Care Food Program, Summer Food Service Program, and Summer Camp Special Milk Program. In fiscal year 2006-07, FNS-FRS processed $309 million in payments. The School Meals Year End Report System collects information entered by participants of the School Meals Program and provides it to the School Aid Unit for the calculation of the State breakfast and lunch payment. The Local Education Review System provides verification information of free and reduced meals to the U.S. Department of Agriculture (USDA). Claim forms are generated in each of the five claim collection systems from application data that was entered through CNAP by participants. Each month, participants enter the number of meals served into the on-line claim forms. The batch payment processing system uses data from the claim forms to calculate meal reimbursement amounts based on USDA per meal rates for payments to participants. As of April 2008, payments were made through the Grants Cash Management Reporting System. However, MDE plans to pay all reimbursements through CMS in fiscal year 2008-09. There are approximately 2,800 system users, including MDE staff, school districts, childcare centers, day-care home sponsors, residential childcare facilities, and summer camps and summer food service sponsors.

Michigan Education Information System (MEIS)

MEIS is the user authentication system for all MDE systems available on the Internet. MEIS provides an initial layer of security. All users with access to MDE systems have a unique MEIS account. After authentication to MEIS, users log into MEGS, CMS, CNAP, and FNS-FRS with another user account that provides an additional layer of security. MEIS was developed in 1996.

Michigan Department of Information Technology (MDIT)

MDIT Technical Services provides information system support services to SAMS, MEGS, CMS, CNAP, FNS-FRS, and MEIS, including operating system configuration, database administration, and physical security. MDIT Technical Services also provides application development and maintenance for SAMS and MEIS. Application project management, development, and maintenance are provided by contracted developers for MEGS, CMS, CNAP, and FNS-FRS.

Audit Objectives

Our performance audit* of Selected Payment and Related Systems, Michigan Department of Education (MDE) and Michigan Department of Information Technology (MDIT), had the following objectives:

1. To assess the effectiveness* of MDE and MDIT's security and access controls over the selected information systems.

2. To assess the effectiveness of system controls to ensure the integrity* of data maintained by MDE and MDIT for use in the selected information systems.

3. To assess the effectiveness of MDE and MDIT's efforts to ensure that the selected information systems accurately calculate federal and State payments.

Audit Scope

Our audit scope was to examine the information processing and other records of selected Michigan Department of Education information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances. Our audit procedures, conducted from August 2007 through April 2008, generally covered the period October 1, 2005 through April 30, 2008.

Audit Methodology

To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified MDE's information systems and performed a risk assessment* of selected systems to determine those with a high risk to MDE's operations. We used the results of our preliminary review to determine the extent of our detailed

** See glossary at end of report for definition.*

analysis and testing. We identified MDE's systems related to federal and State payments that are essential to MDE's operations.

2. Detailed Analysis and Testing Phase

We performed an assessment of general and application controls over selected information systems:

a. Security and Access Controls:

(1) We examined and tested user identification and password controls over the State Aid Management System (SAMS), Michigan Electronic Grants System (MEGS), Cash Management System (CMS), Child Nutrition Application Program (CNAP), and Food Nutrition System - Fiscal Reporting System (FNS-FRS).

(2) We examined and tested user access permissions for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

(3) We reviewed and assessed the oversight of security for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

(4) We reviewed and assessed data and database management controls for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

(5) We reviewed and assessed controls over operating system security configuration and operating system security management for SAMS, MEGS, CMS, CNAP, FNS-FRS, and the Michigan Education Information System (MEIS).

b. System Controls to Ensure Data Integrity:

(1) We analyzed selected data fields within SAMS, MEGS, CMS, CNAP, and FNS-FRS to determine their accuracy and completeness.

(2) We reviewed policies and procedures for managing program and data changes for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

(3) We examined and tested the effectiveness of controls to ensure that only tested and authorized changes are placed into production for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

(4) We interviewed MDIT staff to obtain an understanding of backup and recovery controls over MDE's information systems.

(5) We reviewed and evaluated MDIT's access to backup files.

(6) We reviewed and evaluated disaster recovery and business continuity plans for MDE.

c. Accuracy of Payment Calculations:

(1) We reviewed and evaluated MDE's controls over the calculations of federal and State payments.

(2) We evaluated and tested input, processing, and output controls for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

Agency Responses

Our audit report contains 12 findings and 12 corresponding recommendations. MDE's and MDIT's preliminary responses indicated that MDE and MDIT generally agree with 11 recommendations and disagree with 1.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require MDE and MDIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

SECURITY AND ACCESS CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of the Michigan Department of Education (MDE) and the Michigan Department of Information Technology's (MDIT's) security and access controls over the selected information systems.

Audit Conclusion: MDE and MDIT's security and access controls over the selected information systems were not effective. Our assessment disclosed two material conditions*. MDE had not established a comprehensive information systems security program and effective access controls over MDE information systems (Finding 1). Also, MDIT and MDE had not fully established security controls over the State Aid Management System (SAMS), Michigan Electronic Grants System (MEGS), Cash Management System (CMS), Child Nutrition Application Program (CNAP), and Food and Nutrition System - Fiscal Reporting System (FNS-FRS) databases (Finding 2). Our assessment also disclosed one reportable condition* related to operating system security (Finding 3).

FINDING

1. Security Program and Access Controls

   MDE had not established a comprehensive information systems security program and effective access controls over MDE information systems. The lack of a security program and effective access controls could result in unauthorized access and changes to data and unauthorized payments occurring and going undetected.

   In Special Publication 800-53, the National Institute of Standards and Technology* (NIST) recommends that security controls be employed as a part of a well-defined information systems security program. A comprehensive security program should define and implement effective policies and procedures for granting access to payment data and data systems. The MDE security officer has not established policies and operating procedures for accessing and safeguarding MDE data. Our

** See glossary at end of report for definition.*

review of system access controls over SAMS, MEGS, CMS, CNAP, and FNS-FRS disclosed the following weaknesses:

a. MDE did not restrict development staff from privileged access* to MDE's production data. Individuals with privileged access have the ability to bypass database and application security controls. We noted that five SAMS developers could change historical information as well as calculate and issue State aid payments in SAMS. Also, two MDIT developers and 18 contracted developers were granted privileged access to MEGS and CMS; two contracted developers were granted privileged access to CNAP; and one MDIT developer and two contracted developers were granted privileged access to FNS-FRS.

b. MDE did not restrict MDE users' access to ensure a separation of duties. We noted:

   (1) The MEGS and CMS project manager used multiple accounts to bypass controls and to initiate and approve the amount grant recipients were eligible to receive. In addition, 16 MEGS and CMS users each had multiple accounts.

   (2) The director and assistant director of the State Aid Unit (SAU) had the ability to both change and approve State aid allocation amounts to schools using SAMS. These duties should be separated between two individuals.

   To detect errors and prevent fraud, user accounts should be assigned so that the same person cannot initiate and approve transactions.

c. MDE did not prevent users from logging on as another user and making changes to MEGS and CMS data. MDE informed us that it established a read-only help desk user account for providing assistance to users by allowing MDE staff to log on as those users. However, we determined that the help desk user account was not read-only and allowed MDE staff to change data.

** See glossary at end of report for definition.*

d. MDE had not established formal documented policies and procedures for assigning and authorizing access to data. As a result, MDE could not ensure that all user access was appropriate. We noted:

(1) MDE did not ensure that only security administrators granted user access to MEGS and CMS. We noted that the contracted project manager and developers granted MEGS and CMS access to seven contracted individuals who did not require access.

(2) MDE did not ensure that school district staff who requested user access to MEGS, CMS, CNAP, and FNS-FRS had the authority to do so. MDE should maintain a list of valid approvers to ensure that requests for access to MEGS, CMS, CNAP, and FNS-FRS were authorized by appropriate personnel.

(3) MDE did not define and document the system access that is appropriate for State employee users of MEGS and CMS based on their job duties. In addition, MDE did not establish written policies on how to assign access to MEGS, CMS, and CNAP based on a user's needs.

(4) MDE did not require security agreements for any State employees who used SAMS, MEGS, CNAP, and FNS-FRS. Signed security agreements ensure that users agree to the conditions of access and have been properly approved for access.

(5) MDE did not obtain security agreements for all grant recipients that use the system to certify* grants. We reviewed a sample of 86 users with access to MEGS, CMS, CNAP, and FNS-FRS. We noted that MDE did not have a signed security agreement for 1 (5%) of 19 MEGS users, 8 (23%) of 35 CMS users, 1 (6%) of 18 CNAP users, and 1 (7%) of 14 FNS-FRS users.

(6) MDE did not properly approve the granting of recipient access to systems. We noted that 3 (16%) of 19 security agreements for MEGS,

** See glossary at end of report for definition.*

1 (3%) of 35 security agreements for CMS, and 3 (21%) of 14 security agreements for FNS-FRS were approved by the person requesting access.

e. MDE did not have an effective process to monitor and remove user access. We noted:

(1) MDE had not developed reports or monitoring tools to ensure that high-risk users were not performing unauthorized activities. We noted 304 users that could perform one or more of the following high-risk activities: create and update user accounts, enter recipient and grant information, approve grant applications, approve amounts made available to recipients, and process payments.

(2) MDE did not have a process to disable user accounts of users who no longer required access. We noted:

(a) In our selection of users from seven school districts and three nonprofit organizations with access to MEGS, CMS, and CNAP, 10 (31%) of 32 users were no longer employed by the school district or organization.

(b) In our review of users with access to SAMS, 1 former contracted developer was no longer under contract with MDE and 1 (13%) of 8 MDE users no longer worked in SAU.

f. MDE did not remove user accounts created for testing data. We noted seven test accounts for MEGS and CMS and two test accounts for CNAP that could change production data. Removing test accounts helps protect production data from unauthorized modification or use.

g. MDE did not prevent privileged users from renaming user accounts. Transactions are recorded in the system by user account. The historical record of who processed a transaction is not accurate if the name on the user account is changed. We identified a privileged user account in which the name on the account was changed from a former contractor to a current employee. Keeping the same name on user accounts would help ensure user accountability.

h. MDE did not lock out usercodes after a reasonable number of invalid sign-on attempts for SAMS, MEGS, CMS, CNAP, and FNS-FRS. Locking out usercodes helps prevent an individual from gaining unauthorized access to an information system.

i. MDE did not disconnect users or use password-protected screen savers after a reasonable period of system inactivity for SAMS and CNAP. This could result in unauthorized system access if a user leaves a work station unattended. ISO/IEC 17799:2005* states that systems should shut down after a period of inactivity that reflects the risk to the security of the data.

j. MDE did not implement strong password controls for SAMS. Control Objectives for Information and Related Technology* (COBIT) requires effective password controls to validate a user's authority to access data.

RECOMMENDATION

We recommend that MDE establish a comprehensive information systems security program and effective access controls over MDE information systems.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that it will work with MDIT to establish a comprehensive security program that will cover all MDE information technology systems.

FINDING

2. Database Security

MDIT and MDE had not fully established security controls over the SAMS, MEGS, CMS, CNAP, and FNS-FRS databases. As a result, MDIT and MDE are unable to prevent or detect inappropriate access to MDE's payment data.

ISO/IEC 17799:2005 states that a database with appropriate security controls provides a protected environment to ensure the integrity and confidentiality of data. Appropriate security controls include using individual user identification (ID) and

** See glossary at end of report for definition.*

passwords, monitoring procedures to ensure that users are performing only activities they have been explicitly authorized to perform, and using audit logs to help identify significant events for security monitoring purposes. Our review of the five databases disclosed:

a. MDIT and MDE did not restrict users' access to SAMS database tables. We noted that 13 users could access the SAMS database without entering a username and password.

b. MDE did not encrypt sensitive data in SAMS. As a result, MDE could not ensure that sensitive data, such as bank account numbers, was protected from unauthorized disclosure. System tables with sensitive data could be viewed by anyone with access to SAMS.

c. MDIT did not monitor the activity of privileged user accounts on any of the five databases. Privileged users, such as database administrators, have access capabilities that allow them to make changes to database triggers, stored procedures, and database configurations. However, MDIT did not create reports or queries to monitor these activities.

d. MDIT and MDE did not maintain and review automated audit logs of failed login attempts or other high-risk events on any of the five databases. MDIT informed us that continuously running audit logs on its databases could impact performance. However, the recording and monitoring of selected high-risk events would enhance database security.

e. MDIT did not remove or disable unnecessary stored procedures for the MEGS, CMS, CNAP, and FNS-FRS databases. Stored procedures are short programs that can be shared by several databases to provide efficiency for common actions, such as controlling access. We noted that MDIT did not remove 48 (96%) of 50 stored procedures that the Center for Internet Security recommends be removed.

f. MDIT and MDE did not develop data dictionaries for any of the five databases. A data dictionary contains detailed information about data, which is critical in minimizing data redundancy and maintaining data integrity. Therefore, MDIT

and MDE could not ensure that they minimized data redundancy and maintained data integrity.

RECOMMENDATION

We recommend that MDIT and MDE fully establish security controls over the SAMS, MEGS, CMS, CNAP, and FNS-FRS databases.

AGENCY PRELIMINARY RESPONSE

MDE and MDIT agree and informed us that MDE will work with MDIT to establish security controls for all systems named in this audit. MDE and MDIT informed us that a project plan to implement the security controls will be developed by December 31, 2008 and the SAMS redevelopment project in progress will fix the database access findings related to SAMS. MDE and MDIT also informed us that they will establish mechanisms to monitor privileged user activity, maintain audit logs, disable unnecessary stored procedures, and create data dictionaries for the other systems specified in the finding. In addition, MDE and MDIT informed us that the new SAMS system is scheduled for parallel implementation with the existing SAMS system by fall 2009.

FINDING

3. Operating System Security

MDIT had not established effective security controls over the server operating systems*. As a result, MDE could not ensure that data was protected from unauthorized modification, loss, or disclosure.

A well-secured operating system helps provide a stable environment on which to run MDE's information systems. MDIT procedure 1350.11, Security Operational Guidelines for Servers, requires the secure establishment, maintenance, and administration of servers, including operating system software, and the data residing on the servers. Operating system security controls should be established to protect information and resources from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. In addition, the Carnegie Mellon Software Engineering Institute states that an operating system

** See glossary at end of report for definition.*

should be installed with a minimal service configuration to reduce the risk of network intrusion and exploitation of well-known operating system vulnerabilities.

Our review of six servers that contain the databases and four Web servers for MEGS, CMS, CNAP, FNS-FRS, and the Michigan Education Information System identified vulnerable operating system configurations. Due to the confidentiality of operating system configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to MDIT.

RECOMMENDATION

We recommend that MDIT establish effective security controls over the server operating systems.

AGENCY PRELIMINARY RESPONSE

MDE and MDIT agree and informed us that MDIT will strengthen security controls over the server operating systems. MDE and MDIT informed us that all servers associated with this audit are scheduled to be replaced and are in the purchasing process at this time. Also, MDE and MDIT informed us that all accounts identified in the audit as unnecessary have been disabled or removed.

In addition, MDIT informed us that all new servers will be compliant in fiscal year 2008-09 with Server Configuration Standards policy based on State of Michigan security policies and industry best practices. Further, MDIT informed us that, as of July 9, 2008, the local settings for the audit policies have been set to the State of Michigan server policies. In addition, MDIT informed us that it will work with MDE to strengthen security controls over the server operating systems by December 31, 2009.

SYSTEM CONTROLS TO ENSURE DATA INTEGRITY

COMMENT

Audit Objective: To assess the effectiveness of system controls to ensure the integrity of data maintained by MDE and MDIT for use in the selected information systems.

Audit Conclusion: MDE and MDIT were moderately effective in their efforts to ensure the integrity of data maintained by MDE and MDIT for use in the selected information systems. Our assessment disclosed one material condition. MDE and MDIT had not developed a comprehensive change control process for SAMS, MEGS, CMS, CNAP, and FNS-FRS (Finding 4). Our assessment also disclosed three reportable conditions related to SAMS, MEGS, CMS, and CNAP data integrity; disaster recovery; and audit trails (Findings 5 through 7).

FINDING

4. Change Control Process

MDE and MDIT had not developed a comprehensive change control process for SAMS, MEGS, CMS, CNAP, and FNS-FRS. As a result, MDE and MDIT could not ensure that the program files and database files were protected from corruption and unauthorized changes.

COBIT states that effective change controls ensure that only authorized programs and modifications are implemented. This is accomplished by the establishment of a formal change management process that institutes policies, procedures, and techniques to help ensure that all program and database changes are properly authorized, tested, and approved and that proper separation of duties exists over the change control process.

We reviewed program and database changes to SAMS, MEGS, CMS, CNAP, and FNS-FRS from October 2005 through January 2008. Our review disclosed:

a. MDE and MDIT did not ensure proper separation of duties for the change control process. As a result, unauthorized changes to programs and data could go undetected. We noted that a system developer for SAMS; contracted project managers for MEGS, CMS, and CNAP; and a contracted system developer for FNS-FRS could initiate, test, and authorize program and database changes without documented business owner approvals. As identified in Finding 1, these developers and contractors have privileged access to the programs. Therefore, they have the ability to bypass controls that would prevent or detect malicious and unauthorized changes to the system.

b. MDE and MDIT did not have a formal process for requesting and tracking change requests. As a result, MDE and MDIT could not ensure that only authorized program and database changes were made. ISO/IEC 17799:2005 requires an effective change process to ensure that changes are documented in a way that they can be traced to authorization from the design specifications and functional requirements of the system users. We noted:

(1) MDE and MDIT did not have a documented process for making emergency program and database changes for SAMS, MEGS, CMS, CNAP, and FNS-FRS. As a result, controls for testing and approving emergency changes could be bypassed. Defining the conditions under which emergency changes are allowed as well as testing and approval requirements would help ensure efficient and secure movement of emergency changes to production.

(2) MDE and MDIT did not have effective controls to identify unauthorized program and database changes for SAMS, MEGS, CMS, CNAP, and FNS-FRS. An effective change control process would ensure that any program changes that occur outside the authorized process are detected.

(3) MDE and MDIT did not obtain documented approvals from authorized individuals prior to implementing program and database changes. As a result, MDE and MDIT could not ensure that all program and database changes were appropriately tested and approved by MDE management.

RECOMMENDATION

We recommend that MDE and MDIT develop a comprehensive change control process for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

AGENCY PRELIMINARY RESPONSE

MDE and MDIT agree and informed us that MDE will systematically review the procedures for each system and then create a control process appropriate for each system. MDE also informed us that it will ensure that each system has proper segregation of duties, appropriate audit trails of all program and database changes, a documented emergency change process, an effective control process, and a process for requesting and tracking changes. In addition, MDE and MDIT informed us that they will develop a project plan by December 31, 2008 that will include a

review, validation, and enforcement of change processes for all systems named in this audit, and the target date for compliance with these change control processes is March 31, 2009.

FINDING

5. SAMS, MEGS, CMS, and CNAP Data Integrity

MDE did not fully ensure the completeness and accuracy of SAMS, MEGS, CMS, and CNAP data.

Our review disclosed:

a. MDE did not fully update SAMS and MEGS recipient information with data from the School Code Master (SCM) data file. SCM is the State of Michigan's official database directory of schools and facility information. We identified 14 school names, 9 addresses, 29 SCM inactive status indicators, and 7 federal employer identification numbers (FEINs) in MEGS that did not match to the data in SCM.

b. MDE did not ensure that MEGS and CMS contained accurate recipient FEINs. Without an accurate FEIN, MDE cannot ensure that payments go to the correct recipient. We noted:

(1) MEGS and CMS contained 110 recipients with no FEINs that were coded as eligible to receive grant payments.

(2) MEGS and CMS contained 18 recipients with incorrect FEINs.

(3) MEGS and CMS contained 26 recipients that did not exist in the Michigan Administrative Information Network (MAIN) vendor file by name or FEIN.

As identified in Finding 8, inaccurate FEINs have resulted in payments to the wrong recipients.

c. MDE did not ensure that all agency information was stored within the MEGS agency table. Without complete data, MDE cannot report accurate information. We noted 114 agencies with no political district code,

164 recipients with no building code, and 7 agencies with no agency type. MDE identified these fields as required information.

d. MDE did not ensure that the MEGS grant table always contained the grant award end date. We noted 302 grants with blank grant award end dates. Without a grant award end date, recipients could receive reimbursements for expenditures after the grant's period of availability. Grant expenditures are only permitted during the grant's period of availability. Also, MDE uses the grant award end date to determine when a grant's final expenditure report is due.

e. MDE did not ensure that the recipients' final expenditure reports in CMS accurately reported the actual grant expenditures. When MDE converted data from the Grants Cash Management Reporting System to CMS, it reopened 46 closed final expenditure reports and miscoded the expenditures as disallowed costs. This was done to balance the final expenditure reports in CMS. MDE should correct the inaccurately reported expenditures.

f. MDE did not ensure that the MEGS and CMS user table contained critical identifying information about MEGS and CMS users. We noted 9 MEGS and CMS user accounts that did not have a name or address in the user table. Without identifying information, MDE could not ensure accountability for transactions.

g. MDE did not ensure that the MEGS and CMS grant table contained required MAIN payment coding information. Incorrect payment coding information requires manual user intervention and increases the likelihood of payment errors. We noted 87 grants with no MAIN index code. Index codes are needed to process payments to recipients.

h. MDE did not ensure that MEGS and CMS required that a grant availability start date preceded the grant availability stop date. We identified eight grants whose grant availability start dates in MEGS were later than their grant availability stop dates in MEGS.

i. MDE did not identify and remove duplicate recipient records in CNAP. We noted that 117 (7%) of 1,578 recipients had submitted claims with duplicate

records in the CNAP agency table. Removing duplicate records helps improve the reliability, quality, and exchange of data between information systems.

RECOMMENDATION

We recommend that MDE fully ensure the completeness and accuracy of SAMS, MEGS, CMS, and CNAP data.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that it will continue to work to monitor the completeness and accuracy of SAMS, MEGS, CMS, and CNAP data.

FINDING

6. Disaster Recovery

MDE and MDIT had not established complete backup and recovery controls. As a result, MDE and MDIT cannot fully ensure the integrity and availability of SAMS, MEGS, CMS, CNAP, and FNS-FRS in the event of a business disruption.

ISO/IEC 17799:2005 states that disaster recovery plans should be developed and implemented to ensure availability and security of information in the event of business disruptions.

Our review disclosed:

a. MDE and MDIT had not developed and tested a comprehensive disaster recovery plan for SAMS, MEGS, CMS, CNAP, and FNS-FRS. The lack of a comprehensive plan increases the likelihood that a service disruption could delay State and federal payments to recipients. MDIT has included SAMS, MEGS, and CNAP among its 56 most critical systems.

b. MDIT did not fully restrict contractors' access to backup data files. We noted that 4 (19%) of 21 backup and recovery contractors with access accounts to MDE's backup and recovery data files were no longer employed. Access rights of contractors should be removed upon termination of employment to safeguard MDE's data.

RECOMMENDATION

We recommend that MDE and MDIT establish complete backup and recovery controls.

AGENCY PRELIMINARY RESPONSE

MDE and MDIT agree and informed us that MDIT has already collected approximately 88% of the system data necessary to establish comprehensive disaster recovery plans for the critical MDE systems and, prior to October 2006, performed off-site testing of a legacy desktop SAMS system disaster recovery operation. MDIT also informed us that it will work with MDE to fully establish effective backup and recovery controls by December 31, 2009.

FINDING

7. Audit Trails

MDE did not fully develop and monitor audit trails for SAMS, MEGS, and CMS.

Our review disclosed:

a. MDE did not have audit trails of SAMS transactions and payments. As a result, MDE could not monitor transactions to ensure that malicious or unintended changes to payment data will be detected.

b. MDE did not always record the identity of the user who created or updated a transaction in MEGS and CMS. As a result, MDE are unable to monitor which users performed which transactions. The CMS requirements document states that user information will be contained in all database tables.

COBIT requires that audit trails be designed to record the usercode, date, and time of each transaction to enable MDE to identify and monitor the user who originated or updated each transaction.

RECOMMENDATION

We recommend that MDE fully develop and monitor audit trails for SAMS, MEGS, and CMS.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that CMS has audit trails incorporated in the system. Also, MDE informed us that MEGS and CMS will be reviewed to ensure that all necessary audit trails are developed and monitored. In addition, MDE informed us that a project plan, including an evaluation of MEGS and CMS audit trails, will be developed by December 31, 2008.

Further, MDE informed us that SAMS is currently being rewritten and updated, and the new version of SAMS will include audit trails as part of the security improvement requirements that are included in the design and development of the system. MDE also informed us that the new system is scheduled for parallel implementation with the existing SAMS system by fall 2009.

ACCURACY OF PAYMENT CALCULATIONS

COMMENT

Audit Objective: To assess the effectiveness of MDE and MDIT's efforts to ensure that the selected information systems accurately calculate federal and State payments.

Audit Conclusion: MDE and MDIT were moderately effective in their efforts to ensure that the selected information systems accurately calculated federal and State payments. Our assessment disclosed one material condition. MDE did not ensure the accurate processing of MEGS and CMS grant transactions (Finding 8). Our assessment also disclosed four reportable conditions related to Title I calculation, SAMS security, MEGS and CMS documentation, and FNS-FRS processing (Findings 9 through 12).

FINDING

8. MEGS and CMS Transactions

MDE did not ensure the accurate processing of MEGS and CMS grant transactions. As a result, MDE issued duplicate and inaccurate federal and State payments to recipients.

We reviewed grant payments processed by MEGS and CMS from October 2006 through April 2008. Our review disclosed:

a. MDE did not fully ensure that MEGS and CMS processed only authorized and accurate payments to recipients. We noted:

   (1) CMS did not have controls to prevent duplicate payments. We noted 189 duplicate payments totaling $9.3 million that were issued to grant recipients. These payments were duplicates of a previously issued payment. MDE recouped the duplicate payments by adjusting the recipient's future grant payments.

   (2) CMS processed payments to the wrong recipients. Our review disclosed that 3 payments totaling $570,137 were issued to the wrong recipients because the recipient FEINs in CMS were inaccurate. Subsequent to bringing this to management's attention, MDE recovered the money.

b. MDE did not have controls to limit 30-day cash advances for only eligible federal grants and recipients in MEGS and CMS. MDE processed 91 payments through CMS totaling $6.1 million for 30-day cash advances for federal grants and recipients that did not qualify for a 30-day cash advance.

   MDE should develop a policy that outlines which federal grants and grant recipients are eligible for a 30-day cash advance to help ensure that 30-day cash advances are only permitted for eligible federal grants or grant recipients. In addition, MDE should modify CMS to reflect the policy for cash advances and reject requests for ineligible cash advances.

c. CMS did not alert MDE if a recipient's requested cash advance was not within a reasonable dollar amount to meet the recipient's immediate cash needs. As a result, grant recipients could receive a cash advance that exceeds the immediate needs of the grant recipient. Federal guidelines require that recipients receive grant payments for only as much cash as is necessary to meet the immediate needs of the grant project.

d. MDE did not ensure that all payment adjustments to recipients in CMS were properly documented and approved. Changes to recipient payments are

made in CMS using adjustment transactions. We selected 71 adjustment transactions and noted that 17 (24%) adjustments totaling $417,000 did not have documented support and approval. Without documented support and approval for adjustment transactions, MDE cannot ensure that grant balances and payment amounts are complete and accurate.

RECOMMENDATION

We recommend that MDE ensure the accurate processing of MEGS and CMS grant transactions.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that the exceptions are attributed to programming and human errors during the implementation of CMS. MDE informed us that CMS is being implemented over a phased-in period starting October 2006 through December 2008. In addition, MDE informed us that, during the audit period, MDE processed 25,700 payments totaling $1.3 billion in CMS. The 189 duplicate payments, the 3 payments to the wrong recipients, and the 91 30-day cash advances combined totaled approximately 1.1% of all payments processed in CMS. MDE informed us that the 189 duplicate payments were made as a result of program and human errors that have been identified and corrected. Also, MDE informed us that internal control has been developed to identify inaccurate FEINs in CMS, and a policy change has been adopted to address 30-day cash advances. Further, MDE informed us that, while it hoped that programming and human errors would be minimal, it acknowledges that errors occurred; however, the errors were not due to internal control weaknesses but to implementation complications.

FINDING

9. Title I Calculation

MDE did not implement system controls to ensure the accurate calculation of education finance incentive grant (EFIG) Title I payments for the No Child Left Behind Act of 2001. As a result, MDE made inaccurate EFIG Title I recipient payments.

The U.S. Department of Education Title I Grants to Local Educational Agencies are distributed through four statutory formulas, including the basic grant, concentration grant, targeted grant, and EFIG. The four formulas are based on census poverty

estimates and the education cost in each state. Title I provides financial assistance to schools with a high number of poor children. The system that MDE used for calculating the complex Title I formula did not include controls over application and database access or program change controls.

Our review of the four statutory formulas for 2005-06 and 2006-07 disclosed errors in the programming of the formula to calculate EFIG funds. MDE overpaid $1,016,669 to 31 local educational agencies (LEAs) and charter schools during fiscal year 2005-06 and $488,297 to 27 LEAs and charter schools during fiscal year 2006-07. As a result, MDE underpaid 602 and 455 LEAs and charter schools for the same amount in fiscal years 2005-06 and 2006-07, respectively.

MDE uses the allocation for Title I payments to calculate Education Technology State Grants and Safe and Drug-Free Schools and Communities - State Grants payments. Therefore, these payments may also be in error.

RECOMMENDATION

We recommend that MDE implement system controls to ensure the accurate calculation of EFIG Title I payments for the No Child Left Behind Act of 2001.

AGENCY PRELIMINARY RESPONSE

MDE disagrees with the nature of the finding. MDE informed us that, although there was a human error in the entry of the formula, MDE contends that it was not a weakness of the information technology system.

OFFICE OF THE AUDITOR GENERAL EPILOGUE

We disagree with MDE that this finding was not a weakness of the information technology system. The inaccurate grant payments were caused by errors in the programming of the calculation of Title I formula grants in the system. Information technology controls such as database and program change controls would help ensure the accurate programming of the calculation of Title I formula grants.

FINDING

10. SAMS Security

MDE did not implement separate user roles for processing State aid payments in SAMS. As a result, MDE could not ensure that the appropriate approvals were enforced for calculating and paying recipients in SAMS.

COBIT states that implementing user roles enforces the separation of duties to ensure appropriate approvals that prevent users from initiating and authorizing their own transactions.

We reviewed State aid payments and adjustments calculated between May 2006 and December 2007. Our review disclosed:

a. The same SAU employee calculated and certified 4 of 2,056 State aid payments. Payments should be certified by a person independent of the payment calculation.

b. An SAU employee other than a manager certified 1,749 (85%) of 2,056 payments and adjustments. The SAMS User Manual indicates that payments and adjustments should be certified by the SAU manager. SAMS did not enforce certification of payments by a user with the manager role.

RECOMMENDATION

We recommend that MDE implement separate user roles for processing State aid payments in SAMS.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that it will update its policy and procedures for processing State aid payments by December 31, 2008. MDE also informed us that SAMS is currently in redevelopment and the updated system will ensure that separate roles for system users are enforced. In addition, MDE informed us that the new system is scheduled for parallel implementation with the existing SAMS system by fall 2009.

FINDING

11. MEGS and CMS Documentation

MDE and MDIT did not ensure that the vendor provided complete system documentation for MEGS and CMS as required by the vendor's contract. Without system documentation, which describes the business rules, calculations, system processes, and technical design, MDE and MDIT cannot identify the cause of system problems in MEGS and cannot ensure that the system is working as intended.

Section 18.1485 of the *Michigan Compiled Laws* states that departments shall document systems, communicate system requirements, ensure that the system is functioning as prescribed, and modify as appropriate for changes in the system. The vendor's contract states that project management services include gathering and documenting business requirements, verifying and validating business requirements, and tracking and addressing the impact of changes in requirements. In addition, the contract states that the project manager must provide and maintain up-to-date system documentation including the technical specifications for the business requirements. Our review disclosed:

a. MDE did not ensure that the MEGS and CMS requirements document contained or clearly defined the business rules and calculations for requesting grant funds, reporting grant expenditures, paying grant recipients, and monitoring transactions. In addition, the vendor did not update the MEGS and CMS requirements document as changes were implemented. We noted that MDE did not ensure that high risk transactions within MEGS and CMS could be monitored by MDE staff. MDE should determine which transactions are high risk and work with MDIT to create a method for monitoring.

b. MDE did not require the vendor to provide a data dictionary or the design documents. These documents describe how the system processes data in relation to the business rules and calculations and enable MDE and MDIT to ensure that the system is processing data as intended. We noted:

(1) MDE did not ensure that MEGS prevented the overall grant amount that recipients are eligible to receive from exceeding the overall budgeted amount available to recipients. We noted one grant in which the amount recipients were eligible to receive exceeded the grant budget by $6,548.

Preventing the overall grant amount that recipients are eligible to receive from exceeding the overall budgeted amount available to recipients is a MEGS objective.

(2) MDE did not have reports to identify data errors in MEGS and CMS. For example, CMS did not produce a report comparing CMS payment requests to MAIN payments. MDE identified the report as a CMS requirement.

(3) MDE did not ensure the accuracy of MEGS and CMS reports. We noted that the same report from MEGS and CMS showed different grant balances for the same grant. The accuracy of MEGS and CMS reports is essential because the grant process is entirely automated and MDE relies on recipients and grant program personnel to review output reports to identify errors.

RECOMMENDATION

We recommend that MDE and MDIT ensure that the vendor provides complete system documentation for MEGS and CMS as required by the vendor's contract.

AGENCY PRELIMINARY RESPONSE

MDE and MDIT agree and informed us that they will work together to create complete system documentation, including business rules, calculations, data dictionaries, and design documents for MEGS and CMS. MDE also informed us that a work plan for the MEGS and CMS systems has already been developed for fiscal year 2008-09, which includes creating the necessary system documentation.

FINDING

12. FNS-FRS Processing

MDE did not fully establish processing controls over meal claims calculated by FNS-FRS. As a result, MDE cannot ensure that all meal claims processed in FNS-FRS were accurate.

We reviewed meal claims processed by FNS-FRS from October 2005 through January 2008. Our review disclosed:

a. MDE did not ensure that all meal claims input into FNS-FRS were edited for compliance with payment rules. We noted that four meal claims in the School Meals Program were not edited with the standard system edits. One of the four meal claims resulted in an overpayment of $56. System edits should ensure that payment rules are applied consistently to all meal claims.

b. MDE did not ensure that all system overrides of edits were approved. We noted 10 meal claims in the School Meals Program in which program staff overrode the system edits without documented approval. COBIT states that the override of system edits should have formal documented approval by management.

c. MDE did not have complete and up-to-date documentation of edits in FNS-FRS. Maintaining a complete and current list of edits ensures that business owners and developers are aware of, and agree on, the controls that should be established and enforced in FNS-FRS. System edits include, but are not limited to, validity, reasonableness, existence, completeness, and logical relationship checks.

RECOMMENDATION

We recommend that MDE fully establish processing controls over meal claims calculated by FNS-FRS.

AGENCY PRELIMINARY RESPONSE

MDE agrees and informed us that it will work with MDIT to fully establish controls over meal claims calculated by FNS-FRS. MDE also informed us that all controls will be documented.

GLOSSARY

certify	To confirm grant fund requests and expenditures.
CMS	Cash Management System.
CNAP	Child Nutrition Application Program.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
effectiveness	Program success in achieving mission and goals.
EFIG	education finance incentive grant.
FEIN	federal employer identification number.
FNS-FRS	Food Nutrition System - Fiscal Reporting System.
integrity	Accuracy, completeness, and timeliness of data in an information system.
ISO/IEC 17799:2005	A security standard published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management.
LEA	local educational agency.
MAIN	Michigan Administrative Information Network.

material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
MDE	Michigan Department of Education.
MDIT	Michigan Department of Information Technology.
MEGS	Michigan Electronic Grants System.
MEIS	Michigan Education Information System.
mission	The agency's main purpose or the reason that the agency was established.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
privileged access	Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
recipient	A receiver of a grant payment and/or meal claim reimbursement, including school districts, charter schools,

	colleges and universities, State agencies, childcare centers, day-care home sponsors, residential care facilities, and summer camps and summer food service sponsors.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
risk assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
SAMS	State Aid Management System.
SAU	State Aid Unit.
SCM	School Code Master.
server operating system	The software that manages the application and data files that are shared over a network.
SRSD	Single Record Student Database.
USDA	U.S. Department of Agriculture.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL