MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON

SELECTED PAYMENT AND RELATED SYSTEMS

MICHIGAN DEPARTMENT OF EDUCATION AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

March 2014

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

313-0590-08F

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

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

March 14, 2014

Mr. Michael P. Flanagan
Superintendent of Public Instruction
Michigan Department of Education
John A. Hannah Building
Lansing, Michigan
and
Mr. David B. Behen, Director and Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Flanagan and Mr. Behen:

This is our report on our follow-up of the 4 material conditions (Findings 1, 2, 4, and 8) and 4 corresponding recommendations reported in the performance audit of Selected Payment and Related Systems, Michigan Department of Education (MDE) and Michigan Department of Information Technology (MDIT). That audit report was issued and distributed in November 2008. Additional copies are available on request or at <http://audgen.michigan.gov>.

In March 2010, subsequent to our performance audit, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management, and Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and unexpended balances of appropriations, allocations, or other funds of MDIT to DTMB and abolished MDIT.

This report contains an introduction; our purpose of follow-up; a background; our scope; and follow-up conclusions, results, recommendations, and agency responses; and a glossary of abbreviations and terms.

Our follow-up disclosed that MDE and DTMB had complied with 1 recommendation and had partially complied with 3 recommendations. Material conditions still exist related to security program and access controls (Finding 1), database security (Finding 2), and the change control process (Finding 4). Also, a reportable condition exists for parts of the finding related to security program and access controls (Finding 1). As a result, we have issued 2 repeat recommendations and 1 rewritten recommendation.

If you have any questions, please call me or Scott M. Strong, C.P.A., C.I.A., Deputy Auditor General.

Sincerely,

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

313-0590-08F

This Page Left Intentionally Blank

TABLE OF CONTENTS

FOLLOW-UP REPORT
SELECTED PAYMENT AND RELATED SYSTEMS
MICHIGAN DEPARTMENT OF EDUCATION AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

FOLLOW-UP REPORT
SELECTED PAYMENT AND RELATED SYSTEMS
MICHIGAN DEPARTMENT OF EDUCATION AND DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

INTRODUCTION

This report contains the results of our follow-up of the material conditions* and corresponding recommendations reported in our performance audit* of Selected Payment and Related Systems, Michigan Department of Education (MDE) and Michigan Department of Information Technology (MDIT), (313-0590-08), which was issued and distributed in November 2008. That audit report included 4 material conditions (Findings 1, 2, 4, and 8) and 8 reportable conditions*.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether MDE and the Department of Technology, Management, and Budget (DTMB) had taken appropriate corrective measures in response to the 4 material conditions and 4 corresponding recommendations noted within our November 2008 report.

BACKGROUND

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 School Support Services 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,

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

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 $12.8 billion in federal and State grant payments in fiscal year 2012-13 through the following information systems:

1. State Aid Management System* (SAMS)

   Since the performance audit, MDE and DTMB have rewritten SAMS. The new Web-based version of SAMS was implemented in July 2011. SAMS is used by the Office of State Aid and School Finance to process 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.

   In fiscal year 2012-13, SAMS processed $10.9 billion in payments.

2. Michigan Electronic Grants System Plus* (MEGS+)

   MEGS+ is an automated Web-based information system used to create, submit, approve, track, and amend grant applications. MEGS+ was implemented in April 2011 and replaced the Michigan Electronic Grants System (MEGS) and the Child Nutrition Application Program System (CNAP).

   School districts, local 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. MDE uses MEGS+ to manage the allocation of over 50 federally funded and State-funded grants.

   As of October 2013, MEGS+ had approximately 11,400 users, including MDE staff, school districts, charter schools, colleges and universities, State agencies, childcare centers, day-care home sponsors, residential childcare facilities, and summer camps and summer food service sponsors.

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

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

districts, colleges and universities, day-care home sponsors, and summer camps. CMS processed $1.9 billion in recipient payments during fiscal year 2012-13. 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. As of October 2013, CMS had approximately 2,900 users, including MDE staff, school districts, charter schools, colleges and universities, and State agencies.

4. Food Nutrition System - Fiscal Reporting System* (FNS-FRS)

FNS-FRS consists of 10 subsystems, including 5 claim collection systems; 3 batch payment processing systems for the School Meals Program, Child and Adult Care Food Program, Summer Food Service Program, and Summer Camp Special Milk Program; and 2 reporting systems. Each month, participants enter the number of meals or the cost of meals served into the on-line claim forms. The batch payment processing systems calculate meal reimbursement amounts for payments to the participants. As of October 2013, there were approximately 4,000 system users, including MDE staff, school districts, childcare centers, adult day-care centers, day-care home sponsors, residential childcare facilities, and summer camps and summer food service sponsors.

Michigan Education Information System* (MEIS)

MEIS is a front end data authentication tool for some MDE Web applications available on the Internet and MDE's Intranet. All users with access to MDE systems have a unique MEIS account. Once a user is authenticated in MEIS, MEIS determines whether the user is authorized to access a system (such as MEGS+, CMS, and FNS-FRS) and grants or denies access to the system. MEIS was developed in 1996.

Department of Technology, Management, and Budget (DTMB)

Executive Order No. 2009-55, effective March 21, 2010, abolished MDIT and renamed the Department of Management and Budget as DTMB. DTMB's Customer Services provides information system support services to SAMS, MEGS+, CMS, FNS-FRS, and

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

MEIS, including operating system configuration, database administration, and physical security. Customer 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, and FNS-FRS.

SCOPE

We interviewed employees from MDE and DTMB to determine the status of compliance with our audit recommendations. We reviewed access rights to the systems and data. We also reviewed documentation to determine whether access to databases was properly restricted and sensitive data was encrypted. In addition, we reviewed database documentation to determine whether privileged user activity was monitored, audit logs were maintained and reviewed for high-risk activity, unnecessary stored procedures were removed or disabled, and data dictionaries were developed. Further, we reviewed policies and procedures related to change management and tested compliance with those policies and procedures. We also tested CMS payment data for duplicate payments, payments made to incorrect recipients, and controls related to 30-day cash advances and adjustment transactions processed in CMS.

FOLLOW-UP CONCLUSIONS, RESULTS, RECOMMENDATIONS, AND AGENCY RESPONSES

SECURITY AND ACCESS CONTROLS

SUMMARY OF THE NOVEMBER 2008 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. Our 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.

   b. MDE did not restrict MDE users' access to ensure a segregation 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 had the ability to both change and approve State aid allocation amounts to schools using SAMS.

   c. MDE did not prevent users from logging on as another user and making changes to MEGS and CMS 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. We noted:

(1) MDE did not ensure that only security administrators granted user access to MEGS and CMS.

(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.

(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.

(5) MDE did not obtain security agreements for all grant recipients that use the system to certify* grants.

(6) MDE did not properly approve the granting of recipient access to systems.

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.

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

f. MDE did not remove user accounts created for testing data.

g. MDE did not prevent privileged users from renaming user accounts.

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

h. MDE did not lock out usercodes after a reasonable number of invalid login attempts for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

i. MDE did not disconnect users or use password-protected screen savers after a reasonable period of system inactivity for SAMS and CNAP.

j. MDE did not implement strong password controls for SAMS.

RECOMMENDATION (AS REPORTED IN NOVEMBER 2008)

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.

FOLLOW-UP CONCLUSION

We concluded that MDE had partially complied with the recommendation. However, a material condition still exists because MDE had not restricted development staff from privileged access to MDE's production data (part a.), did not restrict MDE users' access (part b.(1)), did not ensure that only security administrators granted user access to MEGS+ and CMS (part d.(1)), and did not fully establish an effective process to monitor user access for CMS (part e.(1)).

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, MDE complied with the recommendation as it relates to SAMS and FNS-FRS. MDE partially complied with part a. as it relates to MEGS+ and CMS. MDE developed a security access policy that requires that the most restrictive set of privileges needed to perform job duties should be assigned to users. Also, MDE upgraded SAMS since the prior audit. SAMS developers no longer have privileged access to production data or the ability to change historical information or calculate and issue State aid

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

payments in SAMS. Also, DTMB developers and contracted developers no longer have privileged access to production data in FNS-FRS.

In regard to MEGS+ and CMS, 17 of the 20 developers with privileged access to MEGS+ and CMS in the original finding had their access removed; however, 1 individual still had privileged access to production data in MEGS+ and 2 individuals had privileged access to production data in both MEGS+ and CMS. These three individuals are no longer developers. Two of these individuals are working as contracted project managers and the other is working for DTMB. Access for all three of these individuals is excessive for their current positions. In addition, one contracted developer had privileged access to CMS production data. As a result of the four individuals with privileged access, a material condition still exists for MEGS+ and CMS.

b. Regarding part b. of the finding, MDE partially complied with the recommendation. We noted:

(1) MDE removed the multiple accounts for the project manager and users of MEGS+ and CMS. However, as of August 2013, we identified one MEGS+ user with multiple user accounts who had the ability to approve and certify grant applications. Three additional MEGS+ users also had multiple accounts. The roles assigned to these three users with multiple accounts did not allow them to bypass controls. However, allowing users to have multiple active user accounts increases the risk that incompatible roles will be assigned to a single user which allow the user to bypass established system controls. As a result, a material condition still exists for MEGS+.

(2) MDE modified access rights for SAMS to enforce segregation of duties. The director and assistant director of the State Aid Unit no longer had access rights to change and approve State aid allocation amounts to schools. As a result, a material condition no longer exists for SAMS.

c. Regarding part c. of the finding, MDE complied with the recommendation. MDE no longer allows users to "log-in as" other users of CMS. MDE still allows MEGS+ to use the "log-in as" function; however, MDE monitors the

activity of the individuals using this function. In addition, the changes that users can make in MEGS+ while using the "log-in as" function have been limited.

d. Regarding part d. of the finding, MDE partially complied with the recommendation. We noted:

(1) The contracted project manager still had the ability to grant user access to CMS. In addition, one developer and one former developer had the ability to grant user access to CMS. MDE also allowed one secretary and one contracted project manager, who is also a former developer, to have the ability to grant user access to MEGS+. The contracted project manager granted access to 4 MEGS+ users during 2011. As a result, a material condition still exists. After bringing this matter to management's attention, MDE removed this ability from the contracted project manager for MEGS+.

(2) MDE policy defines the titles of the individuals allowed to request access to each system. Prior to granting access, MDE employees for MEGS+, CMS, and FNS-FRS verify that the requestor who signed the form requesting school district staff access to the systems is an authorized requestor. As a result, a material condition no longer exists.

(3) MDE established a policy on how to assign user access to school district users for MEGS+ and CMS based on user needs. However, MDE had not defined or documented the appropriate level of system access for State employee users based on their job duties or combinations of roles. Because MDE partially complied by establishing a policy on assigning access, a reportable condition exists.

(4) MDE established, but did not consistently enforce, policies requiring State employees to sign and submit security agreements before being granted access to MDE systems. These policies also require that access be granted based on an individual's need for the information. All State employees requesting access to FNS-FRS are required to submit a security agreement form. We randomly sampled 20 MDE employees to

whom MDE had granted access to MEGS+ and noted that MDE did not have a signed security agreement for 5 (25%) of the 20 users. We also noted that MDE did not require read-only users of SAMS and MEGS+ to submit security agreements. In addition, we noted that SAMS users from the Department of Treasury did not sign security agreements because MDE did not require the users' signatures. As a result, a reportable condition exists for SAMS and MEGS+.

(5) MDE established policies to require security agreements for all grant recipients that use MEGS+, CMS, and FNS-FRS to certify grants. We selected a sample of users from each of the three systems and determined that all of the users in our MEGS+ and CMS sample had signed security agreements on file. However, 1 (5%) of the 20 users in our sample of FNS-FRS recipient users did not have a signed security agreement on file.

MDE also established policies requiring an annual audit of a sample of users of each system to verify that security agreements were on file. However, MDE did not perform the annual audit of FNS-FRS users and did not maintain the original security agreements when it conducted annual audits of CMS users.

Because MDE partially implemented its security agreement policies, a reportable condition exists for CMS and FNS-FRS.

(6) MDE properly approved the granting of recipient user access to MEGS+, CMS, and FNS-FRS. We selected a sample of 20 recipient security agreements for each system and verified that the appropriate individuals approved user access. As a result, a material condition no longer exists.

e. Regarding part e. of the finding, MDE partially complied with the recommendation. We noted:

(1) MDE monitored high-risk user activity for MEGS+ and CMS by reviewing high-risk transaction reports. However, for CMS, this review was done by a privileged user who had access rights to process payments. As a

result, unauthorized changes made by this user may not be detected. In addition, the report used to monitor high-risk activity did not include all users with privileged access to CMS. As a result, a material condition still exists for CMS.

(2) MDE had taken steps to disable user accounts of users who no longer required access. MDE implemented an annual process to confirm, on a sample basis, that CMS user access was still appropriate. Also, MDE configured MEGS+ and CMS to disable user accounts if users do not log in for an extended period of time. However, this control did not function as intended as users who did not require access to MEGS+ and CMS still had active user accounts.

We reviewed the users who were noted in the original audit as no longer requiring access to MEGS+ and CMS to determine if those users still had active user accounts. We noted that MDE had disabled the CMS user accounts. However, MDE had not disabled the three MEGS+ users who no longer required access. We contacted the recipient agencies to determine whether these three users required access and were informed that the users were no longer employed by those agencies and that the agencies no longer use MEGS+.

We also judgmentally selected users for MEGS+ and CMS to determine if their access was still appropriate. We noted that 3 (23%) of 13 MEGS+ users and 3 (25%) of 12 CMS users no longer required access. The recipient agency had submitted the appropriate removal form to the Center for Educational Performance and Information (CEPI), as instructed by the form, to have the CEPI account for one user disabled; however, MDE did not receive the form from CEPI to disable the MEGS+ and CMS accounts. We also noted one former MDE employee who still had the ability to update data in CMS. As a result, a reportable condition exists for MEGS+ and CMS.

Our review of SAMS disclosed that MDE had developed and implemented policies and procedures for removing user access for SAMS. We reviewed the current user list and verified that all users were

current State employees. As a result, a material condition no longer exists for SAMS.

f. Regarding part f. of the finding, MDE complied with the recommendation. MDE had removed all test accounts in CMS. MEGS+ still used test accounts; however, we confirmed that the test accounts no longer have access rights to change production data.

g. Regarding part g. of the finding, MDE complied with the recommendation. MDE no longer allows users to rename user accounts in either MEGS+ or CMS. MEGS+ and CMS user accounts are created and maintained in MEIS. We verified that MEIS prevents users from renaming an existing user account.

h. Regarding part h. of the finding, MDE complied with the recommendation as it relates to SAMS and FNS-FRS but did not comply with regards to MEGS+ and CMS. MDE worked with DTMB in 2011 to update SAMS to lock user accounts after five invalid login attempts. MDE and DTMB also worked together to add this functionality to FNS-FRS. Initially, this control was not functioning as intended in FNS-FRS. When we brought this to management's attention, MDE and DTMB modified FNS-FRS to lock user accounts after five invalid login attempts. However, MDE had not taken steps to ensure that MEGS+ and CMS lock out users after a reasonable number of invalid login attempts. As a result, a reportable condition exists for MEGS+ and CMS.

i. Regarding part i. of the finding, MDE complied with the recommendation. MDE updated SAMS and MEGS+ to disconnect users after 20 minutes of inactivity.

j. Regarding part j. of the finding, MDE complied with the recommendation. MDE implemented strong password controls in SAMS that meet the State's requirement for security.

FOLLOW-UP RECOMMENDATION

We again recommend that MDE and DTMB continue to fully establish a comprehensive information systems security program and effective access controls over MDE information systems.

FOLLOW-UP AGENCY RESPONSE

MDE and DTMB agree with the recommendation.

In response to part a. of the follow-up results, MDE informed us that it reviewed MEGS+ access levels for all non-MDE employees. For MEGS+, MDE assigned new security levels to two contracted staff in accordance with their responsibilities. For a third user, MDE downgraded the user's security level. Access for this user will be monitored on a regular basis during the MEGS+ high-risk transaction reviews. MDE also informed us that the CMS project manager's privileged access is restricted and is reported on the administrative CMS high-risk activity report, which is reviewed by the assistant director of the Office of Financial Management on a quarterly basis. According to MDE, the project manager's contract is not being renewed and will be replaced by DTMB information technology staff on or before September 30, 2014.

In response to part b. of the follow-up results, MDE informed us that it has reviewed all cases of users having multiple accounts. One Child Nutrition Program employee has two distinct functions to perform in MEGS+ and maintains two separate accounts. MDE informed us that it has reviewed and changed the employee's security level so this user is not able to approve and certify applications. Activities for the new security level will be reviewed as part of the high-risk transaction review process. MDE informed us that it resolved the other cases by removing nonrequired access or by reviewing the case.

In response to part d. of the follow-up results, MDE informed us that it reviewed and updated security levels as recommended. Specifically, only Grants Coordination Support Services staff from the Office of School Support Services have permission to grant access to MEGS+. MDE informed us that it will develop appropriate guidance for system access for State employees based on their job duties and combination of roles. This documentation will be completed by May 31, 2014. Also, through the annual audit process, MDE will review and verify security agreements. For the year ended December 31, 2013, MDE completed the annual security audit as required in the MDE security policy. However, MDE informed us that it will not require signed security agreements from the Department of Treasury users of SAMS.

In response to part e. of the follow-up results, MDE informed us that an additional monitoring report was established. The monitoring activity report will be run quarterly to identify users not covered under the high-risk activity report based on user roles. MDE will assign the responsibility of generating the quarterly report to the chief accountant, who is not a CMS privileged user. MDE also informed us that access for all users who have not accessed MEGS+ or CMS for 15 months will be inactivated.

In response to part h. of the follow-up results, MDE informed us that it is updating both MEGS+ and CMS to lock out users after five invalid login attempts. MDE plans to update MEGS+ by April 30, 2014 and CMS by September 30, 2014. The CMS update is dependent upon the upgrade of the .net framework.

SUMMARY OF THE NOVEMBER 2008 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. Our review of the five databases disclosed:

a. MDIT and MDE did not restrict users' access to SAMS database tables.

b. MDE did not encrypt sensitive data in SAMS.

c. MDIT did not monitor the activity of privileged user accounts on any of the five databases.

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.

e. MDIT did not remove or disable unnecessary stored procedures for the MEGS, CMS, CNAP, and FNS-FRS databases.

f. MDIT and MDE did not develop data dictionaries for any of the five databases.

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

RECOMMENDATION (AS REPORTED IN NOVEMBER 2008)

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.

FOLLOW-UP CONCLUSION

We concluded that MDE and DTMB had partially complied with the recommendation. MDE and DTMB had complied with the recommendation as it relates to parts a., b., e., and f. of the finding. However, a material condition still exists because DTMB did not monitor the activity of privileged user accounts or high-risk events on the SAMS, MEGS+, CMS, or FNS-FRS databases (parts c. and d.).

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, DTMB and MDE updated SAMS to require all users to enter a username and password before gaining access to SAMS.

b. Regarding part b. of the finding, MDE encrypted all sensitive data in SAMS.

c. Regarding part c. of the finding, DTMB logged some activity of privileged user accounts; however, it did not monitor the activity to identify unauthorized actions. As a result, a material condition still exists for SAMS, MEGS+, CMS, and FNS-FRS.

d. Regarding part d. of the finding, DTMB implemented an automated audit log which allowed it to monitor failed login attempts and other high-risk events. However, DTMB and MDE did not have a policy or procedure in place to require staff to review the audit logs. In addition, DTMB did not maintain evidence that the logs were reviewed. As a result, a material condition still exists for SAMS, MEGS+, CMS, and FNS-FRS.

e. Regarding part e. of the finding, DTMB informed us that it reviewed the stored procedures in the databases and disabled unnecessary stored procedures. Stored procedures are programs shared by several databases to provide efficiency for common actions such as controlling access. We reviewed the stored procedures for the SAMS, MEGS+, CMS, and FNS-FRS databases and confirmed that DTMB had disabled unnecessary stored procedures as recommended by the Center for Internet Security*.

f. Regarding part f. of the finding, DTMB and MDE had developed data dictionaries for the SAMS, MEGS+, CMS, and FNS-FRS databases.

FOLLOW-UP RECOMMENDATION

We recommend that DTMB and MDE monitor privileged user activity and automated audit logs of high-risk events for the SAMS, MEGS+, CMS, and FNS-FRS databases.

FOLLOW-UP AGENCY RESPONSE

DTMB and MDE agree with the recommendation and informed us that they will implement procedures to require staff to review audit logs to comply with the recommendation by June 30, 2014.

SYSTEM CONTROLS TO ENSURE DATA INTEGRITY

SUMMARY OF THE NOVEMBER 2008 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

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

ensure that the program files and database files were protected from corruption and unauthorized changes. Control Objectives for Information and Related Technology* (COBIT) states that effective change controls ensure that only authorized programs and modifications are implemented. 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 segregation of duties for the change control process.

b. MDE and MDIT did not have a formal process for requesting and tracking change requests:

   (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.

   (2) MDE and MDIT did not have effective controls to identify unauthorized program and database changes for SAMS, MEGS, CMS, CNAP, and FNS-FRS.

   (3) MDE and MDIT did not obtain documented approvals from authorized individuals prior to implementing program and database changes.

RECOMMENDATION (AS REPORTED IN NOVEMBER 2008)

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

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

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.

FOLLOW-UP CONCLUSION

We concluded that MDE and DTMB had complied with the recommendation regarding SAMS and CMS, had partially complied with the recommendation regarding MEGS+, and had not complied with the recommendation regarding FNS-FRS. A material condition still exists for MEGS+ and FNS-FRS because MDE and DTMB did not ensure proper segregation of duties for the change control process (part a.) and because MDE and DTMB did not have a formal process for requesting and tracking change requests, including emergency program and database changes; effective controls to identify unauthorized program and database changes; and a process for obtaining documented approvals from authorized individuals prior to implementing program and database changes (part b.).

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, MDE and DTMB restricted access so that developers and contracted project managers working on SAMS and CMS no longer had the ability to initiate, test, and authorize program and database changes without obtaining documented business owner approval prior to implementing the program and database changes. However, with regard to MEGS+ and FNS-FRS, contracted project managers and contracted developers were still able to initiate, test, and authorize program and database changes without documented business owner approval. As noted in the follow-up results for Finding 1, part a., the MEGS+ contracted project managers had privileged access to MEGS+ and, therefore, had the ability to bypass controls that would prevent or detect malicious and unauthorized changes to MEGS+. As a result, a material condition still exists for MEGS+ and FNS-FRS.

b. Regarding part b. of the finding, MDE and DTMB established and implemented an emergency change process for SAMS and CMS. MDE and

DTMB documented an emergency change process for MEGS+; however, MDE and DTMB did not consistently apply this process when emergency changes were made. In addition, MDE and DTMB had not documented an emergency change management process for FNS-FRS. Business owners did not always test or approve emergency changes prior to implementing the changes. As a result, a material condition still exists for MEGS+ and FNS-FRS.

MDE and DTMB implemented controls to identify unauthorized program and database changes for SAMS and CMS. However, with regard to MEGS+ and FNS-FRS, MDE and DTMB had not implemented controls to identify unauthorized changes. MDE and DTMB were unable to trace 4 (44%) of 9 sampled MEGS+ changes from the initial request to the resolution. For 2 of the 9 changes, MDE and DTMB were unable to determine whether the request resulted in a program or database change. In addition, MDE and DTMB did not test 2 (50%) of 4 sampled FNS-FRS changes prior to implementation. As a result, a material condition still exists for MEGS+ and FNS-FRS.

MDE and DTMB obtain documented approvals showing that MDE management tested and approved program and database changes prior to implementing the changes in SAMS and CMS. We sampled recently implemented SAMS and CMS change requests and noted that MDE and DTMB obtained documented business owner approvals for all changes in our sample prior to implementing program and database changes. However, with regard to MEGS+ and FNS-FRS, MDE and DTMB had not obtained documented business owner approvals prior to implementing program and database changes. We noted that documented business owner approvals were obtained for only 5 (56%) of 9 MEGS+ changes included in our sample. Four (100%) of 4 sampled changes for FNS-FRS were approved by the contracted developer or contracted project manager rather than by designated business owners. As a result, a material condition still exists for MEGS+ and FNS-FRS.

FOLLOW-UP RECOMMENDATION

We again recommend that MDE and DTMB continue to develop a comprehensive change control process for MEGS+ and FNS-FRS.

FOLLOW-UP AGENCY RESPONSE

MDE and DTMB agree with the recommendation and informed us that they will continue to develop a comprehensive change control process. DTMB has developed a change management process and guidelines that will serve as the framework of MDE's change control process. This includes both segregation of duties and the process for requesting and tracking change requests. MDE informed us that it will use Team Foundation Server to document and approve all types of change requests, including emergency changes. MDE and DTMB will complete training for their staff to have the process and guidelines implemented by April 30, 2014.

ACCURACY OF PAYMENT CALCULATIONS

SUMMARY OF THE NOVEMBER 2008 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.

Our review disclosed:

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

(1) CMS did not have controls to prevent duplicate payments.

(2) CMS processed payments to the wrong recipients.

b. MDE did not have controls to limit 30-day cash advances for only eligible federal grants and recipients in MEGS and CMS.

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.

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

RECOMMENDATION (AS REPORTED IN NOVEMBER 2008)

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 federal employer identification numbers (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.

FOLLOW-UP CONCLUSION

We concluded that MDE had complied with the recommendation.

FOLLOW-UP RESULTS

Our follow-up disclosed:

a. Regarding part a. of the finding, we noted:

   (1) MDE informed us that the duplicate payments issued during the original audit were because of an issue with the implementation of CMS and not a control weakness. We verified that CMS had not issued duplicate payments during fiscal year 2012-13.

(2) MDE verified the FEIN in CMS to ensure that it matches an FEIN in the Michigan Administrative Information Network* (MAIN) prior to processing the initial payment to a recipient. In addition, the payments noted in the original finding as being made to incorrect recipients were because of FEINs being blank or all zeroes in CMS. We verified that all recipients who were issued payments during fiscal year 2012-13 had valid FEINs in CMS and that payments were made to the correct recipients.

b. Regarding part b. of the finding, MDE no longer offers 30-day cash advances to grant recipients. We verified that the last 30-day cash advance was processed in October 2008. Therefore, this part of the finding is no longer applicable.

c. Regarding part c. of the finding, this part is no longer applicable. As noted in part b., MDE no longer offers cash advances to grant recipients.

d. Regarding part d. of the finding, MDE maintains documented support and approval for payment adjustments made to recipients in CMS. We selected a sample of 5 adjustment transactions and verified that MDE had documented support and approvals for each transaction.

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

Cash Management System (CMS)	An automated Web-based information system used to input, process, monitor, and control grant cash disbursements to recipients.
Center for Internet Security	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.
CEPI	Center for Educational Performance and Information.
certify	To confirm grant fund requests and expenditures.
change controls	Controls that ensure that program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.
CNAP	Child Nutrition Application Program System.
confidentiality	Protection of data from unauthorized disclosure.
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 standards for good practices for controls over information technology.
DTMB	Department of Technology, Management, and Budget.
FEIN	federal employer identification number.

Food Nutrition System - Fiscal Reporting System (FNS-FRS)	A group of claim collection, batch payment processing, and reporting systems that collect claim information and calculate and process payments for Michigan nutrition programs.
information technology	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
integrity	Accuracy, completeness, and timeliness of data in an information system.
ISO/IEC 17799:2005	A security standard published by the International Organization for Standardization (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.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and 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.

Michigan Administrative Information Network (MAIN)	The State's automated administrative management system that supports accounting, purchasing, and other financial management activities.
Michigan Education Information System (MEIS)	The user authentication system for some MDE Web applications available on the Internet and MDE's Intranet.
Michigan Electronic Grants System Plus (MEGS+)	An automated Web-based information system used to create, submit, approve, track, and amend grant applications.
mission	The agency's main purpose or the reason that the agency was established.
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 persons 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, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
State Aid Management System (SAMS)	An automated, Web-based information system used by the Office of State Aid and School Finance to process State school aid payments for distribution to the State's school districts and charter school recipients.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL