MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

SELECTED GENERAL AND APPLICATION CONTROLS

DEPARTMENT OF NATURAL RESOURCES AND ENVIRONMENT AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

October 2010

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

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

October 20, 2010

Ms. Rebecca A. Humphries, Director
Department of Natural Resources and Environment
Constitution Hall
Lansing, Michigan
and
Ms. Phyllis Mellon, Acting Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Humphries and Ms. Mellon:

This is our report on our follow-up of the 2 material conditions (Findings 1 and 3) and 2 corresponding recommendations reported in the performance audit of Selected General and Application Controls, Department of Environmental Quality (DEQ) and Department of Information Technology (DIT). That audit report was issued and distributed in December 2006. Additional copies are available on request or at <http://www.audgen.michigan.gov>. Executive Order No. 2009-45 created the Department of Natural Resources and Environment (DNRE), effective January 17, 2010. It transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and budgetary resources of the Department of Natural Resources and DEQ to DNRE and abolished the Department of Natural Resources and DEQ. Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of DIT to DTMB and abolished DIT.

Our follow-up disclosed that DNRE and DTMB had complied with 1 recommendation and had partially complied with 1 recommendation. However, a reportable condition exists for the security program and security and access controls recommendation.

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

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

SELECTED GENERAL AND APPLICATION CONTROLS
DEPARTMENT OF NATURAL RESOURCES AND ENVIRONMENT AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
FOLLOW-UP REPORT

Page

Report Letter 1

Introduction 4

Purpose of Follow-Up 4

Background 4

Scope 5

Follow-Up Results

Security and Access 6

1. Security Program and Security and Access Controls 6

Change Management 7

3. Change Management Controls 7

SELECTED GENERAL AND APPLICATION CONTROLS
DEPARTMENT OF NATURAL RESOURCES AND ENVIRONMENT AND DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material conditions and corresponding recommendations and the agency's preliminary response as reported in our performance audit of Selected General and Application Controls, Department of Environmental Quality (DEQ) and Department of Information Technology (DIT) (761-0590-05), which was issued and distributed in December 2006. That audit report included 2 material conditions (Findings 1 and 3) and 3 other reportable conditions.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Natural Resources and Environment (DNRE) and Department of Technology, Management & Budget (DTMB) have taken appropriate corrective measures in response to the 2 material conditions and 2 corresponding recommendations.

BACKGROUND

DNRE information systems contain environmental data necessary to protect public health and preserve the State's environmental resources. DTMB provides information support services to DNRE for Navision, LABWORKS, and the Environmental Response Networked Information Exchange (ERNIE), including operating system configuration, application development and maintenance, database administration, program and data change controls, and backup and recovery controls.

Executive Order No. 2009-45 created DNRE, effective January 17, 2010. It transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and budgetary resources of the Department of Natural Resources and DEQ to DNRE and abolished the Department of Natural Resources and DEQ.

Executive Order No. 2009-55 renamed the Department of Management and Budget as DTMB, effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of DIT to DTMB and abolished DIT.

SCOPE

Our fieldwork was performed between May and July 2010. We interviewed employees from DNRE and DTMB to determine the status of compliance with our audit recommendations. We reviewed access to data and data systems, monitoring for unusual or inappropriate transactions, and policies and procedures related to change management. We tested compliance with change management policies and procedures.

FOLLOW-UP RESULTS

SECURITY AND ACCESS

RECOMMENDATION AND RESPONSE AS REPORTED IN DECEMBER 2006:

1. Security Program and Security and Access Controls

RECOMMENDATION

We recommend that DEQ, in conjunction with DIT, establish and implement an information systems security program and security and access controls over data and data systems.

AGENCY PRELIMINARY RESPONSE

DEQ agrees and noted that the findings identify similar security weaknesses in several of DEQ's application systems. DEQ informed us that its security committee, established early in fiscal year 2005-06, recently issued a draft information security plan. The plan contains several recommended improvements for implementing an overall information security program, including establishment of a central security function/advisory team, establishment of new policies and procedures, and ongoing risk assessment practices. DEQ will implement plan recommendations in upcoming months and will determine appropriate resource alignments necessary to achieve outcomes identified in the plan.

FOLLOW-UP CONCLUSION

DNRE and DTMB had not fully addressed 5 of the 6 conditions cited in our 2006 audit and, therefore, has only partially complied with this recommendation. A reportable condition still exists. Specifically, our follow-up disclosed:

a. DNRE had not established a security officer position or assigned the responsibility and authority to implement information security policies, standards, and operating procedures for the safeguarding of DNRE data and data systems. DNRE had drafted a security plan that included the establishment of an information security officer as well as several draft information security control policies. However, DNRE informed us that it had not yet adopted the security plan because of a lack of resources.

b. DNRE, in conjunction with DTMB, restricted system development staff access to production data. We noted that DNRE removed DTMB database administrators' and developers' privileged access to Navision, LABWORKS, and ERNIE. In addition, DNRE assigned the responsibility for administering security and access to ERNIE to the Remediation and Redevelopment Division of DNRE.

c. DNRE restricted privileged access to Navision. Also, DNRE established specific user roles and appropriately assigned the access required for those roles to all LABWORKS users.

However, DNRE did not remove user access to ERNIE for two users who had departed DNRE.

d. DNRE restricted privileged access to Navision audit logs. However, DNRE did not restrict privileged access to LABWORKS audit logs. Also, DNRE established a process to monitor Navision audit logs for unusual and inappropriate transactions and privileged access.

e. DNRE did not ensure that laboratory data changes could be made only through the LABWORKS application.

f. DNRE and DTMB did not encrypt the password files in LABWORKS. However, DNRE informed us that it is working with the vendor and DTMB to implement encrypted password files.

CHANGE MANAGEMENT

RECOMMENDATION AND RESPONSE AS REPORTED IN DECEMBER 2006:

3. Change Management Controls

RECOMMENDATION

We recommend DEQ and DIT establish effective change management controls.

AGENCY PRELIMINARY RESPONSE

DEQ and DIT agree and DEQ will work with DIT to establish appropriate controls as part of implementing an information security plan. DIT informed us that it has initiated a project to adapt its enterprise level change control process to the local change activities for its support areas. DIT also informed us that its support staff for DEQ is working with enterprise change managers to adapt and implement a Local Change Control Board with authority over DEQ information technology operations. DIT has informed us that it will achieve full compliance by September 30, 2007.

FOLLOW-UP CONCLUSION

We concluded that DNRE and DTMB had complied with this recommendation. DTMB issued a Systems Engineering Methodology (SEM) policy in June 2009 requiring DTMB and its client agencies to follow the SEM and the SEM Maintenance Guidebook for all enhancements and maintenance of existing systems. Also, DTMB established procedure 1370.00.01.01 to identify and document a process for controlling changes to information systems. Specifically, our follow-up disclosed:

a. DNRE and DTMB established change control policies and procedures and a change control board to ensure that program and data changes are properly authorized, tested, and approved before being moved to production.

b. DNRE and DTMB established appropriate segregation of duties for the change management process and removed DTMB developer access to the production source code as well as the ability to move the source code into production.

c. DNRE and DTMB implemented system tools to maintain logs of program changes that provide an audit trail and ensure that program changes are authorized and approved by management.

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL