MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT ON THE NETWORK APPLICATION SERVER CONTROLS

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

October 2010

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

084-0555-05F

> 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 26, 2010

Ms. Phyllis Mellon, Acting Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Mellon:

This is our report on our follow-up of the 4 material findings and 4 corresponding recommendations reported in the performance audit of Network Application Server Controls, Department of Information Technology (DIT). That audit report was issued and distributed in October 2006. Additional copies are available on request or at <http://www.audgen.michigan.gov>. Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB). 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 DTMB had not complied with 1 recommendation and had partially complied with 3 recommendations. A material condition still exists relating to management plans and reportable conditions exist relating to network application servers outside of the Technical Services Division's control, identification of critical network application servers, and technical policies.

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

NETWORK APPLICATION SERVER CONTROLS

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

FOLLOW-UP REPORT

NETWORK APPLICATION SERVER CONTROLS 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 Network Application Server Controls, Department of Information Technology (084-0555-05), which was issued and distributed in October 2006. That audit report included 4 material conditions (Findings 1 through 4).

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Technology, Management & Budget (DTMB) has taken appropriate corrective measures in response to the 4 material conditions and 4 corresponding recommendations.

BACKGROUND

DTMB is responsible for achieving a unified and more cost-effective approach for managing information technology among all executive branch agencies. DTMB's Technical Services Division is responsible for configuring and managing approximately 2,500 network application servers. Management and security controls over network application servers directly affect the confidentiality, integrity, and availability of data on the State's information network. DTMB's Technical Services Division and Office of Enterprise Security (OES) share responsibility for securing the State's network application servers.

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

SCOPE

Our fieldwork was performed between May and August 2010. We interviewed DTMB employees to determine the status of compliance with our audit recommendations. We reviewed policies and procedures regarding system administration, server management, and policy and procedure creation. We also reviewed position descriptions, job classifications, individual development plans, and training records of server administrators.

FOLLOW-UP RESULTS

EFFECTIVENESS OF NETWORK APPLICATION SERVER CONFIGURATION

RECOMMENDATION AND RESPONSE AS REPORTED IN OCTOBER 2006:

1. Network Application Servers Outside of Technical Services Division's Control

RECOMMENDATION

We recommend that DIT control or provide oversight of all the State's network application server resources as required by Executive Order No. 2001-3.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will control and monitor or establish written agreements and provide oversight to all of the State's network application server resources to ensure that all network application servers are configured, managed, and secured based on DIT's policies, standards, procedures, or industry best practices. DIT Technical Services Division managers will be directly responsible for DIT network application system administrators to ensure adequate oversight. DIT will transfer system administration functions and resources managed by the Agency Services Division to the Technical Services Division. DIT will work to achieve full compliance by December 31, 2007.

FOLLOW-UP CONCLUSION

DTMB did not fully address 1 of the 3 parts of our finding and did not address the other 2 parts. Therefore, DTMB had partially complied with our recommendation and a reportable condition still exists. Specifically, our follow-up disclosed:

a. DTMB transferred network application servers to its control that were previously managed by State agencies. However, DTMB had not yet ensured that servers managed by third parties are monitored, administered, and secured in a manner consistent with State standards. DTMB informed us that it is still in the process of developing a procedure to address servers managed by third parties and it is evaluating tools that can be configured to monitor servers for compliance with DTMB policies, standards, procedures, and industry best practices.

b. DTMB had not ensured that all DTMB Technical Services Division system administrators reported to DTMB Technical Services Division managers. However, DTMB informed us that it is working with the DTMB Agency Services Division for the Department of Civil Rights and the Center for Geographic Information to transfer the system administration to DTMB Technical Services Division.

c. DTMB had reduced the number of network application servers administered by the DTMB Agency Services Division. However, DTMB had not transferred the responsibility for system administration of 64 network application servers from the DTMB Agency Services Division to the DTMB Technical Services Division.

RECOMMENDATION AND RESPONSE AS REPORTED IN OCTOBER 2006:

2. Identification of Critical Network Application Servers

RECOMMENDATION

We recommend that DIT and its customer agencies establish a complete list of network application servers that are critical to State operations.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue its work with the other agencies to establish a complete list of network application servers that are critical to State operations. DIT will expand its criteria requirements for critical applications to include the security and internal control objectives of confidentiality, integrity, and availability of information and information systems. DIT informed us that a complete inventory of network application servers that are critical to State operations will be available by March 2007.

FOLLOW-UP CONCLUSION

We concluded that DTMB had partially complied with the recommendation; however, a reportable condition still exists. DTMB maintains the Configuration Management Database (CMDB), which is the central repository of applications and servers in the State. Also, DTMB identified the applications that are associated with critical State services and the network application servers upon which those applications reside. In addition, DTMB defined the service criticality for all servers in the State's infrastructure. Service criticality is how quickly an agency requires

DTMB to restore the availability of a server and the impact of the server on the business of the agency. However, DTMB had not assessed the confidentiality and integrity of data residing on all network application servers. Evaluating service criticality in conjunction with confidentiality and integrity will help ensure that DTMB establishes a complete list of network application servers that are critical to State operations. DTMB informed us that it has several processes in place that help assess confidentiality and integrity of system data and it will use these processes to document criticality ranking in the CMDB.

EFFECTIVENESS OF POLICIES AND PROCEDURES

RECOMMENDATION AND RESPONSE AS REPORTED IN OCTOBER 2006:

3. Technical Policies

RECOMMENDATION

We recommend that DIT establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that complement the State's technology architecture plan to create an enterprise-wide system and comply with Control Objectives for Information and Related Technology (COBIT) standards.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue to work to establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that comply with COBIT standards. DIT Enterprise Architecture (in conjunction with the Office of Enterprise Security and the Technical Services Division) will update existing technical policies that align with DIT's adoption of the *Secure Michigan Initiative* and COBIT by June 30, 2007. DIT informed us that training is an ongoing commitment and COBIT training will be held for the Technical Services Division by June 30, 2007. DIT will work to achieve full compliance by December 31, 2007.

FOLLOW-UP CONCLUSION

DTMB did not fully address 3 of the 5 parts of our finding. Therefore, DTMB had partially complied with our recommendation and a reportable condition still exists. Specifically, our review disclosed:

a. DTMB had not established and implemented system administration policies and procedures recommended by COBIT, the National Institute of Standards and Technology, and the International Standards Organization in areas such as policy communication, defined roles and responsibilities for system administrators, server security certification and accreditation, server reaccreditation, and security training and education.

b. DTMB established a quality assurance team to review, evaluate, and rewrite technical policies and procedures. Also, DTMB developed a draft procedure for creating, updating, and rescinding policies, standards, and procedures.

c. DTMB made available and communicated its approved server security policies to server teams.

d. DTMB did not train all its Technical Services Division staff on COBIT standards. However, DTMB provided COBIT foundation training to the quality assurance team and technical service system managers in August 2010.

e. DTMB did not conduct periodic technical security training for system administrators. However, system administrators received introductory server administration security training from the Office of Enterprise Security and system administration training related to specific platforms from vendors.

EFFECTIVENESS OF MANAGEMENT PLANS

RECOMMENDATION AND RESPONSE AS REPORTED IN OCTOBER 2006:

4. Management Plans

RECOMMENDATION

We recommend DIT define its future operating environment and develop an implementation plan to achieve it.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue to define its operating environment and implement action plans that ensure current initiatives address the challenges of establishing an effective and efficient system administration function to support the State's network application servers. DIT informed us that it has launched the Technical Services Optimization project which, in May 2006, established senior standards and the core classification (including job duties and position descriptions) for the Technical Services Division. In addition, DIT informed us that, during the past nine months, it has completed 64% of all Technical Services Division individual development plans and that the remaining 36% will be completed by March 2007. DIT will partner with the Department of Civil Service to further refine the current information technology classification and compensation system. DIT will work to achieve full compliance by December 31, 2007.

FOLLOW-UP CONCLUSION

DTMB did not fully address 4 of the 6 parts of our finding. Therefore, DTMB has not complied with the recommendation and a material condition still exists. Specifically, our review disclosed:

a. DTMB defined in position descriptions the detailed technical competencies to perform the system administration function. However, DTMB had not defined the detailed security competencies.

b. DTMB defined the job classification structure and the specific duties and responsibilities for current information technology job classifications. Also, DTMB created position descriptions to define the required knowledge, skills, and abilities for server administration, but, did not include the knowledge, skills, and abilities for server security administration.

c. DTMB did not complete up-to-date and accurate position descriptions for all system administrators. However, DTMB informed us that it is in the process of creating approved specialist position descriptions.

d. DTMB did not complete a gap analysis between the skills needed and the skills currently available for the system administration function.

e. DTMB prepared individual development plans for system administrators.

f. DTMB did not complete a technical training curriculum for the server support job role.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL