MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

QUALIFIED VOTER FILE AND DIGITAL DRIVER'S LICENSE SYSTEMS

DEPARTMENT OF STATE AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

September 2010

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

231-0591-04F

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

September 10, 2010

The Honorable Terri Lynn Land
Secretary of State
Richard H. Austin Building
Lansing, Michigan
and
Mr. Kenneth D. Theis, Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Secretary Land and Mr. Theis:

This is our report on our follow-up of the 2 material conditions (Findings 1 and 2) and 2 corresponding recommendations reported in the performance audit of the Qualified Voter File (QVF) and Digital Driver's License (DDL) Systems, Department of State and Department of Information Technology (DIT). That audit report was issued and distributed in March 2005. Additional copies are available on request or at <http://www.audgen.michigan.gov>. In March 2010, 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 the Department of State and DTMB had partially complied with the 2 recommendations. However, a material condition still exists relating to QVF database server security and a reportable condition still exists relating to security concerns with the DDL contract.

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

QUALIFIED VOTER FILE AND DIGITAL DRIVER'S LICENSE SYSTEMS
DEPARTMENT OF STATE AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
FOLLOW-UP REPORT

QUALIFIED VOTER FILE AND DIGITAL DRIVER'S LICENSE SYSTEMS DEPARTMENT OF STATE 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 the Qualified Voter File (QVF) and Digital Driver's License (DDL) Systems, Department of State and Department of Information Technology (DIT) (23-591-04), which was issued and distributed in March 2005. That audit report included 2 material conditions (Findings 1 and 2).

PURPOSE OF FOLLOW-UP

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

BACKGROUND

The Department of State operates the QVF System in order to maintain a single Statewide database of registered voters. It also operates the DDL System to electronically record, store, and query images and signatures of Michigan drivers and personal identification card applicants. DTMB provides services to the Department of State. These services include such things as security, server operation and administration, and network communications.

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 by a Type III transfer and abolished DIT.

SCOPE

Our fieldwork was performed between February and May 2010. We interviewed employees from the Department of State and DTMB to determine the status of compliance with our audit recommendations. We reviewed QVF database configuration tables, QVF System security assessment, DTMB policy and procedures, industry best practices, and a recent Office of the Auditor General audit of server security. We also reviewed the contract, monitoring practices, and security plan for the DDL System.

FOLLOW-UP RESULTS

EFFECTIVENESS IN CONTROLLING ACCESS TO THE CENTRAL QVF SYSTEM DATABASE SERVER

RECOMMENDATION AND RESPONSE AS REPORTED IN MARCH 2005:

1. QVF Database Server Security

RECOMMENDATION

We recommend that the Departments effectively secure the QVF database server.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and DIT agreed with the finding.

The Departments have continued to work together to evaluate and implement reasonable and cost-effective strategies that mitigate the level of risk to the State's QVF database server. The Departments informed us that they have developed a security plan consistent with the State's security guidelines and have already corrected significant vulnerabilities identified with the existing configuration.

Additional security measures are also being reviewed. The Departments also informed us that despite these vulnerabilities, they were not aware of any instances in which the confidentiality, integrity, and availability of QVF information was compromised.

FOLLOW-UP CONCLUSION

The Department of State and DTMB have made significant improvements in the overall security of the QVF database. These improvements have reduced the overall security risk; however, additional improvements are needed. Based on the remaining work to be completed, we have concluded that the Department of State and DTMB have partially complied with this recommendation. However, the remaining vulnerabilities and control weaknesses indicate that a material condition still exists.

While performing our procedures, we reported the detailed results of our review to management. However, for security purposes, this report only summarizes the conditions we identified. Specifically, our follow-up disclosed:

a. In May 2006, DTMB completed its move of the QVF production database server away from direct exposure to the Internet. Moving the server away from direct exposure reduces the risk to the QVF production database from Internet-based threats.

b. DTMB has not implemented several critical controls needed to maintain the security of the QVF production database. Although DTMB has remediated some vulnerabilities, other database and operating system vulnerabilities remain.

c. In March 2006, the Department of State and DTMB prepared a security assessment of the proposed design changes to the QVF network architecture. The Departments' assessment categorized the confidentiality, integrity, and availability risk as "high" for the QVF System. The high-risk security classification required the implementation of 18 recommendations that were included in the assessment. One such recommendation required the Office of Enterprise Security (OES) to conduct annual security reviews of the QVF System. However, OES informed us that these annual security reviews have not occurred since the assessment was completed in March 2006. These annual security reviews would have provided management with timely information needed to monitor the implementation of our prior audit recommendations and the other 17 security assessment recommendations. OES asserted that it does not have sufficient resources to conduct the annual security reviews.

EFFECTIVENESS IN MONITORING CONTRACTOR'S EFFORTS TO SECURE THE DDL SYSTEM

RECOMMENDATION AND RESPONSE AS REPORTED IN MARCH 2005:

2. Security Concerns With DDL Contract

RECOMMENDATION

We recommend that the Departments ensure that the third-party contractor effectively secures the DDL System.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and DIT agreed with the finding.

The Department of State, in consultation with DIT, has continued to work with the third-party contractor to effectively secure the DDL System. The Departments informed us that as part of this effort, a special physical security review was conducted late in 2004 and discussions are continuing on additional monitoring requirements. In addition, the Departments will compare the existing security arrangements with the State's information security standards and will continue to work with the Department of Management and Budget to ensure future contracts routinely provide language which ensures that the security standard is upheld. The Departments also informed us that despite the noted risks, they were not aware of any instances in which the confidentiality, integrity, and availability of DDL System information was compromised.

FOLLOW-UP CONCLUSION

The Departments have not fully addressed 2 of the 3 conditions cited in this finding and, therefore, have only partially complied with the recommendation to ensure that the third-party contractor effectively secures the DDL System. A reportable condition still exists. Specifically, our follow-up disclosed:

a. The Departments did not evaluate the effectiveness of security and internal controls in their monitoring of the third party contractor's management of the DDL System. Specifically, the Departments did not obtain independent certification and accreditation of security and internal controls over the DDL

System. However, the Departments informed us that the contractor will be moving the location of the DDL System in fall 2010 and that the security for the system at the new location has been reviewed and independently certified.

b. The Departments made significant efforts to establish an information security plan for the DDL System, but the efforts were not complete. The Departments incorporated a security plan developed by the contractor for the DDL System into the service contract. The Departments also worked with the contractor to identify and document the controls in a security assessment (Form DIT-0170). However, the Departments had not identified, documented, and evaluated the security risk based on those controls in the security assessment.

c. The Departments ensured that the third-party DDL System contract language included a detailed security plan and monitoring practices.

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