MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY

June 2007

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

231-0590-03F

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

June 8, 2007

The Honorable Terri Lynn Land
Secretary of State
Richard H. Austin Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Secretary Land and Ms. Takai:

This is our report on our follow-up of the 6 material findings (Findings 1 through 6) and 6 corresponding recommendations reported in the performance audit of the Automated Information Systems, Department of State and Department of Information Technology. That audit report was issued and distributed in August 2004; however, additional copies are available on request or at <http://www.audgen.michigan.gov>.

Our follow-up disclosed that the Department of State and the Department Information Technology had generally complied with 1 recommendation and had partially complied with 5 recommendations.

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

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY
FOLLOW-UP REPORT

	Page
Report Letter	1
Introduction	4
Purpose of Follow-Up	4
Background	4
Scope	5
Follow-Up Results	6
Effectiveness of General Controls	6
1. Comprehensive Information Systems Security Program	6
2. Organizational Controls	7
3. Access to System Account	9
4. Access to Mainframe Information System Files	10
5. Access to Mainframe Information Systems	11
6. Program and Data Change Controls	12

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF STATE AND
DEPARTMENT OF INFORMATION TECHNOLOGY
FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material findings and corresponding recommendations and the agency's preliminary response as reported in our performance audit of the Automated Information Systems, Department of State and Department of Information Technology (23-590-03), which was issued and distributed in August 2004. That audit report contained 6 material conditions (Findings 1 through 6).

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of State and the Department of Information Technology had taken appropriate corrective measures in response to the 6 material findings and 6 corresponding recommendations.

BACKGROUND

The mission of the Department of State is to continually improve customer service using innovation and new technology. The Department serves the citizens of Michigan with programs designed to enhance driver safety, protect automotive consumers, and ensure the integrity of the motor vehicle administration system and the Statewide elections process.

The Department of State developed and operates large complex information systems to manage driver vehicle information, vehicle-licensing records, vehicle violations, and fee collections.

The Department of Information Technology is responsible for maintaining and supporting the information technology (IT) infrastructure for the Department of State. In

addition, the Department of Information Technology provides technical support for Department of State application development and maintenance, database management, and help desk services.

SCOPE

Our fieldwork was performed during February and March 2007. We interviewed security personnel, IT development managers, and internal auditors at the Department of State. We reviewed the policies and procedures related to the comprehensive information security program, organizational controls, access to mainframe information system files, access to mainframe information systems, and program and data change controls. We tested compliance with selected policies and procedures.

FOLLOW-UP RESULTS

EFFECTIVENESS OF GENERAL CONTROLS

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

1. Comprehensive Information Systems Security Program

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology continue their efforts to fully implement a comprehensive information systems security program.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding for the time period covered by this performance audit and will continue with their efforts to fully implement a comprehensive security program. As noted by the Office of the Auditor General, in January 2003, the Department of Information Technology initiated the *Secure Michigan Initiative*, which identifies a comprehensive information security program including six high priority steps to address the Departments' primary information system security risks. As part of this program, in December 2003, the Department of State established an information security function which is intended to complement the efforts of the Department of Information Technology. Also, the two Departments are proceeding with the development of a new automated information system intended to support Department of State business processes into future years. A mandatory requirement of this new information system is security over the customers' records. The implementation phase of this project is expected to begin in fiscal year 2004-05.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had partially complied with this recommendation.

The Departments had not fully implemented the recommendations of the *Secure Michigan Initiative* or the recommendations discussed in Findings 2 through 6. However, the Departments have taken steps to improve the security of the mainframe information systems through development of policies and procedures,

establishment of an independent security officer function within the Department of State, reduction of access to critical production and mainframe system resources, adoption of the Control Objectives for Information and Related Technology (COBIT) security and controls framework, and completion of periodic disaster recovery tests and some risk assessments. In addition, the Departments developed a security system that monitors access to mainframe information system files.

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

2. Organizational Controls

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective organizational controls to support mainframe information systems.

AGENCY PRELIMINARY RESPONSE

Both the Department of State and the Department of Information Technology agree with the finding for the period covered by the audit. The Departments informed us that since November 2003 organizational controls have been enhanced as the Department of State has now established an information security function and a service level agreement has been finalized that identifies the conditions and expectations of the two Departments regarding the delivery of IT services.

In addition, the Department of State and the Department of Information Technology will plan to continue to use widely accepted control objectives in evaluating IT activities and will work to further integrate these concepts into building and managing systems, formalizing additional policies and procedures when needed. The Departments will also continue to explore and offer training opportunities to better enable staff with necessary skills associated with information system security and controls.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had partially complied with this recommendation. Specifically, our follow-up disclosed:

a. The Departments still had incompatible job functions assigned to IT development staff. Also, the Department of Information Technology development staff still acted as security administrators for the job-scheduling and program change control systems. However, the Department of Information Technology transferred the Statewide management of the mainframe security system from Department of Information Technology Agency Services to the Department of Information Technology Data Center Operations. Also, the Department of State created the Bureau of Information Security which took responsibility for a majority of the security officer and administrator functions including monitoring access to the mainframe production systems.

b. The Departments adopted COBIT as its framework for IT security and controls.

c. The Departments had not provided technical security administration training to those individuals responsible for managing the mainframe's file system, database management system, user account system, job-scheduling system, program change control system, and transaction control system.

d. The Departments had not developed controls to monitor privileged activity and security for the program change control system. However, the Departments developed procedures and reports to monitor privileged activity and security of some of the mainframe systems.

e. The Departments established a service level agreement to ensure compliance with Executive Order No. 2001-3. The service level agreements defined the responsibilities, expectations, and processing needs of the Department of State.

f. The Departments had not completely developed security policies and procedures for administering and monitoring activity on the mainframe's file system and database management system. However, the Departments had

established some procedures to manage certain IT security functions, such as access to the mainframe production systems and the mainframe security system.

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

3. Access to System Account

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology control access to the critical production system account and job-scheduling utility.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with this finding and have informed us that they have taken steps to limit access to the critical production system account and job-scheduling utility to appropriate staff. Additional security procedures to protect against this access risk will be accomplished by December 2004.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had partially complied with this recommendation.

The Departments still had not established effective controls or established a policy and procedure governing the administration of and access to the job-scheduling utility.

In addition, some Department of Information Technology users not directly responsible for job scheduling still had access to the critical production system account and job-scheduling utility. However, the Departments reduced the number of users with access to critical production system accounts and the job-scheduling utility.

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

4. Access to Mainframe Information System Files

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective access controls over mainframe information system files.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding and will establish new controls to limit the access to confidential mainframe information system files by December 2004. Despite the risks associated with having this monitored by IT staff during this transition period, the Departments are not aware of any instances in which the confidentiality, integrity, and availability of information system resources was inappropriately compromised.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had partially complied with this recommendation. Specifically, our follow-up disclosed:

a. Although the Departments reduced the number of users with access to the Department of State's mainframe production databases, excessive access still exists. This condition could compromise the integrity and security of the Department of State's information systems.

   In addition, although the Departments developed an informal process to authorize access to the mainframe production databases, they did not ensure that authorization was documented, maintained, and periodically reviewed for appropriateness.

b. The Departments still had not established effective access controls over mainframe application files. However, the Departments developed a security monitoring report that goes to the Department of State security administrator for review.

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

5. Access to Mainframe Information Systems

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective access controls over mainframe production information systems.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding. The Departments informed us that access rights for staff in both Departments have been analyzed and updated in a special project completed since November 2003. Also, both Departments will continue to work together to establish policies and procedures, based on business risk assessments, to limit access to mainframe production information systems by March 2005.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had partially complied with this recommendation. Specifically, our follow-up disclosed:

a. The Departments had not developed procedures governing access to the mainframe databases. However, the Departments had developed detailed procedures governing access to the mainframe production systems and high-level procedures governing access to the mainframe security system.

b. The Departments had not completed risk assessments for all critical mainframe information systems. However, the Departments had conducted risk assessments on some of the mainframe production information systems.

c. The Departments restricted access to the mainframe production information systems to only users with a business need.

RECOMMENDATION AND RESPONSE AS REPORTED IN AUGUST 2004:

6. Program and Data Change Controls

RECOMMENDATION

We recommend that the Department of State and the Department of Information Technology establish effective program and data change controls.

AGENCY PRELIMINARY RESPONSE

The Department of State and the Department of Information Technology agree with the finding. The Departments informed us that procedures now require that only project managers, assigned by the business owner, have the authority to authorize "project-related" program releases. In addition, the Departments will review and revise additional procedures that ensure appropriate controls are maintained over program and data changes by October 2004.

FOLLOW-UP CONCLUSION

We concluded that the Department of State and Department of Information Technology had generally complied with this recommendation. Specifically, our follow-up disclosed:

a. The Departments implemented change control procedures to ensure that only authorized program changes or data fixes were initiated.

b. The Departments established a technical review board and a change control board that provide oversight to ensure that program and data changes are properly authorized, tested, and approved before being moved to production.

c. The Departments established controls to ensure the security and integrity of program versions through upgrades to the program change control system.

d. The Departments reduced access and authorization capability in the program change control system. However, Department of Information Technology staff still had excessive access to the program change control system that could allow staff to circumvent the program and data change control process.

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL