MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF TREASURY

March 2005

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

27-590-01F

"...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 may 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 22, 2005

Mr. Jay B. Rising
State Treasurer
Treasury Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Mr. Rising and Ms. Takai:

This is our report on our follow-up of the 6 material findings (Findings 1 through 6) and 6 related recommendations reported in the performance audit of the Automated Information Systems, Department of Treasury. That audit report was issued and distributed in June 2003; however, additional copies are available on request or at <http://www.audgen.michigan.gov>. Subsequent to our original audit, Executive Order No. 2001-3 transferred the responsibility for all information technology services to the Department of Information Technology.

Our follow-up disclosed that the Department of Treasury has complied with the 6 recommendations. Of the 5 recommendations related to the Department of Information Technology, it has complied with 4 recommendations and has partially complied with 1 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

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF TREASURY
FOLLOW-UP REPORT

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF TREASURY
FOLLOW-UP REPORT

INTRODUCTION

This report contains the results of our follow-up of the material findings and related recommendations and the agency's preliminary response as reported in our performance audit report of the Automated Information Systems, Department of Treasury (#2759001), which was issued and distributed in June 2003. That audit report included 6 material findings (Findings 1 through 6) and no other reportable conditions.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Treasury and the Department of Information Technology (DIT) have taken appropriate corrective measures in response to the 6 material findings and 6 related recommendations.

BACKGROUND

Subsequent to our original audit, Executive Order No. 2001-3 transferred the responsibility for all information technology services to DIT. The mission of DIT is to provide effective solutions, through skilled and valued employees, in its partnership with the Department of Treasury. DIT is responsible for providing data processing services to the Department. The Department, as the business owner, retains responsibility for all agency business applications. In addition, the Department retains ownership of all data processed through any systems developed in conjunction with DIT.

SCOPE

We interviewed security officers, information technology (IT) development managers, database administrators, operations support managers, and internal auditors at the

Department of Treasury and DIT. We reviewed the policies and procedures drafted to address information systems security, organizational controls, access to the system account, access to information system files, access to tax systems, and program and data change controls. We tested the Department's and DIT's compliance with selected policies and procedures.

FOLLOW-UP RESULTS

EFFECTIVENESS OF ACCESS CONTROLS

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

1. Comprehensive Information Systems Security Program

RECOMMENDATION

WE AGAIN RECOMMEND THAT THE DEPARTMENT ESTABLISH A COMPREHENSIVE INFORMATION SYSTEMS SECURITY PROGRAM.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation. With Executive Order No. 2001-03, the Governor created DIT. The Department informed us that in June 2002, the director established the Office of Security and Disaster Recovery and appointed the first chief enterprise security officer who reports directly to the State Chief Information Officer. The Department also informed us that, since then, the chief enterprise security officer and his staff performed a rapid risk assessment and published the Secure Michigan Initiative, which compiles:

- Primary vulnerabilities within all State departments;
- Six immediate strategies that mitigate those vulnerabilities;
- Many other quick-hit, low-cost remedies to improve the security of the State's data and systems; and
- Data that will help direct each department to target its own weaknesses.

The Department appointed a security officer in August 2002. The Department's security officer will develop security policies and guidelines supportive of the Statewide requirements and compliant with Department statutes and regulations by September 2003.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury has complied and DIT has partially complied with this recommendation.

Both the Department of Treasury and DIT have demonstrated a high level of commitment and support to improve the security of the Department's mainframe information systems. The leadership and partnership of both the Department's Office of Security and DIT's Agency Services have resulted in significant improvements in the controls over access to mainframe information systems. These improvements include raising security awareness among employees, establishing extensive information security policies and procedures, and defining roles and responsibilities for the security of information systems. These improvements, if adopted into ongoing day-to-day business operations, will facilitate efforts to protect the confidentiality, integrity, and availability of taxpayer data.

In addition, the Department, DIT, and the Department of Management and Budget have partnered to enhance the biennial internal control evaluation of the State's critical information systems. The enhancement is based on the Control Objectives for Information and Related Technology (COBIT) framework outlined by the Information Systems Audit and Control Foundation to manage, use, and audit information technology. COBIT consists of 34 high-level control objectives associated with primary information technology processes, grouped into four domains. The four domains are planning and organization, acquisition and implementation, delivery and support, and monitoring. It is expected that the results of these evaluations will aid in risk management and the design of superior business processes.

DIT has made progress toward creating a Statewide IT security risk management program. DIT has adopted COBIT as a framework for IT security and control. In addition, DIT has established a charter for its Office of Enterprise Security with responsibility to manage and mitigate security risks and vulnerabilities. Further, DIT has started to conduct risk assessments for new IT system projects.

However, the extent of the State's success in securing its information resources will be limited if DIT does not implement several critical recommendations from its own Secure Michigan Initiative. These recommendations are the basis for creating an

effective IT security risk management program throughout State government. These recommendations include establishing a State policy and standard that requires security risk management and a formal security risk management program for conducting risk assessments and creating risk mitigation plans for all IT systems. IT security risk management is one of the six "immediate strategies" that are compiled in the Secure Michigan Initiative, as mentioned in the agency preliminary response.

Without an effective Statewide IT security risk management program, the State cannot ensure that the threats and vulnerabilities to all of its information systems and resources are reduced to an acceptable level. We concur with the State's chief information security officer's warning that "If the recommendations in this report [Secure Michigan Initiative] are not acted upon, state government IT systems face very serious consequences and risks." According to the Secure Michigan Initiative some of the more serious consequences and risks include the inability to identify a security breach, loss in reputation and public confidence, and unauthorized access to data resulting in federal and State statute violations.

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

2. Organizational Controls

RECOMMENDATION

We recommend that the Department establish effective organizational controls to support its critical information systems.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve further compliance by June 2003. Both the Department and DIT will work together to ensure that appropriate organizational controls are put in place. Both the Department and DIT expressed concern that budget limitations may hinder their efforts to provide needed training to IT security and other department employees.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury and DIT have complied with this recommendation.

The Department of Treasury and DIT have implemented policies and procedures that reassign IT operational support and security functions to individuals independent of IT development. The Department and DIT have also implemented policies and procedures that assign responsibility for maintaining the security of the Department's information systems. The Department and DIT both have adopted COBIT as a framework for security and control of information technology. The Department has implemented a comprehensive IT security/control training program to administer the security of the Department's information systems.

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

3. Access to System Account

RECOMMENDATION

We recommend that the Department control access to the critical production system account.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and will comply with the recommendation by April 30, 2003. Both the Department and DIT will work together to control access to critical production system accounts.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury and DIT have complied with this recommendation.

The Department of Treasury and DIT have implemented policies and procedures that control access to the Department's production system account and DIT's critical job-scheduling utility. During our follow-up, we confirmed that the Department and DIT had limited IT developer access to the production system account to an appropriate level.

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

4. Access to Department Information System Files

RECOMMENDATION

We recommend that the Department establish effective access controls to its mainframe information system files.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by September 30, 2003. Both the Department and DIT will work together to establish effective access controls to department mainframe information systems files.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury and DIT have complied with this recommendation.

The Department of Treasury and DIT have implemented policies and procedures that restrict and control access to the Department's mainframe production databases and application disk files. Further, the Department and DIT have removed inappropriate access to mainframe production databases and have established processes to monitor compliance with the Department's security standards.

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

5. Access to Tax Systems

RECOMMENDATION

We recommend that the Department establish effective access controls to its production tax and other information systems.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by

June 30, 2003. Both the Department and DIT will work together to establish effective access controls to its tax and other information systems.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury has complied with this recommendation.

The Department of Treasury has implemented policies and procedures that provide a framework to control access to the individual income tax system and to monitor the activity of privileged security administrators. Further, the Department has established an audit trail and a process to monitor access to the individual income tax database. The Department indicated that it will continue to develop monitoring processes for other confidential data that the Department maintains in its databases.

The Department of Treasury has established policy and reviewed the risks related to transactions used to access the Department's information systems. Further, the Department's policy limits DIT developers' access to tax systems to the extent necessary to perform their job functions.

RECOMMENDATION AND RESPONSE AS REPORTED IN JUNE 2003:

6. Program and Data Change Controls

RECOMMENDATION

We recommend that the Department establish effective program and data change controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by June 30, 2003. Both the Department and DIT will work together to establish effective program and data change controls.

FOLLOW-UP CONCLUSION

We concluded that the Department of Treasury and DIT have complied with this recommendation.

The Department of Treasury and DIT implemented in policy and procedure the program and data change process. The Department and DIT no longer allow DIT developers to have unrestricted and unmonitored access into program code libraries and production data. The Department and DIT have designed an environment in which management can provide reasonable assurance that program and data changes will be properly authorized, tested, and approved before they are promoted to the production environment.

This page left intentionally blank.


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL