MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

MICHIGAN DEPARTMENT OF TRANSPORTATION ARCHITECTURE PROJECT, USER APPLICATION AND REGISTRATION SYSTEM, BID EXPRESS SYSTEM, AND CONSTRUCTION RELATED SYSTEMS

MICHIGAN DEPARTMENT OF TRANSPORTATION AND
DEPARTMENT OF INFORMATION TECHNOLOGY

July 2007

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

591-0590-06

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

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Michigan Department of Transportation Architecture Project, User Application and Registration System, Bid Express System, and Construction Related Systems

Michigan Department of Transportation(MDOT) and Department of Information Technology (DIT)

Report Number:
591-0590-06

Released:
July 2007

MDOT maintains and operates over 250 information systems that process and store data to assist MDOT in providing transportation services. DIT provides information support services to MDOT for Michigan Department of Transportation Architecture Project (MAP), User Application and Registration System (UARS), and construction related systems, including operating system configuration, application development and maintenance, database administration, and physical security. MDOT contracts with a third-party contractor to administer the Bid Express System.

Audit Objective:

To assess the effectiveness of MDOT and DIT's security and access controls over selected information systems.

Audit Conclusion:

MDOT and DIT's security and access controls over selected information systems were not effective. We noted one material condition (Finding 1) and five reportable conditions (Findings 2 through 6).

Material Condition:

MDOT had not established and implemented a comprehensive information systems security program (Finding 1).

Reportable Conditions:

DIT had not established effective security controls over the server operating systems (Finding 2).

DIT had not established effective security and access controls over MAP Financial Obligation System, MAP Project Information System, Project Accounting and Billing System, Trns*port, and UARS databases (Finding 3).

MDOT and DIT did not effectively plan for and implement effective security controls over UARS (Finding 4).

MDOT had not established effective access controls over its non-Web-based information systems (Finding 5).

DIT had not established effective physical security controls over network resources (Finding 6).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:

To assess the effectiveness of MDOT and DIT's efforts to ensure the integrity of data for selected information systems.

Audit Conclusion:

MDOT and DIT were moderately effective in their efforts to ensure the integrity of data for selected information systems. We noted two reportable conditions (Findings 7 and 8).

Reportable Conditions:

MDOT did not implement data edits to ensure the integrity of MAP and Trns*port data (Finding 7).

MDOT did not ensure that system audit trails provide complete identifying information about each transaction in Trns*port (Finding 8).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 8 findings and 8 corresponding recommendations. MDOT's and DIT's preliminary responses indicate that they agree with all of the recommendations and will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

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

July 3, 2007

Mr. Ted B. Wahby, Chair
State Transportation Commission
and
Kirk T. Steudle, P.E., Director
Michigan Department of Transportation
Murray Van Wagoner Transportation Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Wahby, Mr. Steudle, and Ms. Takai:

This is our report on the performance audit of the Michigan Department of Transportation Architecture Project, User Application and Registration System, Bid Express System, and Construction Related Systems, Michigan Department of Transportation and Department of Information Technology.

This report contains our report summary; description of systems; audit objectives, scope, and methodology and agency responses and prior audit follow-up; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

MICHIGAN DEPARTMENT OF TRANSPORTATION ARCHITECTURE PROJECT, USER APPLICATION AND REGISTRATION SYSTEM, BID EXPRESS SYSTEM, AND CONSTRUCTION RELATED SYSTEMS
MICHIGAN DEPARTMENT OF TRANSPORTATION AND DEPARTMENT OF INFORMATION TECHNOLOGY

GLOSSARY

Michigan Department of Transportation (MDOT)

MDOT maintains and operates over 250 information systems that process and store data to assist MDOT in providing transportation services.

The major systems that we reviewed include:

a. MDOT Architecture Project (MAP)

MAP is a database repository that stores data related to MDOT's construction projects including State trunkline capital improvement projects and local improvement projects that receive federal aid. MAP provides the foundation for MDOT's strategic information systems, including MAP Financial Obligation System and MAP Project Information System. Approximately 30 other systems access MAP to read or update data.

b. User Application and Registration System (UARS)

UARS is a single sign-on system for approximately 23 MDOT Web-based information systems. UARS enables MDOT to efficiently manage user log-ins for the 23 systems. UARS allows a user to enter one usercode and password to access all the Web-based systems for which they were granted access.

c. Bid Express System

The Bid Express System is an on-line information service used by contractors to bid on MDOT's construction projects. MDOT uses the Bid Express System to advertise construction projects that are up for bid to the contracting community and to receive on-line secure bid submission from the contracting community. MDOT contracts with a third-party contractor to administer the Bid Express System.

d. Construction Related Systems

MDOT uses several automated systems to process data for its road and bridge construction projects:

(1) FieldManager

FieldManager is a construction management system used by MDOT to monitor and review the work activities that occur throughout the life of each

road, bridge, and airport construction project. MDOT's region offices and transportation service centers, local government agencies, and construction contractors use FieldManager. FieldManager automates the recording and processing of MDOT's construction activities, such as inspectors' daily reports, daily diaries, work items progress, contract modifications, material usage, stockpile management, project finalization, and contractor payments. FieldManager was developed for MDOT in 1995 by a software consulting firm. MDOT processes approximately $1.5 billion annually through FieldManager for road, bridge, and airport construction projects.

(2) Finance Daily Update (FINDLYUP)

FINDLYUP is a 30-year-old mainframe system that MDOT uses to prepare federal and local billing documents for highway and aeronautic funded projects. In the future, MDOT will replace FINDLYUP with the Project Accounting and Billing System (PAB).

(3) MAP Financial Obligation System (MFOS)

MFOS automates MDOT's process of obtaining and obligating Federal Highway Administration authorization and funding for highway projects. MFOS contains information to assist MDOT in monitoring all highway funding sources. MDOT plans to enhance MFOS to also provide functionality to obligate and monitor funding for aeronautics and public transportation projects. During the fiscal year ended September 30, 2006, MFOS processed approximately $3.7 billion.

(4) MAP Project Information System (MPINS)

MPINS is a project management system that MDOT uses to track the scope, schedule, and budget of construction jobs. Planning for all construction jobs is initiated in MPINS. MPINS provides central and region office access to project related information from initial project scoping through design. MPINS collects project information that is needed to track a job and to expend capital by assigning a job number. MDOT implemented MPINS in 1996. MPINS manages and monitors approximately $1.5 billion for construction projects annually.

(5) Project Accounting and Billing System (PAB)

PAB is an information system used to process and maintain accounting and billing records for highway and aeronautics funded projects. MDOT uses PAB to record project expenditures and revenues and maintain project transaction history and balances. PAB accounting functions were implemented in June 2005. In the future, PAB billing functions will replace FINDLYUP for highway and aeronautics funded projects. During the fiscal year ended September 30, 2006, FINDLYUP and PAB together processed approximately $4.3 billion in expenditure, revenue, and billing transactions.

(6) Trns*port

Trns*port is a series of related, automated systems for managing construction projects that perform functions such as price and quantity estimates, funding, proposal preparation, contractor prequalification and certification, letting, and field office construction activities including contractor payments and project history. Trns*port contains data related to MDOT's approximately 2,200 construction projects in process. MDOT's central office, region offices, transportation service centers, design consultant companies, and construction contractors use Trns*port. Trns*port is licensed by the American Association of State Highway and Transportation Officials.

Department of Information Technology (DIT)

DIT provides information support services to MDOT for MAP, UARS, and construction related systems, including operating system configuration, application development and maintenance, database administration, and physical security.

Audit Objectives

Our performance audit* of the Michigan Department of Transportation Architecture Project (MAP), User Application and Registration System (UARS), Bid Express System, and construction related systems, Michigan Department of Transportation (MDOT) and Department of Information Technology (DIT), had the following objectives:

1. To assess the effectiveness* of MDOT and DIT's security and access controls over selected information systems.

2. To assess the effectiveness of MDOT and DIT's efforts to ensure the integrity* of data for selected information systems.

Audit Scope

Our audit scope was to examine the information processing and other records related to the Michigan Department of Transportation Architecture Project, User Application and Registration System, Bid Express System, and construction related systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances. Our audit procedures, conducted from May 2006 through January 2007, generally covered the period December 1, 2003 through January 31, 2007.

Audit Methodology

To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We identified MDOT's information systems and performed a risk assessment* of selected systems to determine those with a high risk* to MDOT operations. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

* *See glossary at end of report for definition.*

2. Detailed Analysis and Testing Phase

We performed an assessment of general and application controls over selected information systems. Specifically, we assessed:

a. Security and Access Controls:

(1) We examined and tested user identification and password controls over construction related systems such as FieldManager, Finance Daily Update (FINDLYUP), MAP Financial Obligation System (MFOS), MAP Project Information System (MPINS), Project Accounting and Billing System (PAB), and Trns*port.

(2) We examined and tested user access permissions for FieldManager, FINDLYUP, MFOS, MPINS, PAB, and Trns*port.

(3) We reviewed and assessed the oversight of Bid Express System security.

(4) We reviewed and assessed Web application security over UARS.

(5) We reviewed and assessed controls over data, physical security, database management controls, operating system, and security management.

(6) DIT Office of Enterprise Security performed a vulnerability* scan of the network operating systems for FieldManager, MFOS, MAP, MPINS, PAB, Trns*port, and UARS. We evaluated and validated the results of the vulnerability scans and performed additional tests of the operating systems.

b. Integrity of Data:

(1) We reviewed and assessed controls over data transfers for FieldManager, MFOS, MPINS, PAB, and Trns*port.

* *See glossary at end of report for definition.*

(2) We analyzed selected data fields to determine their accuracy and completeness for MFOS, MPINS, PAB, and Trns*port.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

We use a risk and opportunity based approach when selecting activities or programs to be audited. Accordingly, our audit efforts are focused on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. By design, our limited audit resources are used to identify where and how improvements can be made. Consequently, our performance audit reports are prepared on an exception basis.

Agency Reponses and Prior Audit Follow-Up

Our audit report contains 8 findings and 8 corresponding recommendations. MDOT's and DIT's preliminary responses indicate that they agree with all of the recommendations and will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Departments to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

We released our prior performance and financial related audit of the Automated Information Systems, Michigan Department of Transportation (59-590-99), in July 2000. Within the scope of this audit, we followed up 8 of the 28 recommendations. MDOT complied with 1 of the 8 prior audit recommendations, 2 prior audit recommendations were repeated, and 5 prior audit recommendations were rewritten for inclusion in this audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

SECURITY AND ACCESS CONTROLS

COMMENT

Background: Security controls include the implementation of policies, procedures, and guidelines to ensure the security of information resources and data. Access controls protect data from unauthorized modification, loss, or destruction by restricting access or detecting inappropriate access attempts. Effective controls include granting access to data and program files only to the extent necessary for individuals to perform their assigned duties.

Audit Objective: To assess the effectiveness of the Michigan Department of Transportation (MDOT) and the Department of Information Technology's (DIT's) security and access controls over selected information systems. These selected systems include Michigan Department of Transportation Architecture Project, User Application and Registration System, Bid Express System, and construction related systems.

Conclusion: MDOT and DIT's security and access controls over selected information systems were not effective. Our assessment disclosed one material condition*. MDOT had not established and implemented a comprehensive information systems security program (Finding 1). Our assessment also disclosed five reportable conditions* related to operating system security, database access, User Application and Registration System (UARS) security over Web-based systems, access controls over MDOT's non-Web-based information systems, and physical security (Findings 2 through 6).

FINDING

1. Security Program

   MDOT had not established and implemented a comprehensive information systems security program. Without an information systems security program, management cannot effectively maintain the integrity and availability of information systems and data.

   A comprehensive security program is the foundation of an entity's security control structure. It is also a method for executive management to address security risks.

* *See glossary at end of report for definition.*

A comprehensive security program should include periodic risk assessments, resources for independent monitoring of information systems activity, and detailed policies and procedures for safeguarding all information system resources and data. We noted:

a. MDOT had not established an information security officer position. Security officer duties include establishing a security program, developing and enforcing security policies and procedures, and monitoring system-recorded security activities and violations.

b. MDOT had not completely documented security risk assessments on its critical information systems. Also, MDOT did not determine the amount of time that MDOT can operate without the information systems in the event of a disaster or unauthorized access to the data and program files. Although MDOT and DIT have conducted risk assessments on some critical information systems, conducting risk assessments on other critical information systems would help MDOT identify and reduce risks associated with software and data security, personnel security, and contingency plans to meet information systems' processing needs in the event of a disaster. MDOT and DIT informed us that MDOT has a process to conduct risk assessments on new information systems.

c. MDOT, in conjunction with DIT, had not fully developed, documented, and tested a disaster recovery plan for MDOT's information systems. Without a documented and tested disaster recovery plan, MDOT and DIT cannot ensure continued operation and processing of MDOT information systems in the event of a disaster or other service disruption.

We reported these conditions in our prior audit. MDOT agreed with our prior audit recommendation and indicated that it had assigned a new security officer and that the duties of the security officer have been expanded. MDOT also informed us that the security officer role transferred to DIT at the time of DIT's creation.

RECOMMENDATION

WE AGAIN RECOMMEND THAT MDOT ESTABLISH AND IMPLEMENT A COMPREHENSIVE INFORMATION SYSTEMS SECURITY PROGRAM.

AGENCY PRELIMINARY RESPONSE

MDOT agrees and informed us that it has taken preliminary steps to comply with the finding. MDOT informed us that it will work with DIT to develop a preliminary security program in 60 days and will develop a comprehensive security program by December 2007. MDOT also informed us that it established a security officer position in May 2007. In addition, MDOT informed us that it documented risk assessments for its critical information systems and determined the amount of time that MDOT can operate without the critical information systems in the event of a disaster or unauthorized access to the data and program files. MDOT further informed us that it worked with DIT to create a draft disaster recovery plan for general information technology disasters and will develop a documented and tested disaster recovery plan by December 2007.

FINDING

2. Operating System Security

DIT had not established effective security controls over the server operating systems*. As a result, MDOT could not ensure that data was protected from unauthorized modification, loss, or disclosure.

A well-secured operating system helps provide a stable platform on which to run MDOT's information systems. Operating system security controls should be established to protect information and resources from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. In addition, an operating system should be installed with a minimal service configuration to reduce the risk of network intrusion and exploitation of well-known operating system vulnerabilities.

Our review of the seven servers that contain FieldManager, MAP Financial Obligation System (MFOS), MDOT Architecture Project (MAP), MAP Project Information System (MPINS), Project Accounting and Billing (PAB), Trns*port, and UARS applications and databases identified vulnerable operating system security controls and configurations. In addition, DIT had not established policies and standards for operating system configuration. Further, DIT had not documented the current operating system configuration.

* *See glossary at end of report for definition.*

RECOMMENDATION

We recommend that DIT establish effective security controls over the server operating systems.

AGENCY PRELIMINARY RESPONSE

DIT agrees and informed us that it will comply with the finding. DIT informed us that it started moving MDOT servers to one of the three DIT hosting centers during March 2007 and plans to complete the move of MDOT servers in November 2007. DIT also informed us that documented operating system policies and procedures will be implemented to provide effective system security controls and configurations. In addition, DIT informed us that as servers are replaced, the operating systems will be configured based upon a standard operating system template. DIT further informed us that it actively scans and reports monthly on the operating system vulnerabilities and compliance with standards to ensure that the proper patches and upgrades are implemented for the server operating systems.

FINDING

3. Database Access

DIT had not established effective security and access controls over the MFOS, MPINS, PAB, Trns*port, and UARS databases. Effective database security and access controls would help prevent or detect inappropriate access to MDOT's data.

An effective database security model includes configuration of the database with strong security settings and access controls. Our review of 4 databases disclosed:

a. DIT did not restrict certain accounts from having privileged access* to all 4 databases. Accounts with privileged access have the ability to make changes to the database that affect security or performance.

b. DIT did not implement strong database password control policies and log-in parameters on all 4 databases. Effective password controls are one of the primary means to prevent unauthorized access to information resources.

* *See glossary at end of report for definition.*

c. DIT had not established a formal process for monitoring privileged user access to all 4 databases. Formal processes would help DIT manage user access and ensure that users only have access required to perform their jobs.

d. DIT did not restrict access to a sensitive database table on all 4 databases. This could allow users to obtain inappropriate access to the database.

e. DIT did not effectively configure security settings for 1 of the 4 databases. Database security settings help to prevent unauthorized access.

f. DIT did not restrict system development staff access to database files on 3 of the 4 databases. DIT should restrict development staff access to database files because they have the ability to make unauthorized changes to MDOT data.

g. DIT did not use database audit logs to monitor database administrator activity for all 4 databases. Audit logs can be configured to record privileged access and identify unusual or unauthorized activity.

RECOMMENDATION

We recommend that DIT establish effective security and access controls over MFOS, MPINS, PAB, Trns*port, and UARS databases.

AGENCY PRELIMINARY RESPONSE

DIT agrees and informed us that it will establish effective security and access controls over MFOS, MPINS, PAB, Trns*port, and UARS databases by July 2007. DIT informed us that it modified processes and procedures to comply with the finding. DIT also informed us that, as part of the modification, password access is more stringent and developer access to production data is limited. In addition, DIT informed us that it will continue to review database settings to improve security and continue to address security and performance issues.

FINDING

4. UARS Security Over Web-Based Systems

MDOT and DIT did not effectively plan for and implement effective security controls over UARS. Without effective security controls, MDOT and DIT cannot ensure that UARS securely and properly grants access to MDOT's Web-based systems.

The Control Objectives for Information and Related Technology* (COBIT) highlights the importance of effectively and efficiently securing information systems to safeguard information against unauthorized use, disclosure, modification, damage, or loss. We noted:

a. DIT did not encrypt confidential UARS usercodes, passwords, and security questions and answers during transmission. Also, DIT did not encrypt the UARS passwords and security questions and answers with a secure method within UARS. Encryption is a method used to change data into an unreadable format. Confidential information should be encrypted when transmitted and when stored on the database.

b. MDOT and DIT did not ensure the confidentiality of UARS user passwords. UARS automatically creates and e-mails a computer-generated password to a user when the user forgets his or her password. However, UARS also e-mails the password to the UARS contractor. In addition, MDOT and DIT allowed the UARS contractor and system administrators to manually create user passwords. MDOT and DIT should modify UARS to e-mail passwords only to users and prevent the UARS contractor and system administrators from manually creating passwords.

c. MDOT and DIT did not disable UARS usercodes of users who no longer required access. We reviewed 417 usercodes and noted that 23 (5.5%) belonged to users who no longer required access. Also, MDOT and DIT did not disable 1,739 usercodes for users who have never signed on to UARS.

d. MDOT and DIT were unable to identify the work location or agency for 2,476 UARS users. UARS user profile information did not contain adequate identifying information for system administrators to completely identify the

* *See glossary at end of report for definition.*

user work location or agency. Although UARS system administrators had user information such as username, log-in identification, and address, the identification of the user work location or agency would help system administrators identify UARS users to monitor user access needs and ensure that users are still valid.

e. MDOT and DIT did not restrict DIT developer access to UARS usercodes and user information. This could result in inappropriate access to MDOT information systems.

f. MDOT and DIT did not periodically review UARS audit logs. Periodically reviewing audit logs would help to detect unusual, high-risk, or inappropriate activity on UARS.

g. MDOT and DIT did not ensure that users had only one usercode on UARS. We noted 65 users with duplicate usercodes. Having more than one usercode allows users to sign on at two terminals at the same time. This increases the risk that the user would leave a terminal unattended while signed on to UARS.

h. MDOT and DIT did not develop and enforce standards for usercode composition. We noted two users whose usercode was their social security number.

i. MDOT and DIT did not have formal policies and procedures for granting access, revoking access, or assigning access levels to UARS. Formal procedures would help MDOT and DIT manage user access and ensure that only authorized users had access to UARS.

j. MDOT and DIT did not prepare system documentation. MDOT could not provide us with system narratives, flowcharts, system and program specifications, test plans and test results, a data dictionary, and user manuals. The contractor that developed UARS is no longer providing service to MDOT and DIT. Without documentation, MDOT and DIT do not have a complete understanding of UARS processes and cannot ensure proper assignment of user access to MDOT Web applications.

k. MDOT and DIT did not display security banners on UARS. Security banners should inform anyone accessing UARS that unauthorized access is prohibited. In the event of disclosures of confidential data, banners would aid in prosecuting intruders by helping to establish that intruders were aware that they were trespassing.

RECOMMENDATION

We recommend that MDOT and DIT effectively plan for and implement effective security controls over UARS.

AGENCY PRELIMINARY RESPONSE

MDOT and DIT agree and informed us that they created a detailed development and implementation plan to comply with the finding. MDOT and DIT informed us that final software changes will be implemented in June 2007. MDOT and DIT informed us that UARS was developed as a temporary solution and MDOT will migrate to the proposed DIT enterprise identity management solution in the future.

FINDING

5. Access Controls Over MDOT's Non-Web-Based Information Systems

MDOT had not established effective access controls over its non-Web-based information systems. Without effective access controls, MDOT and DIT cannot ensure the security and integrity of data.

Department of Management and Budget Administrative Guide procedures 1310.02 and 1410.17 provide guidance and requirements to State departments for developing and implementing access controls. The proper assignment of usercodes and passwords is a significant factor in maintaining data security and ensuring that only authorized users access or change data. We reviewed access controls over six of MDOT's non-Web-based client server* information systems: FieldManager, FINDLYUP, MFOS, MPINS, PAB, and Trns*port. We noted:

a. MDOT did not disable employee access to all information systems upon employee departure. Disabling employee access upon employee departure

* *See glossary at end of report for definition.*

helps protect information system data from unauthorized modification or use. We noted:

(1) Our sample of 31 FieldManager usercodes disclosed that 8 (26%) belonged to former employees.

(2) Our sample of 20 Trns*port usercodes disclosed that 1 (5%) belonged to a former employee.

b. MDOT did not require users to periodically change their passwords for MFOS, PAB, and Trns*port. Changing passwords on a regular basis helps ensure password confidentiality and reduces the risk of unauthorized access to the systems. We reported this condition in our prior audit as it related to MFOS and Trns*port.

c. MDOT did not lock out usercodes after a reasonable number of invalid sign-on attempts for FieldManager, MFOS, PAB, and Trns*port. Locking out usercodes prevents an individual from attempting to gain unauthorized access to an information system.

d. MDOT did not establish unique usercodes and passwords for all FieldManager and Trns*port system users. We noted that up to 28 users shared a single Trns*port usercode. Establishing unique usercodes and passwords would help ensure that users perform only those duties that management authorized them to perform. It would also help provide accountability for transactions. We reported this condition in our prior audit as it relates to Trns*port.

e. MDOT did not require users to use different passwords at each password change for MFOS, PAB, and Trns*port. Requiring the use of different passwords helps prevent unauthorized access to information systems. We reported this condition in our prior audit as it relates to MFOS and Trns*port.

f. MDOT did not disconnect users or use password-protected screensavers after a reasonable period of inactivity for MFOS, MPINS, PAB, and Trns*port. This could result in unauthorized system access if a user leaves a work station unattended. We reported this condition in our prior audit as it related to MFOS and Trns*port.

g. MDOT did not establish formal policies and procedures for assigning, restricting, removing, or reviewing user access to information systems. Formal policies and procedures would help MDOT manage its user access and ensure that only authorized users had access to the systems.

h. MDOT, in conjunction with DIT, did not obtain signed security agreements for all users prior to granting access to the systems. We reviewed 88 MDOT and DIT users and identified 11 who did not have signed security agreements. A security agreement helps assure management that users are aware of their responsibilities regarding acceptable use of information technology, license restrictions, software usage, confidentiality of information, applicable laws and department policies, and penalties for noncompliance with the security agreements.

i. MDOT did not prevent users with read-only access from altering MFOS and PAB data. We identified MFOS and PAB users with read only access who could change the review status of municipal agreements and the project indicator status, respectively. The ability to change the review status of municipal agreements should be restricted to program control staff. The ability to change the project indicator status should be restricted to project accounting staff. After we brought this matter to management's attention, MDOT made adjustments to properly restrict read-only access rights.

RECOMMENDATION

We recommend that MDOT establish effective access controls over its non-Web-based information systems.

AGENCY PRELIMINARY RESPONSE

MDOT agrees and informed us that it will take steps to comply with the finding. MDOT informed us that it is developing policy and procedures for employee access to information systems. MDOT informed us that it plans to complete the policy and procedures by September 2007.

MDOT and DIT also informed us that security and authenticity is essential for protecting data. In addition, MDOT and DIT informed us that they have chosen to control security and access at the network level and will evaluate changing specific systems when making major changes to MDOT's critical information systems.

MDOT and DIT further informed us that it will research the feasibility of establishing a centralized identity management solution.

FINDING

6. Physical Security

DIT had not established effective physical security controls over network resources. Effective physical security controls would help ensure that network resources are safeguarded and that access is limited to individuals responsible for managing the network resources. Our review of physical security controls disclosed:

a. DIT did not store critical network servers in a secure location. We found critical network servers stored in an unlocked office. The office had a locking door; however, DIT did not always lock the door. Also, DIT did not track the assignment and return of keys to the office. DIT was unable to provide us with a listing of all individuals who were given keys to the office. Storing network servers in a secure location would help ensure the safety of the network equipment.

   After we brought this to management's attention, DIT moved the critical network servers to the server room.

b. DIT could not verify that it changed the access code to the server room after an employee left his or her job with DIT. Changing the server room access code upon employee departure would help prevent unauthorized individuals from accessing the server room.

c. DIT did not maintain a log of authorized personnel and visitors who entered the server room. Maintaining a log would help DIT identify who was in the server room in the event of a questionable action occurring to network resources.

d. DIT had not defined and documented policies and procedures regarding employee behavior, visitor access, environmental security tests, disaster recovery, and emergency response for the server room. Documented policies

and procedures would help ensure that servers are safeguarded on a daily basis and in the case of an emergency.

RECOMMENDATION

We recommend that DIT establish effective physical security controls over network resources.

AGENCY PRELIMINARY RESPONSE

DIT agrees and informed us that it has already taken steps to comply with the finding. DIT informed us that it locked the server room in January 2007 and limited access to only the server team. DIT also informed us that it is in the process of moving the MDOT servers to one of three DIT hosting centers. In addition, DIT informed us that it plans to complete the MDOT server moves in November 2007 and will adhere to physical security protocols of the DIT hosting centers.

INTEGRITY OF DATA

COMMENT

Audit Objective: To assess the effectiveness of MDOT and DIT's efforts to ensure the integrity of data for selected information systems.

Conclusion: MDOT and DIT were moderately effective in their efforts to ensure the integrity of data for selected information systems. Our assessment disclosed two reportable conditions related to data integrity and audit trails (Findings 7 and 8).

FINDING

7. Data Integrity

MDOT did not implement data edits to ensure the integrity of MAP and Trns*port data. Without data edits, inaccurate or missing information could affect MDOT's road and bridge construction projects.

Data edits help ensure complete data processing and the integrity of data throughout the construction process. We conducted an analytical review of MAP

and Trns*port data for the period December 2003 through August 2006. We noted:

a. MDOT did not ensure the accuracy and completeness of data in MAP. MAP contains information about each of MDOT's construction jobs. Approximately 30 MDOT information systems access and update the data on the MAP database. Our review of MAP data edits disclosed:

   (1) MDOT did not ensure that MAP contained a valid physical roadway number for each job. We identified 11 jobs with invalid physical roadway numbers.

   (2) MDOT did not ensure that MAP contained a non-let reason code for all non-let jobs. Non-let jobs are projects not subject to competitive bidding. We identified 56 non-let jobs without a non-let reason code. Non-let reason codes are used to provide management with assurance that jobs coded as non-let follow the appropriate process.

   (3) MDOT did not ensure that MAP contained a let date for all competitively bid jobs. We identified 43 jobs without a let date. The let date identifies when MDOT opened and reviewed bids for contracted jobs.

   (4) MDOT did not ensure that MAP contained a scheduled contract bid review date for all jobs. We identified 4 jobs without a scheduled contract bid review date. The scheduled contract bid review date represents the date when MDOT plans to open and review bids for contracted jobs.

   After we brought the test results to management's attention, MDOT corrected all of the invalid and missing data. However, MDOT did not make changes to MAP to prevent such errors from occurring in the future.

b. MDOT did not ensure the accuracy and completeness of data in Trns*port. Trns*port contains project proposals, contractor bids, project costs, and quantities of materials used. Trns*port transfers data to and from other MDOT

systems to process accumulated project costs and contractor payments. Our review of Trns*port data edits disclosed:

(1) MDOT did not ensure that Trns*port contained a work type code for all projects. We identified 58 projects without a work type code. MDOT staff prepare summary reports by work type code to summarize project costs.

(2) MDOT did not program Trns*port to reject invalid project completion date and award date combinations. We identified one project in which the project completion date was before the award date. After we brought the test results to management's attention, MDOT corrected the project dates. However, MDOT did not make changes to Trns*port to prevent invalid dates from occurring in the future.

RECOMMENDATION

We recommend that MDOT implement data edits to ensure the integrity of MAP and Trns*port data.

AGENCY PRELIMINARY RESPONSE

MDOT agrees and informed us that where possible, it will develop edit checks within specific information systems that provide data to MAP. MDOT informed us that as an interim step it will notify users by July 2007 of the importance of ensuring the accuracy of data entered into the information systems.

MDOT also informed us that it is unable to modify the Trns*port source code as it licenses the system from the American Association of State Highway and Transportation Officials (AASHTO). In addition, MDOT informed us that modifying Trns*port data integrity edits are dependent on funding and priorities of other states. MDOT further informed us that it will evaluate the business risk, development cost, and other benefits prior to requesting AASHTO to modify Trns*port.

FINDING

8. Audit Trails

MDOT did not ensure that system audit trails provide complete identifying information about each transaction in Trns*port.

We noted that Trns*port did not record complete identifying information about each transaction entered into Trns*port. The system did not record the date, time, and usercode of each transaction. Recording this information would enable MDOT to identify the originator of each transaction. We reported this condition in our prior audit. MDOT agreed with the finding.

RECOMMENDATION

WE AGAIN RECOMMEND THAT MDOT ENSURE THAT SYSTEM AUDIT TRAILS PROVIDE COMPLETE IDENTIFYING INFORMATION ABOUT EACH TRANSACTION IN TRNS*PORT.

AGENCY PRELIMINARY RESPONSE

MDOT agrees and informed us that it is unable to modify the Trns*port source code as it licenses the system from the AASHTO. MDOT informed us that AASHTO is rewriting Trns*port to include date, time, and usercode audit trails. MDOT also informed us that the rewrite is expected to be completed over the next few years.

GLOSSARY

Glossary of Acronyms and Terms

AASHTO	American Association of State Highway and Transportation Officials.
client server	An architecture in which one computer can get information from another. The client is the computer that asks for access to data, software, or services. The server, which can be anything from a personal computer to a mainframe, supplies the requested data or services for the client.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.
DIT	Department of Information Technology.
effectiveness	Program success in achieving mission and goals.
FINDLYUP	Finance Daily Update.
integrity	The accuracy, completeness, and timeliness of data in an information system.
MAP	MDOT Architecture Project.
material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
MDOT	Michigan Department of Transportation.

MFOS	MAP Financial Obligation System.
MPINS	MAP Project Information System.
PAB	Project Accounting and Billing System.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
privileged access	Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
risk	The probability that a particular security threat will exploit a system vulnerability.
risk assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

server operating system	The software that manages the application and data files that are shared over a network.
UARS	User Application and Registration System is a single sign-on system for approximately 23 MDOT Web-based information systems.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL