JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF TRANSPORTATION
LANSING

KIRK T. STEUDLE
DIRECTOR

February 21, 2008

Mr. Michael Moody, Director
Office of Financial Management
Department of Management and Budget
Romney Building, 7th Floor
111 South Capitol Avenue
Lansing, Michigan 48933

Dear Mr. Moody:

As the Michigan Department of Transportation's (MDOT's) interim information security officer, I am submitting the findings and follow-up responses for the Michigan Department of Transportation's and Michigan Department of Information Technology's (MDIT's) Auditor General's Audit Report of the Michigan Department of Transportation Architecture Project, User Application and Registration System, Bid Express System, and Construction Related Systems.

FINDING

1. Security Program

RECOMMENDATION

We again recommend that MDOT establish and implement a comprehensive information systems security program.

AGENCY UPDATE

Finding 1a
As reported in our previous follow-up response, MDOT has taken preliminary steps to establish a security program including: establishing a temporary information security officer position; documenting its critical system risk assessments; and, determining 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.

Additionally, MDOT has developed a Security Program framework and a draft of the Security Program that includes roles and responsibilities, policies and procedures, risk management and security controls. MDOT has also developed a position description for the permanent MDOT Information Security Officer and has approval to fill the position. After the position is established, MDOT will work with Office of Human Resources to quickly fill the position.

MDOT has established a Security Policy Committee which has developed and approved policies for Use of IT Resources, IT Security Awareness and Training, Passwords, and Storage of Sensitive Information on Mobile Devices and Portable Media. Additionally, policies have been drafted for Data Classification, Remote Access, and Incident Handling which are currently moving through the MDOT approval process. Future policies to be drafted include Access Control, Authentication and Authorization, Audit and Risk Assessment, and Business Continuity Planning.

All IT security policies are reviewed and approved by the department's Information Technology Operations Team (ITOT) and MDOT Executive prior to implementation.

MDOT continues efforts to develop a comprehensive security program and establish a permanent MDOT Information Security Officer.

Finding 1b
As indicated in our previous follow-up response, MDOT completed the updating of system risk assessments on June 6, 2007, and included this information in the Information Technology Application Portfolio (ITAP) system.

Finding 1c
As indicated in our follow-up response, MDIT and the stakeholder agencies are in the process of establishing comprehensive Disaster Recovery Plans for the most critical systems to the State of Michigan. Disaster Recovery Plans for less-critical systems will be created following the completion of the plans for the critical systems.

As reported previously, MDIT has also implemented an Active Monitoring System that provides notification when critical systems are experiencing a service outage. Currently the MIPARS system is actively monitored for any service problems or issues. Future plans include obtaining pricing to expand the monitoring to other critical systems. Based on the pricing and the agencies funding, the monitoring system will be expanded to other critical systems.

FINDING

2. Operating System Security

RECOMMENDATION

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

AGENCY UPDATE

MDIT has completed the server move of the MDOT servers from the Van Wagoner Building to the MDIT State Hosting Centers. The physical moves started in March 2007, and were completed in November 2007. As servers are replaced, the operating systems will be based on the M1 standard build OS template.

Item closed.

FINDING

3. Database Access

RECOMMENDATION

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

AGENCY UPDATE

As indicated in our previous follow-up response, MDIT has established security and access controls over MFOS, MPINS, PAB, Trns*port, and UARS databases effective July 31, 2007.

The production PowerBuilder code compilation and the creation of encrypted passwords were moved to the DIT Configuration Management - Quality Assurance Team of Agency Support Services. This removes the risk of developers having access to database passwords. This also removes the responsibility from the development organization and provides a clear separation of roles. Since developers don't have access to the production source code or executable, the only way to access the production database would be by using the application. The new process was implemented for MFOS and PAB on December 19, 2007, and MPINS on January 4, 2008.

Item closed.

FINDING

4. UARS Security Over Web-Based Systems

RECOMMENDATION

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

AGENCY UPDATE

As indicated in our follow-up response, MDOT and MDIT have taken steps to address all of the findings for UARS Security over web-based systems. These changes were completed June 2007.

UARS was developed as a temporary solution. MDOT will migrate to the proposed MDIT enterprise identity management solution once a contract is awarded for the effort. As the contract to obtain the enterprise identity management solution has been delayed, MDOT will not be able to meet the planned second quarter of Fiscal Year 2008 due date for the proposed solution. MDOT will continue to work with MDIT to address effective security controls over UARS and to obtain the enterprise identity management solution.

FINDING

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

RECOMMENDATION

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

AGENCY UPDATE

Finding 5a, d, g & h
As indicated in our initial and follow-up responses, MDOT is taking steps to correct the situation. The department has developed a comprehensive security plan and is developing access control policies. The Access Control and Remote Access policies will be completed by the end of second quarter Fiscal Year 2008.

Finding 5b, c, e & f
As indicated in our initial and follow-up responses, MDIT is in the process of identifying the development costs to implement a centralized identity management solution. MDOT will migrate to the proposed MDIT enterprise identity management solution once a contract is awarded for the effort. As the contract to obtain the enterprise identity management solution has been delayed, MDOT did not meet the original September 2007 date. In the event that a state-wide solution is not available, MDIT will work with MDOT on a solution to address the issues raised by the audit findings.

FINDING

6. Physical Security

RECOMMENDATION

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

AGENCY UPDATE

In November 2007, MDIT completed the close down of the Van Wagoner server room. All servers now fall under the MDIT hosting center procedures for physical security requirements and will adhere to the physical security protocols of the MDIT Hosting Center.

Item closed.

FINDING

7. Data Integrity

RECOMMENDATION

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

AGENCY UPDATE

As indicated in our initial response, MDOT will develop edit checks to the specific systems that provide data to MAP, as part of major system changes.

The interim step of notifying system users of the importance of assuring the accuracy of data entered into the system was completed on October 24, 2007.

In regards to 7b of the finding, MDOT provided a letter to the Trns*port Task Force Chair on October 26, 2007, indicating our commitment to data integrity and urging them to prioritize edits checks in the future release of the software.

FINDING

8. Audit Trails

RECOMMENDATION

We again recommend that MDOT ensure that system audit trails provide complete identifying information about each transaction in Trns*port.

AGENCY RESPONSE

As indicated above, MDOT provided a letter to the Trns*port Task Force Chair on October 26, 2007, indicating our commitment to data integrity and urging them to prioritize system audit trails in the future release of the software.

If you have any questions regarding this response for Michigan Department of Transportation, please contact Myron Frierson, Bureau Director, Bureau of Finance and Administration, at 517-373-2117 or Jerry J. Jones, Commission Auditor, at 517-373-2384. If you have any questions for Michigan Department of Information Technology, please contact John Juarez, Internal Auditor, at 517-241-2713.

Sincerely,

Signature Redacted

Coleen Hines, Interim Information Security Officer
Michigan Department of Transportation

cc: J. Jones
L. Hank
M. Frierson
D. Couto
B. Stoddard
A. Dickenson
M. Bowerman
S. Maynard
R. Nixon
W. Hoard