STATE OF MICHIGAN

DEPARTMENT OF INFORMATION TECHNOLOGY

LANSING

JENNIFER M. GRANHOLM
GOVERNOR

MICHIGAN DEPARTMENT OF dit INFORMATION TECHNOLOGY

TERESA M. TAKAI
DIRECTOR

July 9, 2007

Mr. Michael J. Moody, Director
Office of Financial Management
Department of Management and Budget
George W. Romney Building
111 South Capitol Avenue
Lansing, Michigan 48913

Dear Mr. Moody:

The following are our agency preliminary responses to the recommendations contained in the report of the Auditor General's performance audit of Enterprise Information Security Program, Department of Information Technology (MDIT).

1. Information Security Governance

MDIT agrees with the recommendation. The National Association of State Chief Information Officers (NASCIO) and other external organizations have recognized that the department has implemented numerous successful projects, i.e., new backup generators, new intrusion detection systems, anomaly detection systems, web and spam filtering, new firewalls, and over a dozen other mission-critical projects. These award-winning projects have validated the department's successes in managing the reduction of IT security risk for the state.

The department will continue to fully integrate security into the department's governance model and business processes and has launched Phase II of the State Unified Information Technology Environment (SUITE) project, which includes the Software Engineering Model (SEM). The Office of Enterprise Security (OSE) is an integral part of the SUITE implementation to ensure the state integrates security best practices into our business processes. MDIT will work with our infrastructure areas and lifecycle management process to ensure that based on availability of resources, security issues are prioritized and addressed.

In addition, OES has implemented the majority of the Secure Michigan Initiative (SMI) framework which included actions to establish the implementation and enforcement of an information security framework across state agencies. In addition, new statewide policies have been submitted to the Department of Management and Budget (DMB) for inclusion in the State's Administrative Guide. MDIT has developed detailed budget recommendations based on OES Strategic Plan which was published in January 2007. Lastly, MDIT will prioritize these projects, with their associated expenditures, and work with other state departments to implement security based on the availability of state resources.

2. Enterprise Information Security Framework

MDIT agrees and will fully implement a comprehensive enterprise information security framework. The department created the MDIT Strategic Security Plan, published by the OES in January 2007, which will assist state agencies assess their current status of security, including an analysis of priorities for next steps to be taken to ensure appropriate security for their mission critical applications, data, and to ensure business continuity. The plan's major categories include a comprehensive set of security policies, training, risk reduction, business continuity, and agency security plan template. MDIT's Strategic Security plan is strategic in nature and contains plans projected for FY 2007 through 2010; tactical projects are also included for implementation during FY 2007 and 2008.

With regard to item b., we agree and a statewide master information security policy establishing an overall approach to managing information security for all state agencies was written and submitted to DMB in February 2007 for inclusion and publication in the State's Administrative Guide.

With regard to item c., MDIT has established and updated many policies, standards and procedures, although the department recognizes the need for additional policies. As a result, MDIT has established an information security framework and submitted policies to DMB in February 2007 for inclusion and publication in the State's Administrative Guide. As current policies are revised and new policies standards and procedures are created, the department will integrate them into the new information security framework.

With regard to item d., MDIT will ensure that employees are trained on policies and procedures in accordance with the planned timelines as detailed in the department's Security Strategic Plan.

3. MITEC Security Subcommittee
MDIT agrees and will work with the MITEC security subgroup to prioritize the security issues addressed within the MDIT Strategic Security Plan. MDIT will also establish an annual meeting calendar for the MITEC's Security Subcommittee and develop a monitoring and reporting process to advise the subcommittee of the progress being made on the implementation of OES' Strategic Plan. In addition, the state's CIO will review the current MITEC charter and determine if any changes, amendments, deletions or additions are appropriate. MDIT will work to achieve full compliance by December 31, 2007.

4. Security Training
The department agrees and will fully develop and implement a comprehensive information security training program. In January 2007, the department created the MDIT Strategic Security Plan, published by OES which includes a comprehensive set of security policies, training, risk reduction, business continuity, and agency security plan template. OES will ensure an information security training plan and curriculum is executed over the next four years. In FY2007, OES will develop a security curriculum and formally present the curriculum to MDIT's Office of Employee and Financial Services for inclusion into employee's individual development plans.

The department, will once again, formally request the Department of Civil Services and the Office of the State Employer to require security awareness training and will attempt to make the training required for all state employees by the end of FY2008. To date, the department has established a formal awareness program through the development of the Department of Civil Service's Quick Knowledge program. Michigan's cybersecurity website, www.michigan.gov/cybersecurity, provides a self-paced security awareness training available to all state employees. This award-winning website has been used by other states, corporations, businesses and citizens to improve cybersecurity awareness on an informal basis.

5. Enterprise Information Security Risk Management Program
MDIT agrees with the finding. The department created the MDIT Strategic Security Plan, published by OES in January 2007 which will assist state agencies assess their current status of security, including an analysis of priorities, for next steps to be taken to ensure appropriate security for their mission critical applications, data, and to ensure business continuity.

The plan's major categories include a comprehensive set of security policies, training, risk reduction, business continuity, and agency security plan template. MDIT's Strategic Security Plan is strategic in nature and contains plans projected for FY 2007 through 2010; tactical projects are also included for implementation during FY 2007 and 2008. The department will continue to fully integrate security into the department's governance model and business processes and has launched Phase II of the State

Unified Information Technology Environment (SUITE) project, which includes the Software Engineering Model (SEM). While MDIT has developed formal processes for responding to information security incidents, the department will also develop a formal process for tracking the remediation of "lessons learned" from information security incidents. OES is responsible for ensuring the State integrates security best practices into business processes and will continue to expand the State's certification and accreditation efforts as resources become available.

6. Incorporation of Security Throughout the System Development
MDIT agrees with the recommendation and will implement a more effective process for incorporating security throughout an information system's SDLC.

With regard to item a., the department will continue to fully integrate security and security guidance into the department's governance model and business processes and has launched Phase II of the SUITE project which includes the SEM. The implementation team, which includes an OES team member, has already begun the process of incorporating security deliverables from the OES Resource Guide.

With regard to item b., while security liaisons are included in the early phases of system development projects, additional guidance about how and when to include security liaisons will be incorporated into the SUITE and Software Engineering Model. Furthermore, MDIT is working with client agencies to increase the number of security liaisons, providing security guidance and expertise and has increased security liaison support to the Department of Management and Budget and the Department of Civil Service.

With regard to item c., a fully integrated set of security policies are being written, as well as security templates to assist State agencies develop their own agency security plans. The templates and plans will enable agencies to assess the status of their security level, including action steps to ensure appropriate security for all their applications, data, and business continuity.

7. Disaster Recovery Planning
MDIT agrees and will develop an integrated and comprehensive process to oversee and direct the state's disaster recovery (DR) planning.

In the spring of 2006, MDIT began a project to identify critical business functions in the agencies that are supported by IT infrastructure and systems within MDIT. The project includes developing recommendations for an organizational structure, funding model and staffing to support the DR framework, policies, procedures and implementation guidance for MDIT and our customers. MDIT believes these processes must be fully integrated into the department's daily work processes and as a result, the framework will be integrated with MDIT's System Design Methodology as well as all of the ITIL-based problem management, configuration management, change management and incident management processes. In addition, the department has authorized a new position within Data Center Operations to oversee the disaster recovery processes. The department has also set a goal to identify and validate the thirty-five critical state IT functions by December 2007.

8. IT Internal Audit Function
MDIT agrees with the recommendation. MDIT's priorities will continue to focus on assigning the department's limited resources to correct known security deficiencies. The department will continue to strengthen and integrate internal controls into the department's governance model and business processes and has launched Phase II of the State Unified Information Technology Environment (SUITE) project. With SUITE, MDIT will continue to explore all alternatives to increase our monitoring of internal controls. In addition, MDIT will continue the work with our infrastructure areas and lifecycle management processes to ensure that based on the availability of resources, internal controls are

addressed. Lastly, MDIT will continue to recommend that state agencies ensure sufficient IT audit resources are assigned to audit application controls for their critical applications.

9. Performance Metrics for IT Security Program
MDIT agrees and OES will fully develop and implement performance metrics for critical components of the department's information security program. OES has developed and implemented a significant number of critical performance metrics and will complete a formal assessment to determine the appropriate performance metrics for measuring critical components of its information security program. In addition, the MDIT Security Strategic Plan, published by OES in January 2007, has specific actions, deliverables, performance metrics and deadlines.

In addition, below is additional clarifying language submitted to the OAG for inclusion in the report:

The Department of Information Technology is actively engaged in protecting the state's computer systems each and every day. The security over the state's computer systems is taken very seriously, and it is important to note that the Auditor General staff found in their audit that "DIT's enterprise information security risk management program included incident, threat, vulnerability and emergency management practices as well as practices to restrict the State's end-users from accessing risky or inappropriate websites."

Some of the material weaknesses identified in this audit represent an independent validation of the concerns identified by MDIT's Secure Michigan Initiative (SMI). MDIT believes that this audit illustrates that significant reforms and improvement in IT security controls have been achieved since 2002. Tremendous progress has been made in every aspect of our information security program and MDIT has already implemented many of the findings reported in this audit with new policies, procedures and projects. Lastly, the newly released Strategic Security Plan created and published OES, addresses the remaining weaknesses with resolutions scheduled in the months ahead.

Enclosed is Exhibit A outlining the citations in which we are working towards compliance. If you have any questions concerning these responses, please contact John Juarez, of MDIT Internal Audit, at 241-2713.

Sincerely,

Signature Redacted

Kenneth D. Theis
Chief Deputy Director

Enclosure

c: Office of the Auditor General
DMB Budget Office
Teri Takai
Dan Lohrmann
Pat Hale
Doug Couto
Carol Sherman
Kurt Weiss
Rick Lowe
John Juarez

EXHIBIT A

Performance Audit of
Network Application Server Controls,
Michigan Department of Information Technology (MDIT)

Audit Response Summary

Period Covered: May 2005 through January 2006

1. Citations fully complied with:

   None.

2. Citations the agency agrees with and will comply with:

   a. Finding #1.

   b. Finding #2.

   c. Finding #3.

   d. Finding #4.

   e. Finding #5.

   f. Finding #6.

   g. Finding #7.

   h. Finding #8.

   i. Finding #9.

3. Citations the agency disagrees with:

   None.