MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

ENTERPRISE INFORMATION SECURITY PROGRAM

DEPARTMENT OF INFORMATION TECHNOLOGY

April 2007

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

084-0581-06

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

Enterprise Information Security Program

Department of Information Technology (DIT)

Report Number:
084-0581-06

Released:
April 2007

An enterprise information security program is the foundation of the State's security control structure and reflects management's commitment to address security risks. The Office of Enterprise Security (OES) is responsible for identifying, managing, and mitigating security risks and vulnerabilities. OES is charged with leading disaster recovery planning, risk management, and security awareness and training; working with State agencies on security issues; and enforcing State security policies.

Audit Objective:
To assess the effectiveness of DIT's efforts to fully implement an effective information security framework.

Audit Conclusion:
DIT's efforts to fully implement an effective information security framework were not effective. We noted four material conditions.

Material Conditions:
DIT had not fully developed its information security governance program (Finding 1). Also, DIT had not fully implemented a comprehensive enterprise information security framework (Finding 2). In addition, DIT did not ensure that the Michigan Information Technology Executive Council security subcommittee provided effective information security governance for the State (Finding 3). Further, DIT had not fully developed and implemented a comprehensive information security training program (Finding 4).

Noteworthy Accomplishments:
The State's chief information security officer was named Executive Alliance's Information Security Executive of the Year Central for 2006. The award recognizes individuals who have demonstrated outstanding leadership in the field of information security.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's efforts to evaluate and manage the State's exposure to information security risks.

Audit Conclusion:
DIT's efforts to evaluate and manage the State's exposure to information security risks were moderately effective. Our assessment disclosed 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 high-risk or inappropriate Web sites. However, we noted three material conditions.

Material Conditions:
DIT had not fully implemented a comprehensive enterprise information security risk management program (Finding 5). Also, DIT needs to implement a more effective process for incorporating

security throughout an information system's system development life cycle (Finding 6). DIT had not established an integrated and comprehensive process to oversee and direct the State's disaster recovery planning efforts. In addition, DIT did not have fully documented and tested disaster recovery plans for critical enterprise systems and the State's infrastructure (Finding 7).

Noteworthy Accomplishments:

In 2003 and 2004, the State received National Association of State Chief Information Officers (NASCIO) recognition awards for security and emergency management. In 2003, the State won the award for the *Secure Michigan Initiative* project. The project included a rapid risk assessment to determine high-risk issues in relation to the security of the State's information technology (IT) infrastructure, policies, procedures, and systems.

In 2004, the State won the NASCIO award for the Michigan Critical Incident Management System (CIMS). During the August 2003 electrical blackout, DIT used CIMS to track and monitor data on the status of the State's critical infrastructure. Use of CIMS allowed DIT to quickly restore critical systems and desktop services in an orderly manner.

In February 2006, DIT participated in Cyber Storm, the first government-led cyber security exercise to examine the response, coordination, and recovery mechanisms to a simulated cyber event within international, federal, state, and local governments. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:

To assess the effectiveness of DIT's efforts to evaluate and enforce compliance with information security policies and procedures.

Audit Conclusion:

DIT's efforts to evaluate and enforce compliance with information security policies and procedures were moderately effective. However, we noted two material conditions.

Material Conditions:

DIT did not sufficiently staff its internal audit function to effectively audit the State's IT environment. In addition, DIT did not coordinate with State agencies to ensure that sufficient IT audit resources were assigned to audit application controls for critical information systems (Finding 8). The Office of Enterprise Security had not fully developed and implemented performance metrics for critical components of its information security program (Finding 9).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 9 findings and 11 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and has complied or 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

April 10, 2007

Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Ms. Takai:

This is our report on the performance audit of the Enterprise Information Security Program, Department of Information Technology.

This report contains our report summary; description of program; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; two exhibits, presented as supplemental information; 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 agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency 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.

Sincerely,

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

This Page Left Intentionally Blank

TABLE OF CONTENTS

ENTERPRISE INFORMATION SECURITY PROGRAM
DEPARTMENT OF INFORMATION TECHNOLOGY

	Page
INTRODUCTION	
Report Summary	1
Report Letter	3
Description of Program	7
Audit Objectives, Scope, and Methodology and Agency Responses	10
COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES	
Efforts to Fully Implement an Effective Information Security Framework	15
1. Information Security Governance	17
2. Enterprise Information Security Framework	20
3. MITEC Security Subcommittee	22
4. Security Training	24
Efforts to Evaluate and Manage the State's Exposure to Information Security Risks	25
5. Enterprise Information Security Risk Management Program	27
6. Incorporation of Security Throughout the System Development Life Cycle	30
7. Disaster Recovery Planning	32
Efforts to Evaluate and Enforce Compliance With Information Security Policies and Procedures	36
8. IT Internal Audit Function	36
9. Performance Metrics for IT Security Program	38

SUPPLEMENTAL INFORMATION

Exhibit 1 - Summary of Office of the Auditor General Information Technology Audit Report Findings, Released October 2001 through July 2006 42

Exhibit 2 - Control Objectives for Information and Related Technology (COBIT) Maturity Model, DS5 Deliver and Support, Ensure Systems Security 44

GLOSSARY

Glossary of Acronyms and Terms 47

Description of Program

Enterprise* Information Security Program

The State's information systems and the information they contain represent significant assets and are critical to the State's ability to perform its mission and business functions. An enterprise information security program* is the foundation of the State's security control structure and reflects management's commitment to address security risks*.

Department of Information Technology (DIT)

In October 2001, Executive Order No. 2001-3 created DIT to achieve a more efficient and cost-effective approach for managing information technology* (IT), including information security, among all executive branch agencies. The Executive Order requires DIT to coordinate a unified executive branch strategic IT plan, identify best practices from executive branch agencies and other public and private sector entities, and develop and implement processes to replicate IT best practices and standards throughout the executive branch.

In May 2002, DIT's director appointed the director of its Office of Enterprise Security (OES) as Michigan's first chief information security officer (CISO). In March 2005, DIT's director signed OES's charter, formally defining the responsibilities of OES and CISO to serve as the advisor, to oversee policy, and to provide daily operational staff supervision for issues relating to digital, electronic, telecommunications, computer, and IT security matters of any nature. Through the charter, OES is accountable to the director for identifying, managing, and mitigating security risks and vulnerabilities* within State of Michigan government computing, communication, and technology resources. In addition, OES is charged with leading disaster recovery planning*, risk management*, and security awareness* and training; working with State agencies to assist with their security issues; and enforcing State security policies and procedures intended to maintain suitable and equal levels of enterprise-wide security. The charter authorizes OES to ensure that appropriate levels of security protection are implemented and sustained in order to maintain data integrity*, ensure system and application availability*, and protect government IT resources.

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

The major sections of OES include:

a. Risk Management and Compliance Section

The Risk Management and Compliance Section is responsible for identifying security risks through risk assessments* and mitigating those risks. Its responsibilities also include oversight of the State of Michigan's security architecture, intrusion detection, IT incident response, and ensuring compliance with State of Michigan security policies and standards.

b. Agency Liaison Section

The Agency Liaison Section consists of State of Michigan information security officers. The Section serves as a consultant to other State executive branch agencies to help define security functions and assist in implementing security recommendations. It is involved in security assessments and audits, development of metrics* and benchmarks, and the creation of Statewide IT security-reporting strategies according to industry best practices.

c. Communications, Awareness, and Homeland Security Section

Communications, Awareness, and Homeland Security Section is responsible for delivery of enterprise-wide communication of security initiatives and programs. The Section is responsible for the design and planning of targeted security awareness and training. In addition, the Section acts as the Homeland Security liaison to Homeland Security Task Force Cyber Security subcommittee, which researches security vulnerabilities and solutions and communicates issues to appropriate government contact points.

In addition, OES has several projects for specialized security topics, such as identity management, disaster recovery, Local Government Network, and standards architecture. For fiscal year 2005-06, OES had a budget of $4.6 million and 28 full-time equated positions.

*Secure Michigan Initiative**

In December 2002, OES published the *Secure Michigan Initiative*, which identified 12 high-risk and 7 medium-risk deficiencies impacting security over the State's IT infrastructure*. The *Secure Michigan Initiative* included recommendations for improving security. The CISO met with State executives from each agency participating in the risk

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

assessment to discuss the security weaknesses and recommendations particular to their agency.

Michigan Information Technology Executive Council (MITEC)

In June 2003, the State's chief information officer (CIO) established MITEC to advise and assist the State CIO and DIT in addressing current business, service, and technology support needs; developing longer-term IT goals; and setting strategic and tactical direction. MITEC established a security subcommittee that is responsible for setting the overall enterprise-wide information security policy* and framework, reviewing enterprise-wide security requirements and risks and proposing recommended actions, collaborating with IT and business management to provide recommendations for budgeting for security initiatives, coordinating security activities across agencies, and maintaining ongoing business continuity and disaster recovery planning.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Enterprise Information Security Program, Department of Information Technology (DIT), had the following objectives:

1. To assess the effectiveness* of DIT's efforts to fully implement an effective information security framework*.

2. To assess the effectiveness of DIT's efforts to evaluate and manage the State's exposure to information security risks.

3. To assess the effectiveness of DIT's efforts to evaluate and enforce compliance with information security policies and procedures.

Audit Scope

Our audit scope was to examine the information processing and other records related to controls over the Department of Information Technology's enterprise information security program. 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, performed from November 2005 through July 2006, generally covered the period December 1, 2002 through July 12, 2006.

Audit Methodology

The criteria used in the audit included control objectives and audit guidelines outlined in the Control Objectives for Information and Related Technology* (CobiT) issued by the Information Systems Audit and Control Foundation (ISACF) in July 2000, guidelines issued by the National Institute of Standards and Technology (NIST), and other

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

information security and industry best practices. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review of DIT's enterprise information security program. We reviewed and obtained an understanding of DIT's policies and procedures related to information security. We obtained an understanding of the Office of Enterprise Security's roles and responsibilities for information security. We used the results of our review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

   We performed an assessment of DIT's efforts to establish an enterprise information security program in accordance with best practices. Specifically:

   a. Efforts to Fully Implement an Effective Information Security Framework:

      (1) We assessed DIT's information security framework and compared the information security framework against industry best practices.

      (2) We assessed the Michigan Information Technology Executive Council's activities, roles, and responsibilities for enterprise information security.

      (3) We reviewed and evaluated DIT's strategy for developing an enterprise information security training program.

      (4) We interviewed DIT management to obtain an understanding of DIT's information security governance* practices.

   b. Efforts to Evaluate and Manage the State's Exposure to Information Security Risks:

      (1) We interviewed DIT management to obtain an understanding of DIT's risk management program.

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

(2) We reviewed and analyzed DIT's procedures for identifying and remediating risks to the State's information systems and technical infrastructure.

(3) We reviewed and analyzed DIT's activities for integrating security into the information systems' system development life cycle.

(4) We assessed DIT's disaster recovery planning efforts for the State's information systems and technical infrastructure.

c. Efforts to Evaluate and Enforce Compliance With Information Security Policies and Procedures:

(1) We interviewed DIT management to understand how DIT measured the effectiveness of its information security program.

(2) We reviewed the activities of DIT's internal audit function.

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. To the extent practical, we add balance to our audit reports by presenting noteworthy accomplishments for exemplary achievements identified during our audits.

Agency Responses

Our audit report contains 9 findings and 11 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and has complied or will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agency's 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 DIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFORTS TO FULLY IMPLEMENT AN EFFECTIVE INFORMATION SECURITY FRAMEWORK

COMMENT

Background: Electronic information and information systems are critical to the operations of State agencies. Without an effective information security program, State agencies cannot ensure the confidentiality*, integrity*, and availability of their information and information systems. Risks to information systems are increasing with advances in technology and as more systems become interconnected or are accessible from the Internet.

The National Association of State Chief Information Officers (NASCIO), in its May 2006 research brief, *The IT Security Business Case: Sustainable Funding to Manage the Risks*, indicated that State governments may be increasingly targeted by both external and internal threats* because of their rich data stores. As other previously targeted sectors, such as the financial services sector, have implemented heightened security measures to deter such incidences, state governments may become a higher priority target for cyber-criminals.

According to statistics from the Department of Information Technology (DIT), in 2005, the Office of Enterprise Security (OES) stopped 1,791,936 e-mail virus attacks; 12,681,729 attempts to scan ports and gain unauthorized access; 7,802,369 spam e-mails; and 6,037 computer hijack attempts. This represents an increase of 203% from 2004 to 2005 of hijack attempts on State computer systems and the vital data contained on those systems.

Recent Office of the Auditor General audits have identified significant and widespread information security and control weaknesses, such as poor access controls to data and information systems, ineffective program and data change controls, unsecured operating systems and database management systems, and inadequate and untested disaster recovery plans (DRPs) (see Exhibit 1). As indicated in the audit reports, a primary cause for many of the security weaknesses was that DIT and the State agencies had not established a comprehensive information security program based on risk management principles. In the *Secure Michigan Initiative*, the State's chief information security officer (CISO) also reported similar security and control

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

weaknesses. The CISO concluded that if the recommendations in the *Secure Michigan Initiative* were not acted upon, State government IT systems would face serious consequences and risks. To be effective, the State's information security program requires support and commitment from all State agencies.

Audit Objective: To assess the effectiveness of DIT's efforts to fully implement an effective information security framework.

Conclusion: DIT's efforts to fully implement an effective information security framework were not effective. We noted four material conditions*:

- DIT had not fully developed its information security governance program (Finding 1).

- DIT had not fully implemented a comprehensive enterprise information security framework (Finding 2).

- DIT did not ensure that the Michigan Information Technology Executive Council (MITEC) security subcommittee provided effective information security governance for the State (Finding 3).

- DIT had not fully developed and implemented a comprehensive information security training program (Finding 4).

Implementing an effective information security framework is a complex process. Control Objectives for Information and Related Technology Framework (CobiT) established a maturity model (see Exhibit 2) for management to map the level of its controls compared to industry best practices. The levels range from 0 (nonexistent) to 5 (optimized). Our review indicates that level 2 best describes the maturity of DIT's enterprise information security program. Addressing the audit findings will help DIT move to a higher maturity level to ensure its information security program results in the establishment of more consistent, cost-effective, and repeatable information security controls.

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

Noteworthy Accomplishments: The State's CISO was named Executive Alliance's Information Security Executive of the Year Central for 2006. The award recognizes individuals who have demonstrated outstanding leadership in the field of information security.

FINDING

1. Information Security Governance

   DIT had not fully developed its information security governance program. As a result, DIT cannot ensure that the State's information security practices will be implemented effectively and efficiently.

   Information security governance is the establishment and maintenance of the control environment to manage risks relating to the confidentiality, integrity, and availability of information and its supporting processes and systems. The IT Governance Institute (ITGI) in its report, *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, explained that information security is not only a technical issue, but a business and governance challenge that requires the active involvement of an organization's executives to assess emerging threats and to develop the organization's response to them.

   DIT's information security governance program had the following weaknesses:

   a. DIT did not ensure that security was fully integrated into all of its business processes, e.g., its information system development and acquisition process. Failure to integrate security into business processes increases the likelihood that DIT and the State agencies will treat security as a separate technical concern rather than an integral part of the business process. It also is more cost effective to ensure appropriate security measures are designed into the State's information systems rather than to correct a security weakness after the system is operational.

   b. OES did not fully assert its authority for establishing, implementing, and enforcing security practices across State agencies. For example, OES could ensure a more uniform and consistent approach to security by establishing Statewide security policies and procedures and mandating the minimum controls that must be included whenever a new system is developed.

Historically, OES has emphasized its role as a security advisor to State agencies. However, by not taking a stronger approach, OES cannot ensure State agencies are implementing good security practices in a consistent manner.

The OES charter assigned responsibility for the State's information security to OES and the CISO. However, the OES charter may not provide OES and the CISO with sufficient authority to implement and enforce security practices across State agencies. As such, DIT may need to seek an executive directive or legislation to obtain sufficient authority.

c. DIT did not allocate to OES sufficient resources to completely implement critical components of the *Secure Michigan Initiative*, such as disaster recovery and business continuity planning, certification* and accreditation* of systems, and risk assessment and mitigation planning. As such, DIT has not been able to fully implement an information security program for the State.

   In 2004, OES estimated that approximately $33 million would be required to remediate the weaknesses in the *Secure Michigan Initiative*. However, OES did not develop formal budget requests with specific cost estimates for the resources required to fully implement the *Secure Michigan Initiative*. DIT obtained approximately $5 million in federal grants for special security projects. The Government Accountability Office (GAO) has identified sufficient funding as a critical success factor for the establishment of an effective information security program.

d. OES had not fully developed and implemented operational plans* and project plans* to facilitate the implementation of all recommendations in the *Secure Michigan Initiative*. Failure to develop operational plans decreases the likelihood that DIT will successfully implement the recommendations.

   According to CobiT, operational plans should be developed that describe required information technology (IT) initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The operational plans should be sufficiently detailed to allow the definition of project plans. In addition, OES should develop specific project

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

plans for each of the *Secure Michigan Initiative's* focus areas covering the business and information system resources necessary to guide project execution and project control throughout the life of the project.

RECOMMENDATION

We recommend that DIT fully develop its information security governance program.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will continue to fully integrate security into its governance model and business processes. OES will continue to implement the *Secure Michigan Initiative,* which included actions to establish the implementation and enforcement of an information security framework across State agencies. DIT informed us that it launched Phase II of the State Unified Information Technology Environment* (SUITE) project, which includes the Software Engineering Model* (SEM). To ensure that the State integrates security best practices into business processes, OES will be an integral part of the SUITE implementation. DIT will work with its infrastructure areas and life cycle management process to ensure that, based on availability of resources, security issues are prioritized and addressed.

DIT informed us that OES has also submitted new Statewide policies to the Department of Management and Budget (DMB) for inclusion in the Administrative Guide, which will assist in asserting and enforcing security practices across State agencies. In addition, DIT informed us that it has developed detailed budget recommendations based on the DIT Strategic Security Plan. Lastly, DIT will prioritize all of the aforementioned projects and action items, with their associated expenditures, and work with other State agencies to implement security based on the availability of State resources.

DIT is a recognized leader in IT security for State government and believes that it has been highly successful in protecting the State's computer systems 24 hours a day, seven days a week. As a result, DIT is not aware of any data losses. DIT believes that some of the concerns identified in this audit represent an independent validation of the concerns identified by DIT's *Secure Michigan Initiative*, which DIT will continue to implement. The recently released DIT Strategic Security Plan will

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

address many of the remaining concerns identified in this report, with a number of resolutions scheduled in the months ahead.

FINDING

2. Enterprise Information Security Framework

DIT had not fully implemented a comprehensive enterprise information security framework. As a result, DIT cannot ensure that it and the State's agencies consistently and effectively implemented appropriate levels of security within the State's information systems.

An enterprise information security framework establishes the organization's overall approach to information security and internal control. According to COBIT, an enterprise information security framework integrates risk management and security plans, policies, and procedures to support the information security framework.

Our review of DIT's enterprise information security framework disclosed:

a. DIT did not develop a comprehensive enterprise security plan* for assessing risk, developing and implementing security procedures, and monitoring the effectiveness of these procedures for all State information systems. Without a well-designed enterprise security plan, security controls may be inadequate or inconsistently applied and responsibilities may be unclear or improperly implemented. Subsequent to our fieldwork, DIT informed us that it has drafted an enterprise security plan.

b. DIT did not develop a Statewide master information security policy. A Statewide master information security policy establishes an overall approach to managing information security for all State agencies.

According to ISO/IEC 17799:2005*, *Code of Practice for Information Security Management,* the policy should contain a brief explanation of security policies, principles, and standards; an explanation of responsibilities for information security; and references to more detailed documentation that supports the policy. To implement its policy across State agencies, DIT should publish the Statewide master information security policy in the DMB Administrative Guide.

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

c. DIT did not have a complete set of detailed information security policies and procedures to support an information security framework. For example, DIT had not fully developed policies and procedures for access controls, application security, and disaster recovery. In addition, DIT had not updated existing policies and procedures, such as DMB Administrative Guide policy 1310.02, on information processing security to reflect the establishment of DIT or to specify DIT's and the State agencies' roles and responsibilities.

   Although DIT developed several detailed security policies and procedures, it did so without the guidance of an overall Statewide master information security policy (see item b.). A lack of integrated policies and procedures impacts DIT's ability to effectively implement an enterprise information security framework. According to COBIT, management should develop and maintain a set of policies and procedures to support IT strategy. The policies and procedures should be periodically reviewed for changes in organizational, environmental, and technical requirements.

d. OES had not effectively communicated existing security policies and procedures to responsible individuals within DIT and the State. For example, we identified project managers responsible for new system development that were unaware of the OES Resource Guide. In addition, prior OAG audits identified DIT technical support staff that were unaware of DIT's policy for server security or DIT's adoption of COBIT standards. Without effective communication, OES cannot ensure that each individual understands his or her roles and responsibilities for information security.

   COBIT states that management should ensure that IT policies are communicated to appropriate staff and made an integral part of enterprise operations.

RECOMMENDATION

We recommend that DIT fully implement a comprehensive enterprise information security framework.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will fully implement a comprehensive enterprise information security framework. In January 2007, OES published the DIT Strategic Security

Plan, which outlines DIT's efforts to move enterprise security forward for fiscal years 2006-07 through 2009-10. DIT informed us that the Strategic Security Plan's major categories include a comprehensive set of security policies, training, risk reduction, business continuity, and an agency security plan template.

With regard to item b., DIT informed us that it had developed a Statewide master information security policy which establishes an overall approach to managing information security for all State agencies. In February 2007, DIT submitted the policy to DMB for publication in the DMB Administrative Guide.

With regard to item c., DIT informed us that it had updated many policies, procedures, and standards, although it recognizes the need for additional policies. DIT informed us that in February 2007, it submitted the policies to DMB for publication in the DMB Administrative Guide. These policies will form the basis for DIT's information security framework. As current policies are revised and new policies and procedures are developed, DIT plans to integrate them into the new information security framework.

With regard to item d., DIT will ensure that employees are trained on policies and procedures in accordance with the planned time lines as detailed in the DIT Strategic Security Plan.

FINDING

3. MITEC Security Subcommittee

DIT did not ensure that the MITEC security subcommittee provided effective information security governance for the State. A lack of effective information security governance by the MITEC security subcommittee impedes DIT's ability to integrate information security across State agencies. As a result, security gaps exist in information security that could lead to serious breaches or result in State agencies wasting limited resources on duplicate security initiatives.

Our review of the MITEC security subcommittee disclosed:

a. The security subcommittee did not make recommendations to DIT on the formal establishment of information security priorities. Establishing formal

recommendations would help DIT focus on those activities that best support the agencies' business objectives.

b. The security subcommittee had not established a formal monitoring and reporting process to assess the status of security action items. Without a formal monitoring and reporting process, MITEC cannot evaluate the progress and success of DIT's security initiatives.

c. During fiscal years 2004-05 and 2005-06, the security subcommittee did not have regularly scheduled meetings. Regularly scheduled meetings would help DIT and the security subcommittee ensure that information security is dealt with in a proactive and timely manner. The CISO informed us that the security subcommittee has resumed meeting on a regular basis.

Establishing an effective enterprise security program requires the support of the State's executive management. Because the chief information officer (CIO) delegated certain authority for security to MITEC, the CISO requires MITEC's cooperation and support to implement an effective enterprise information security program. Consequently, DIT and the CISO do not have the authority to unilaterally impose security standards on other State agencies regardless of need or cost. Therefore, the MITEC security subcommittee provides the mechanism for DIT and the State agencies to communicate and collaborate on the implementation of the State's information security strategy.

RECOMMENDATION

We recommend that DIT ensure that the MITEC security subcommittee provides effective information security governance for the State.

AGENCY PRELIMINARY RESPONSE

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

FINDING

4. Security Training

DIT had not fully developed and implemented a comprehensive information security training program. Without a fully implemented training program, DIT cannot be assured that the State's employees and contractors are knowledgeable about security threats and vulnerabilities, security controls, and mitigation techniques.

According to the *Secure Michigan Initiative* and the OES charter, OES is responsible for developing end-user security awareness training; coordinating training sessions on security architecture, physical security, and other security issues; and training and communicating the enterprise-wide security program.

Our review of DIT's training program disclosed:

a. DIT did not identify information security training requirements for all DIT employees. Our review disclosed that OES had developed a strategic plan for assessing employee IT security training needs, developing employee training plans, and developing IT security training programs. The strategic plan identified IT security training topics and provided recommendations for training topics based on the employee's job role. However, OES did not ensure that its strategic plan for developing an employee information security training program was executed.

b. OES had not developed training to facilitate the implementation of its enterprise-wide information security program. MITEC security subcommittee members, project managers, and client service directors identified the need for training on risk management and incorporating security into the application development process. To improve the effectiveness of its enterprise information security program, OES should develop training to facilitate the implementation of all critical aspects of the program, such as the information security framework, IT security plans, risk assessments, and DRPs.

c. OES had not established a mechanism to ensure that State employees completed its end-user security awareness training program. As of July 2006, approximately seven months after its inception, only 3,018 (6%) of 53,100 State employees had completed the end-user security awareness training.

OES informed us that it had mandated the end-user security awareness training for all DIT employees and proposed to the Office of the State Employer mandating annual end-user security awareness training, but the Office of the State Employer would not authorize it. DIT's inability to mandate training and the lack of promotion by State agency management may have contributed to the low completion rate.

RECOMMENDATION

We recommend that DIT fully develop and implement a comprehensive information security training program.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will fully develop and implement a comprehensive information security training program. DIT informed us that its Strategic Security Plan provides for the establishment of an information security training plan and curriculum to be executed over the next four years. In fiscal year 2006-07, OES will develop a security curriculum and formally present the curriculum to DIT's Office of Employee and Financial Services for inclusion into employees' individual development plans.

DIT will again formally request the Department of Civil Service (DCS) 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 fiscal year 2007-08. DIT informed us that, to date, it has established a formal security awareness program through DCS's Quick Knowledge program and Michigan's cyber security Web site, <http://www.michigan.gov/cybersecurity>.

EFFORTS TO EVALUATE AND MANAGE THE STATE'S EXPOSURE TO INFORMATION SECURITY RISKS

COMMENT

Audit Objective: To assess the effectiveness of DIT's efforts to evaluate and manage the State's exposure to information security risks.

Conclusion: DIT's efforts to evaluate and manage the State's exposure to information security risks were moderately effective. Our assessment disclosed 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 high-risk or inappropriate Web sites. However, we noted three material conditions:

- DIT had not fully implemented a comprehensive enterprise information security risk management program (Finding 5).

- DIT needs to implement a more effective process for incorporating security throughout an information system's system development life cycle (Finding 6).

- DIT had not established an integrated and comprehensive process to oversee and direct the State's disaster recovery planning efforts. In addition, DIT did not have fully documented and tested DRPs for critical enterprise systems and the State's infrastructure. (Finding 7)

Noteworthy Accomplishments: In 2003 and 2004, the State received NASCIO recognition awards for security and emergency management. In 2003, the State won the award for the *Secure Michigan Initiative* project. The project included a rapid risk assessment to determine high-risk issues in relation to the security of the State's IT infrastructure, policies, procedures, and systems. The goal of the project was to develop a risk analysis to administer to every agency within State government based on State of Michigan requirements, federal guidelines, and IT industry best practices. The *Secure Michigan Initiative* resulted in specific recommendations to improve security for six high-risk focus areas.

In 2004, the State won the NASCIO award for the Michigan Critical Incident Management System (CIMS), the nation's first Statewide deployment of an integrated Geographic Information System (GIS) emergency management system. CIMS was developed by the Michigan Department of State Police's Emergency Management Division to automate key State Emergency Operations Center (SEOC) functions. During the August 2003 electrical blackout, DIT used CIMS to track and monitor data on the status of the State's critical infrastructure. Use of CIMS allowed DIT to quickly restore critical systems and desktop services in an orderly manner.

In February 2006, DIT participated in Cyber Storm, the first government-led cyber security exercise to examine the response, coordination, and recovery mechanisms to a simulated cyber event within international, federal, state, and local governments. The

exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures. The intent of the scenarios was to highlight the interconnectedness of cyber security with the physical infrastructure and to exercise coordination and communication between public and private sectors.

FINDING

5. Enterprise Information Security Risk Management Program

DIT had not fully implemented a comprehensive enterprise information security risk management program. As a result, DIT could not ensure that information and IT security risks were effectively identified, monitored, and mitigated. Also, the lack of a comprehensive enterprise risk management program inhibits DIT's ability to prioritize its activities in a way that reduces the State's IT security risk in the most cost-effective manner possible.

An enterprise risk management program is the organization's complete process for assessing risk, selecting and implementing cost-effective policies and controls, and monitoring and evaluating the effectiveness of established safeguards.

Our review of DIT's risk management program disclosed:

a. DIT had not established comprehensive enterprise risk management procedures for performing information security risk assessments. Therefore, DIT could not ensure its risk assessment process had developed to the point where a structured, organization-wide process is enforced, followed regularly, and managed well.

   DIT's *Secure Michigan Initiative* indicated that DIT should develop a Statewide policy and standard requiring risk management for IT systems. The *Secure Michigan Initiative* also indicated that DIT should develop a formal process for conducting risk assessments and mitigation plans. While DIT has several policies that require IT risk assessments, the policies are not integrated and do not provide sufficient detailed guidance to the user about how to perform a risk assessment and about the risk management process.

b. DIT had not fully developed a formal remediation* process to correct the lessons learned from information security incidents. Without a formal remediation process, DIT could not ensure the underlying cause of significant information security incidents was corrected in an effective and timely manner.

We selected a sample of 10 information security incidents that occurred between October 2004 and March 2006. OES could not provide documentation showing that DIT fully implemented its recommendations for long-term solutions to the 10 incidents. Many of the recommendations were delayed because of resource limitations or the need to develop new processes or change existing processes.

c. DIT did not develop a strategy to implement system security certification and accreditation processes within its information security risk management framework. Without system security certification and accreditation processes, DIT could not ensure the State's information system owners have properly considered and assessed the effectiveness of their information systems' security features and formally accepted any residual risk.

According to the National Institute of Standards and Technology (NIST), security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification.

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

DIT informed us that it did not have the resources required to fully implement a system security certification and accreditation process as prescribed by NIST.

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

Nevertheless, it is important that DIT develop a process which will result in State agencies developing their information systems with acceptable levels of risk in accordance with the objectives of the State's information system security program. DIT's certification and accreditation process should build on and leverage existing risk assessments and security audit requirements.

RECOMMENDATION

We recommend that DIT fully implement a comprehensive enterprise information security risk management program.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will establish more comprehensive enterprise risk management procedures to be used in performing security risk assessments. DIT informed us that while it has developed formal processes for responding to information security incidents, it will develop a formal process for tracking the remediation of "lessons learned" from information security incidents. In addition, OES will continue to expand the State's certification and accreditation efforts as resources become available.

DIT believes that it has achieved significant reforms and improvements in IT security controls since 2002. DIT takes security over the State's computer systems very seriously and it is important to note that the audit found 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 Web sites." DIT believes that it has made tremendous progress in its information security program and is working on new policies, procedures, and projects to address many of the concerns reported in this audit. DIT also noted that NASCIO and other external organizations have recognized DIT projects, such as intrusion detection systems, anomaly detection systems, Web and spam filtering, firewalls, and backup generators, as successful improvement in the State's IT security environment. DIT believes these award-winning projects have validated its successes in managing the reduction of IT security risk for the State.

FINDING

6. Incorporation of Security Throughout the System Development Life Cycle

DIT needs to implement a more effective process for incorporating security throughout an information system's system development life cycle (SDLC). Without improvements, DIT cannot ensure that the State agencies develop information systems with adequate security and controls and that the information systems remain properly secured.

According to NIST, security is most effective and efficient when planned and managed throughout an information system's SDLC, from initial system planning through design, implementation, and operation to disposal. NIST indicates that including security early in the SDLC will usually result in a less expensive and more secure system than adding it to an operational system. In addition, ongoing security reviews need to be conducted to ensure that security keeps up with changes in the system's environment, technology, procedures, and personnel.

OES's Agency Liaison Section assists agencies in selecting the appropriate security controls for their system development projects by performing security assessments. In November 2005, OES published the OES Resource Guide to assist agencies in selecting and implementing effective security controls for their information systems. OES informed us that the Resource Guide was based primarily on NIST standards for incorporating security into the information system SDLC.

Our review of DIT's new SDLC methodology, the OES Resource Guide, security assessments, and interviews with agencies' project managers disclosed:

a. DIT did not provide specific guidance on required security deliverables in its new SDLC methodology or the OES Resource Guide. A lack of specific guidance increases the likelihood that agencies will not ensure proper security controls are built into their information systems.

   The OES Resource Guide identified security deliverables, such as system categorization, risk assessments, security requirements, and security test plans, that should be included in the development of new information systems. However, neither the new SDLC nor the Resource Guide provided guidance to agencies on how to prepare the necessary security deliverables.

b. DIT's SDLC methodology did not ensure that OES security liaisons were involved at the start of an agency's information system development project. The project managers informed us that the OES security liaison did not provide a security assessment until after the system had been designed. As a result, the agencies were less likely to implement the recommended controls.

c. OES had not established standards for the security assessment's format or content. As a result, OES did not always perform uniform and comprehensive security assessments.

   We reviewed a sample of six security assessments for active information system development projects. We noted that the security assessments did not follow a standard format, contain standard content, or consistently address a complete set of generally accepted information security controls. In some instances, we could not determine from the security assessments what security controls were reviewed.

d. DIT did not ensure that OES's security liaison function had assigned sufficient staff to provide effective oversight of the State's information system development projects. The lack of oversight increases the risk that information systems will be implemented with serious security weaknesses.

   Seven agencies, including DMB, DCS, and DIT, did not provide resources for a dedicated security liaison. The lack of a security liaison for these three agencies is of particular concern because they are the State's central control agencies and their Statewide information systems impact large numbers of users. In addition, six agencies only provided resources for a part-time security liaison.

   To provide some oversight, OES assigned security liaisons to work on the seven agencies' major development projects in their down time. As a result, the security liaisons did not provide ongoing security assessments for all phases of an information system's SDLC. The security liaisons focused their activities primarily during a system's initiation and development phases. However, without subsequent involvement in the development process, DIT cannot ensure an information system's controls were implemented properly and continue to operate as intended.

RECOMMENDATION

We recommend that DIT implement a more effective process for incorporating security throughout an information system's SDLC.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will implement a more effective process for incorporating security throughout an information system's SDLC.

With regard to item a., DIT will continue to fully integrate security and security guidance into its governance model and business processes, such its SDLC methodology. DIT informed us that the implementation team for the Phase II SUITE project includes OES and that DIT has begun the process of incorporating deliverables from the OES Resource Guide into SEM.

With regard to items b. and d., DIT will develop additional guidance about how and when to involve security liaisons. The guidance will be incorporated into SUITE and SEM. Furthermore, DIT informed us that it has increased security liaison support to DMB and DCS and it is working with other client agencies to increase the number of security liaisons and provide security guidance and expertise.

With regard to item c., OES will establish standards for the security assessment's format and content.

FINDING

7. Disaster Recovery Planning

DIT had not established an integrated and comprehensive process to oversee and direct the State's disaster recovery planning efforts. In addition, DIT did not have fully documented and tested DRPs for critical enterprise systems and the State's infrastructure. This increases the likelihood that a service interruption will significantly impact the State's business operations.

In March 2003, the director of DMB established the Continuity of Government Initiative (COGI) to coordinate the development of a comprehensive plan to ensure the continuity of the critical functions* of all agencies if normal operations are

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

interrupted by natural forces or other occurrences. COGI will result in a Statewide business continuity plan. As part of the initiative, DIT partnered with State agencies to assist in their development of business continuity plans and DRPs.

We reviewed DIT's activities to assist State agencies and DIT's DRPs for selected enterprise systems. Our review disclosed:

a. DIT had not established a project team responsible for disaster recovery planning. Disaster recovery planning is a significant process that requires coordination and resources from DIT and the State agencies. As such, DIT should establish a project team that is responsible for creating the organizational structure, disaster recovery framework, policies, procedures, and implementation guidance for assisting State agencies in developing DRPs. During our fieldwork, DIT's Agency Services initiated an effort to develop disaster recovery information for critical systems. However, DIT's Agency Services did not coordinate its activities with OES.

b. DIT had not completed and validated its identification of information systems supporting agency critical functions identified for COGI. In addition, for each information system, DIT had not obtained all relevant information that it deemed necessary to assist in disaster recovery efforts. A lack of complete, accurate information diminishes DIT's ability to effectively respond in the event of a disaster.

c. DIT, in conjunction with DMB and State agencies, had not established recovery priorities for all critical functions identified for COGI. In the event of a major disaster, DIT should direct its limited resources to first recovering the State's most critical functions. At a minimum, DIT and State agencies need to prioritize their agency's information systems and establish an overall priority for recovering information systems from a Statewide perspective.

d. DIT did not ensure that agency service level agreements (SLAs) contained detailed descriptions of DIT's and the State agencies' responsibilities and agency resources required for disaster recovery. In addition, DIT did not ensure the SLAs contained specific information regarding the expected availability and functionality of critical systems. For 2 (50%) of the 4 SLAs we reviewed, the SLA did not contain specific system requirements.

DIT informed us that the SLAs documented expected time frames for restoring agency systems. However, to successfully recover agency systems in the expected time frame, agencies must provide DIT the necessary resources, such as funding for redundant hardware and fully documented and tested DRPs. The SLAs did not clearly communicate these requirements. This may result in an expectation gap between DIT and the agencies regarding DIT's ability to restore information systems within the expected time frame.

e. DIT did not require all DRPs to be stored and managed in a central repository. DIT's Data Center Operations developed a central repository for mainframe DRPs; however, DIT did require other DIT organizations and State agencies to store their plans in the repository. A central repository would help ensure DRPs are accessible to the appropriate individuals in the disaster recovery process. A central repository would also help ensure that DRPs are kept up-to-date and properly backed up.

f. DIT policy did not require State agencies to host information systems supporting agencies' critical functions in the State's data center. According to the COGI listing, agencies hosted critical information systems in 20 locations outside of the State's data center. Hosting critical systems outside of the State's data center may increase the risk to the system because the other hosting sites do not have the same level of security and environmental support as the State's data center. In addition, the systems hosted outside the State's data centers were less likely to have documented and tested DRPs. DIT contracted for a risk assessment of physical security at hosting sites outside the State's data center. The risk assessment indicated that 6 (30%) of 20 sites where critical systems were hosted were classified by the contractor as high-risk facilities and 12 (60%) of 20 sites were not included in the risk assessment. The risk assessment indicated that the other two facilities had acceptable risk.

g. DIT had not developed DRPs for all systems supporting DIT critical functions and for the State's infrastructure. Without documented and tested DRPs, DIT may not be able to meet its obligations to recover agency systems in accordance with service level agreements or provide critical services in the event of an emergency. DIT identified 13 critical functions on the COGI listing. However, DIT had not identified the systems supporting its critical functions nor had DIT developed DRPs for these systems.

In addition, DIT had not completed or updated DRPs for all enterprise information systems. Our review of the DRPs for two of the State's mainframes indicated that the DRPs were incomplete and had not been updated since 2000. Further, the DRPs included recovery assumptions that had not been validated.

According to COBIT, organizations should minimize the business impact of major disruptions by aligning a tested DRP with the overall business continuity plan and its related business requirements.

RECOMMENDATIONS

We recommend that DIT establish an integrated and comprehensive process to oversee and direct the State's disaster recovery planning efforts.

We also recommend that DIT fully document and test DRPs for critical enterprise systems and the State's infrastructure.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will develop an integrated and comprehensive process to oversee and direct the State's disaster recovery planning. DIT informed us that, in the spring of 2006, it began a project to identify critical business functions that are supported by IT infrastructure and systems within DIT. The project includes developing recommendations for an organizational structure, funding model, and staffing to support the disaster recovery framework, policies, procedures, and implementation guidance for DIT and DIT's customers. DIT plans to integrate the resulting disaster recovery framework into SUITE as well as daily work processes, such as problem management, configuration management, change management, and incident management. DIT also informed us that it has authorized a new position within Data Center Operations to oversee the disaster recovery processes. In addition, DIT informed us that it has set a goal to identify and validate the disaster recovery information for 35 critical State IT functions by December 2007.

EFFORTS TO EVALUATE AND ENFORCE COMPLIANCE WITH INFORMATION SECURITY POLICIES AND PROCEDURES

COMMENT

Audit Objective: To assess the effectiveness of DIT's efforts to evaluate and enforce compliance with information security policies and procedures.

Conclusion: DIT's efforts to evaluate and enforce compliance with information security policies and procedures were moderately effective. However, we noted two material conditions:

- DIT did not sufficiently staff its internal audit function to effectively audit the State's IT environment. In addition, DIT did not coordinate with State agencies to ensure that sufficient IT audit resources were assigned to audit application controls for critical information systems. (Finding 8)

- OES had not fully developed and implemented performance metrics for critical components of its information security program (Finding 9).

FINDING

8. IT Internal Audit Function

DIT did not sufficiently staff its internal audit function to effectively audit the State's IT environment. In addition, DIT did not coordinate with State agencies to ensure that sufficient IT audit resources were assigned to audit application controls for critical information systems. Without an effective IT audit function, DIT and State agencies cannot obtain assurance that IT controls have been properly designed and placed into operation. The Institute of Internal Auditors' Global Technology Guide, *Management of IT Auditing*, states that the limited presence of an IT internal audit function in a large and complex IT environment, such as the State's, represents a significant deficiency and a strong indicator that a material internal control weakness over financial statement reporting exists.

Executive Order No. 2001-3, which created DIT, transferred all aspects of the management of IT, including security, to DIT. Act 431, P.A. 1984, as amended, requires State agencies to establish effective internal controls over their operations and provide assurance that the internal controls are functioning as intended. DIT and the State agencies agreed in their SLAs to split responsibility for IT controls.

DIT and the agencies agreed that DIT is primarily responsible for ensuring the effectiveness of general controls; whereas agencies are primarily responsible for ensuring the effectiveness of their information systems' application controls. Per the SLAs and in accordance with the Executive Order, DIT has the authority and responsibility to ensure application controls for critical agency information systems are periodically audited.

DIT's Office of Internal Audit (OIA) consists of an IT audit manager and one IT audit specialist position which, at the time of our review, was vacant. Without a sufficient number of appropriately skilled IT auditors, DIT cannot effectively evaluate and monitor the internal control and security over the State's information systems.

OIA developed an audit plan for fiscal years 2003-04 through 2005-06 that identified high-risk control areas. However, OIA had completed only 2 (7%) of 29 planned reviews of the high-risk control areas because of staff limitations and management's assignment of nonaudit activities. The internal auditor informed us that DIT management was considering expanding DIT's internal audit function. However, specific funding for the positions has not been identified.

Similarly, State agencies did not assign sufficient IT audit resources to audit application controls of critical information systems. At the time of our review, 19 State agencies had a total of 4.5 dedicated IT audit positions and a total of approximately 4.75 additional audit positions to perform IT related reviews and assist in system development projects. The agencies completed just 11 IT related audits for fiscal years 2002-03 through 2004-05. Only 2 (18%) of the 11 IT related audits performed were for critical information systems. This shortage of IT audit resources was also reported in the Plante & Moran, LLP, August 2001 report entitled *State of Michigan Internal Audit Project,* which stated that the State's IT internal audit resources were limited and that most of the State's internal audit departments provided little or no IT audit coverage. The report indicated that, given the growth of technology in State government, the lack of IT audit resources is a potential major control weakness. The report recommended that the State consider establishing a pool of IT audit resources in DIT.

RECOMMENDATIONS

We recommend that DIT sufficiently staff its internal audit function to effectively audit the State's IT environment.

We also recommend that DIT coordinate with State agencies to ensure that sufficient IT audit resources are assigned to audit application controls for critical information systems.

AGENCY PRELIMINARY RESPONSE

DIT agrees and recognizes the importance of internal audit. DIT informed us that it recently hired an auditing specialist to focus internal audit efforts in the infrastructure area. DIT will continue to strengthen and integrate internal controls into its governance model and business processes. With the SUITE project, DIT will continue to explore all alternatives to increase monitoring of internal controls, including internal audit involvement, monitoring, and reporting. In addition, DIT will continue the work with its infrastructure areas and life cycle management processes to ensure that, based on availability of resources, internal controls are addressed. DIT informed us that during fiscal year 2005-06, it worked with DMB and DCS to advocate for the need for additional audit resources and to recognize IT auditing as a specialty. DIT will continue to recommend that State agencies ensure sufficient IT audit resources are assigned to audit application controls for their critical applications.

FINDING

9. Performance Metrics for IT Security Program

OES had not fully developed and implemented performance metrics for critical components of its information security program. Without complete metrics, OES cannot fully measure the effectiveness of its information security program.

Performance metrics provide a means for monitoring and reporting the implementation of security controls. They also help assess the effectiveness of these controls in appropriately protecting information resources in support of the organization's mission. COBIT indicates that effective IT performance management requires a monitoring process which includes defining relevant performance indicators, a systematic and timely reporting of performance, and prompt acting on deviations. As such, OES should establish metrics to measure DIT's progress in

implementing the *Secure Michigan Initiative*. For example, metrics related to the *Secure Michigan Initiative* could include:

- The percentage of critical systems with risk assessments.
- The percentage of critical systems with a documented security plan.
- The percentage of critical systems with a documented and tested DRP.
- The percentage of security incidents caused by improperly configured access controls.
- The percentage of end-users who have received basic awareness training.
- The percentage of information system security personnel who have received security training.

OES captures and reports metrics related to the number of virus, worm, and spyware attacks on the State's network and the status of disaster recovery planning efforts for critical information systems. However, establishing a more complete set of information security metrics will enable both OES and DIT management to monitor the status and progress of DIT's information security program over time. The metrics will help OES establish a direct relationship between its security program activities and the business operations of State agencies, thereby helping to demonstrate the value of information security.

RECOMMENDATION

We recommend that OES fully develop and implement performance metrics for critical components of its information security program.

AGENCY PRELIMINARY RESPONSE

DIT agrees and OES will fully develop and implement performance metrics for critical components of DIT's information security program. OES informed us that it 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 DIT Strategic Security Plan has specific actions, deliverables, performance metrics, and deadlines.

This Page Left Intentionally Blank

SUPPLEMENTAL INFORMATION

ENTERPRISE INFORMATION SECURITY PROGRAM

Department of Information Technology

Summary of Office of the Auditor General Information Technology Audit Report Findings

Released October 2001 through July 2006

Project Number	Department	Report Title	**Application Controls**	Input Controls	Output Controls	Processing Controls	Internal Controls	Assessment of Systems Effectiveness and/or Efficiency
07-598-01	DMB	Telecommunication Services and Enterprise Security						
27-590-01	Treasury	Automated Information Systems						
27-550-01	Treasury	Information Technology Services and the Automated Information Systems, Bureau of State Lottery						
19-595-02	DCS	Human Resources Management Network (HRMN)		R	R	R		R
07-560-02	DIT	Michigan Information Database		R				
07-594-02	DIT	Michigan Administrative Information Network					R	
19-596-03	DCS	Human Resources Management Network (HRMN) Self-Service						M
23-590-03	State and DIT	Automated Information Systems						
23-591-04	State and DIT	Qualified Voter File and Digital Driver's License Systems						
39-596-04	DIT and DCH	General Controls of the Medicaid Management Information System (MMIS)						
47-591-04	DOC and DIT	Accuracy of Prisoner Release Dates				M/R	R	
50-520-04	DIT	Teradata Data Warehouse						
50-505-04	DIT	Interdepartmental Billings and Selected Service Delivery Evaluation Efforts						
50-515-04	DIT and DMB	Computer Equipment Surplus and Salvage						
55-595-04	MSP	Sex Offender Registries						M/R
43-595-05	DHS and DIT	Michigan Child Support Enforcement System		R				R

DCH - Department of Community Health
DCS - Department of Civil Service
DHS - Department of Human Services
DIT - Department of Information Technology
DMB - Department of Management and Budget
DOC - Department of Corrections
MSP - Michigan Department of State Police

M - Material Condition
R - Reportable Condition

General Controls	Access Controls	Backup and Disaster Recovery Controls	Data and Program Change Controls	Environmental and Physical Security Controls	Management and Organization Controls	System Development and Documentation	Database Controls	Firewall Controls	Operating System Configuration	Project Management	System Security	Vulnerability Assessment and Penetration	Contract Management and Acquisition Controls	Other Information Technology Related Issues
	R	R			M/R			M/R	R			M		R
	M		M		M									
	R		R		R		R		R					R
			R		R	R				R				
	R				R									
	R		R		R	R								
	M/R		R	R					R					
	M		M		M									
											M		M	
	M	M	M		M	R				R	M			
	M				M									
					M/R		M/R		M					R
				R	R									
														R
							R							R

ENTERPRISE INFORMATION SECURITY PROGRAM
Department of Information Technology
Control Objectives for Information and Related Technology (COBIT) Maturity Model
DS5 Deliver and Support
Ensure Systems Security

Source: COBIT 4.0, used by permission of the IT Governance Institute. ©1996, 1998, 2000, 2005 IT Governance Institute. All rights reserved. COBIT is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

DS 5 Deliver and Support

Ensure Systems Security

Process Importance H

Management of the process of *Ensure Systems Security* that satisfies the business requirements for IT of *maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents* is

0 Non-existent when
The organization does not recognize the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognizable system security administration process.

1 Initial/Ad Hoc when
The organization recognizes the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when
Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analyzed. Services from third parties may not address the specific security needs of the organization. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see that IT security is within its domain.

3 Defined Process when
Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business but is only informally scheduled and managed.

4 Managed and Measurable when
Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorization are standardized. Security certification is pursued for staff who are responsible for the audit and management of security. Security testing is done using standard and formalized processes leading to improvements of security levels. IT security processes are co-ordinated with an overall organization security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is

planned and managed in a manner that responds to business needs and defined security risk profiles. KGIs and KPIs for security management have been defined but are not yet measured.

5 Optimized when
IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimized and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analyzed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organizationwide. KGIs and KPIs for security management are collected and communicated. Management uses KGIs and KPIs to adjust the security plan in a continuous improvement process.

GLOSSARY

accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
availability	Ensuring timely and reliable access to and use of information.
certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
CIMS	Critical Incident Management System.
CIO	chief information officer.
CISO	chief information security officer.
COGI	Continuity of Government Initiative.
confidentiality	The assurance that information is not disclosed to unauthorized individuals or processes.
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.

critical function	According to COGI, critical functions are a direct public service, the cessation of which would immediately affect the safety, health, subsistence, and welfare of the public, or would have an impact such that the ability of state government to operate would be curtailed.
DCS	Department of Civil Service.
disaster recovery planning	Developing and testing written plans for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.
DRP	disaster recovery plan.
effectiveness	Program success in achieving mission and goals.
enterprise	An organization. In the context of this audit report, encompasses DIT and all executive agencies and non-executive agencies with information systems connected to the State's network.
enterprise information security program	According to the Government Accountability Office (GAO), key elements of an enterprise information security program include: identifying and assessing information security risks in terms of business needs, establishing a central management focal point, implementing appropriate policies and related controls, promoting security awareness, and monitoring and evaluating policy and control effectiveness.
enterprise security plan	A document that contains the plan of action that the enterprise intends to use to address its security risks based on the context in which the enterprise operates and a thorough risk review.

information security governance	The establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity, and availability of information and its supporting processes and systems.
information security framework	An organization's overall approach to information security and internal control. An information security framework integrates risk management and security plans, policies, and procedures to support the information security framework.
information security policy	A document that addresses at the enterprise level the issues of security awareness, responsibility, behavior, and deterrence. This is a component of an enterprise security plan.
information technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
infrastructure	In information technology and on the Internet, the physical hardware used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, cable television lines, and satellites and antennas, and also the routers, aggregators, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.
integrity	The accuracy, completeness, and timeliness of data in an information system.
ISO/IEC 17799:2005	A detailed security standard published by the International Standards Organization (ISO). The standard is organized into 10 major sections.

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.
metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
MITEC	Michigan Information Technology Executive Council.
National Association of State Chief Information Officers (NASCIO)	An association that represents state chief information officers and information resource executives and managers from the 50 states, six U.S. territories, and the District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy. NASCIO's vision is government in which the public trust is fully served through the efficient and effective use of technology.
NIST	National Institute of Standards and Technology.
OES	Office of Enterprise Security.
OIA	Office of Internal Audit.
operational plan	Detailed plans for achieving the goals and objectives of a strategic plan.
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.

project plans	A formal, approved document used to guide both project execution and project control. The primary uses of the project plan are to document planning assumptions and decisions; to facilitate communication among stakeholders; and to document approved scope, cost, and schedule baselines.
remediation	Giving a solution or improvement of a problem or difficulty.
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. This part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses.
risk management	The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The ongoing process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.
SDLC	system development life cycle.
Secure Michigan Initiative	A self-assessment report published by DIT in 2003 that identified the security risks, threats, and vulnerabilities of the

	State's entire computer system and provided security recommendations to minimize the identified risks, threats, and vulnerabilities.
security awareness	A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.
SLA	service level agreement.
Software Engineering Model (SEM)	SEM provides guidance for information systems engineering related project management activities and quality assurance practices and procedures. The primary purpose of the methodology is to promote the development of reliable, cost-effective, computer-based solutions while making efficient use of resources. Use of the methodology will also aid in the status tracking, management control, and documentation efforts of a project.
State Unified Information Technology Environment (SUITE)	A framework for facilitating IT projects within the State of Michigan. SUITE encompasses the disciplines of project management, requirements management, systems development, quality assurance (QA), and software configuration management (SCM).
threat	An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.
vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by the threat source.

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL