MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

TERADATA DATA WAREHOUSE

DEPARTMENT OF INFORMATION TECHNOLOGY

November 2005

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

> "...The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof."
>
> – Article IV, Section 53 of the Michigan Constitution

Audit report information may be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Teradata Data Warehouse

Department of Information Technology

Report Number:
50-520-04

Released:
November 2005

The State's Teradata data warehouse (Data Warehouse) is a centralized repository of data used to support State agencies' decision-making and business processes. Much of the data stored on the Data Warehouse is considered sensitive or confidential. State agencies extract data from source systems, transform and format the data, and load the data into the Data Warehouse. State agencies use analytical tools to query data stored on the Data Warehouse to obtain accurate and timely information to support business decisions and for State and federal reporting.

Audit Objective:
To assess the effectiveness of the Department of Information Technology's (DIT's) processes to ensure the confidentiality, integrity, and availability of data within the Data Warehouse.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Conclusion:
DIT's processes to ensure the confidentiality, integrity, and availability of data within the Data Warehouse were ineffective.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Material Conditions:
DIT had not developed a server security plan for the Data Warehouse. Without a documented server security plan, DIT cannot ensure that the Data Warehouse's security requirements are appropriately addressed and consistently applied. (Finding 1)

DIT had not effectively secured the operating systems of the Data Warehouse servers. As a result, DIT cannot ensure that data residing on the servers is protected from unauthorized modification, loss, or disclosure. (Finding 2)

DIT had not established effective security over the Data Warehouse's database. As a result, DIT could not ensure the confidentiality, integrity, or availability of data residing within the Data Warehouse. (Finding 3)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Reportable Conditions:
DIT did not always reconcile data transferred between source systems and the Data Warehouse (Finding 4).

DIT's strategic plan did not include detailed strategic planning requirements for the Data Warehouse (Finding 5).

DIT had not established a Statewide privacy framework to govern the use of confidential and sensitive data maintained in information systems, such as the Data Warehouse. In addition, DIT had not established standards for data-sharing agreements between users of State data. (Finding 6)

DIT had not established data management standards (Finding 7).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Noteworthy Accomplishments:
In 2001 and 2002, the State was awarded National Association of State Chief Information Officers (NASCIO) recognition awards for projects developed on the Data Warehouse.

In 2001, the State was awarded the NASCIO Recognition Award for Innovative Use of Technology for the Department of Treasury's FARSTaR Project.

In 2002, the State was awarded the NASCIO Recognition Award for Enterprise Information Architecture for the Department of Community Health's development of a unique client identifier.

In 2004, DIT sponsored a Michigan Data Warehouse Users Group conference. The purpose of the conference was to bring together the State's data warehousing community, to create a resource to support all Data Warehouse users, and to introduce the Data Warehouse and demonstrate how it is used it in the State.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 7 findings and 8 corresponding recommendations. DIT's preliminary responses indicate that it agreed with all of the findings and will comply with all of the recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

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

November 1, 2005

Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan

Dear Ms. Takai:

This is our report on the performance audit of the Teradata Data Warehouse, Department of Information Technology.

This report contains our report summary; description of Teradata Data Warehouse; audit objective, scope, and methodology and agency responses; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

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.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

TERADATA DATA WAREHOUSE
DEPARTMENT OF INFORMATION TECHNOLOGY

Page

INTRODUCTION

COMMENT, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Teradata Data Warehouse

The State's Teradata data warehouse* (Data Warehouse) is a centralized repository of data used to support State agencies' decision-making and business processes. The Data Warehouse contains a large volume of historical data from multiple data sources. Much of the data stored on the Data Warehouse is considered sensitive or confidential. For example, the Data Warehouse contains client and payment data for the Medicaid program; Women, Infants, and Children (WIC) Program; Newborn Metabolic and Hearing Screening program; and Epidemiology program. Other data stored on the Data Warehouse includes detailed State and federal tax return data, vital records data, Michigan court and offender data, and parental locator data used for child support enforcement.

Periodically, State agencies extract data from source systems, transform and format the data, and load the data into the Data Warehouse. State agencies use analytical tools to combine and query data stored on the Data Warehouse to obtain accurate and timely information to support business decisions and for State and federal reporting. Agencies may also use data stored on the Data Warehouse as input for other business applications.

The Department of Information Technology anticipates that the Data Warehouse will help State agencies accomplish the following:

a. Increased revenue collection by improving the identification of tax fraud and abuse and by reducing and recovering taxes owed to the State.

b. Reduced cost of administering essential public health and education programs by providing advanced decision support solutions.

c. Improved public safety and protection of citizens by improving communications and information-sharing among law enforcement agencies, State courts, public health agencies, and the federal Department of Homeland Security.

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

d. Achieved operating efficiencies by making faster and more effective decisions; by responding more quickly to federal and State reporting requirements; and by providing timely and accurate information to the Governor, the Legislature, and taxpayers.

e. Improved planning and future policy decisions by analyzing program results and conducting predictive analyses to better plan and allocate limited State resources.

The Data Warehouse is maintained, updated, and managed by Data Center Operations, Technical Services, and Agency Services within the Department of Information Technology. Data Center Operations is responsible for the configuration, support, and maintenance of the Data Warehouse's operating system* and relational database management system*. Technical Services manages servers that support the Data Warehouse tools and utilities. Agency Services is responsible for the design and development of agency applications and databases*. In addition, Agency Services has been assigned responsibility for managing the security over agency data resources.

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

Audit Objective, Scope, and Methodology
and Agency Responses

Audit Objective

The objective of our performance audit* of the Teradata Data Warehouse, Department of Information Technology (DIT), was to assess the effectiveness* of DIT's processes to ensure the confidentiality, integrity, and availability of data within the State's Teradata data warehouse (Data Warehouse).

Audit Scope

Our audit scope was to examine the information processing and other records of the State's Teradata data warehouse. 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.

Audit Methodology

Our methodology included examination of DIT's information processing and other records primarily for the period July 1, 2004 through January 31, 2005. We performed our audit fieldwork from July 2004 through January 2005. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in the Control Objectives for Information and Related Technology framework* (COBIT), as issued by the Information Systems Audit and Control Foundation (ISACF) in July 2000, as well as other information security and vendor best practices. To accomplish our audit objective, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We collected background information about the Data Warehouse. We obtained an understanding of the internal control* pertaining to data stored within the Data Warehouse. We used this analysis to determine the extent of our detailed analysis and testing.

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

2. Detailed Analysis and Testing Phase

   We performed an assessment of the effectiveness of DIT's processes to ensure the confidentiality, integrity, and availability of data within the Data Warehouse. Specifically:

   a. We reviewed the security and configuration of the Data Warehouse's operating system and relational database management system.

   b. We evaluated DIT and agency controls over access to data.

   c. We evaluated security and controls over the agencies' extract, transform, and load scripts. In addition, we reviewed agencies' policies and procedures to ensure the completeness of the extract, transform, and load process.

   d. We evaluated DIT's standards and procedures for documenting and defining the data stored on the Data Warehouse. In addition, we reviewed and assessed the agencies' standards and procedures for data sharing.

   e. We reviewed and assessed DIT's procedures for backup and disaster recovery.

3. Evaluation and Reporting Phase

   We evaluated and reported on the results of the detailed analysis and testing phase. This report summarizes information system security weaknesses. Specific information system security weaknesses have been reported separately to DIT management.

Agency Responses

Our audit report contains 7 findings and 8 corresponding recommendations. DIT's preliminary responses indicate that it agreed with all of the findings and will comply with all of the recommendations.

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.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF PROCESSES TO ENSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF DATA

COMMENT

Background: Prior to the establishment of the Department of Information Technology (DIT), the responsibility for the development, management, and security of the State's Teradata data warehouse (Data Warehouse) databases resided with individual State agencies. Executive Order No. 2001-3 transferred the responsibility for the management and security of the Data Warehouse to DIT. Factors surrounding the transfer of responsibility from State agencies to DIT contributed to the findings in this report. Such factors include limited Statewide security policies and procedures as well as the need to define DIT and agency roles and responsibilities. DIT had identified these and other risk factors in the *Secure Michigan Initiative.* However, DIT has not implemented its recommendations.

Audit Objective: To assess the effectiveness of DIT's processes to ensure the confidentiality, integrity, and availability of data within the Data Warehouse.

Conclusion: DIT's processes to ensure the confidentiality, integrity, and availability of data within the Data Warehouse were ineffective. Our assessment disclosed three material conditions*. DIT had not developed a server security plan for the Data Warehouse (Finding 1). Also, DIT had not effectively secured the operating systems of the Data Warehouse servers (Finding 2). In addition, DIT had not established effective security over the Data Warehouse's database (Finding 3). Further, our assessment disclosed reportable conditions* related to database reconciliations, strategic planning, privacy framework, and data management standards (Findings 4 through 7).

Noteworthy Accomplishments: In 2001 and 2002, the State was awarded National Association of State Chief Information Officers* (NASCIO) recognition awards for projects developed on the Data Warehouse. In 2001, the State was awarded the NASCIO Recognition Award for Innovative Use of Technology for the Department of Treasury's FARSTaR Project. FARSTaR (Field Audit Research, Selection, Tracking, and Reporting) provides Department of Treasury auditors and support personnel access

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

to four years of detailed tax return data. As a result, the Department of Treasury has been able to increase its review of business tax returns from approximately 6,000 returns to 450,000 returns annually and improve its audit selection criteria to target the returns most likely to result in a recovery of unpaid taxes.

In 2002, the State was awarded the NASCIO Recognition Award for Enterprise Information Architecture for the Department of Community Health's (DCH's) development of a unique client identifier. The unique client identifier allows DCH to link program data from nine separate health-related agencies on the data warehouse. The integration of data allows DCH to more efficiently analyze client services and associated costs. Specifically, the system enables DCH to perform geographic analysis, cost-benefit analysis, and analysis of specific health care services and patterns of services and expenditures by provider, specialty, county, age, and other categories. This information helps DCH make better decisions about programs, providers, fees, and level of care in a more timely manner based on the knowledge of all services that a recipient is receiving.

In September 2004, DIT sponsored a Michigan Data Warehouse Users Group conference. Over 250 users from multiple State agencies attended the conference. The purpose of the conference was to bring together the State's data warehousing community, to create a resource to support all Data Warehouse users and prospective users, and to introduce the Data Warehouse and demonstrate how it is used in the State.

FINDING

1. Server Security Plan

   DIT had not developed a server security plan for the Data Warehouse. Without a documented server security plan, DIT cannot ensure that the Data Warehouse's security requirements are appropriately addressed and consistently applied.

   State security guidelines require system administrators to develop documented procedures for securely configuring each server connected to the State's network. In developing these procedures, system administrators should first identify vulnerabilities to the server and then assess what actions technical staff should take to reduce or eliminate these vulnerabilities. Server security issues such as operating system configuration, review and approval of system changes, ongoing assessment of information technology (IT) risks, physical security of system hardware, and recovery of system resources in the event of a disaster should be addressed in the server security procedures.

Our review of the Data Warehouse disclosed:

a. DIT did not perform periodic assessments of IT risks for the Data Warehouse. IT risk assessments would help DIT identify and reduce threats and vulnerabilities to the Data Warehouse. Risk assessments should be performed with the input of various stakeholders of the Data Warehouse, including end-users, system and database administrators, and DIT security personnel.

b. DIT had not completed a disaster recovery plan for the Data Warehouse. A documented and tested disaster recovery plan is necessary for the system administrator to restore the Data Warehouse in the event of a disaster, to identify any changes that might negatively affect the recovery process, and to ensure that IT resources are safe in the event of a disaster.

   Subsequent to our audit fieldwork, DIT completed and successfully tested its disaster recovery plan for the Data Warehouse.

c. DIT had not developed procedures for implementing new features of the relational database management system. The most recent version of the Data Warehouse's relational database management system had new features (such as roles and profiles, encryption, and audit trails) that, if implemented, would improve the administration and security of the Data Warehouse. However, without an implementation strategy, DIT may not consistently implement these new features. DIT should develop implementation procedures to ensure that database administrators understand, document, and implement new system capabilities.

d. DIT had not completely developed standards and guidelines for configuring and securing the operating systems of the Data Warehouse. Operating system configuration standards would provide system administrators with a documented benchmark to follow in securely configuring the operating systems of Data Warehouse servers and protecting the data that resides on those servers. DIT had developed operating system configuration guidelines for some of the Data Warehouse servers. However, developing standards and guidelines to assist in the configuration of all servers would help DIT secure its servers from internal and external threats.

The Control Objectives for Information and Related Technology framework (COBIT) states that effective implementation of system security requires the development of server security procedures that establish clear policies and standards, provide for cost-effective implementation, and include monitoring and enforcement processes. As such, DIT should grant its system administrators who are responsible for administering the Data Warehouse the authority to establish security standards.

RECOMMENDATION

We recommend that DIT develop a server security plan for the Data Warehouse.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to evaluate and implement reasonable cost-effective strategies that mitigate the level of risk to the State's servers. DIT informed us that it has established two positions within the Office of Enterprise Security dedicated to providing security services to existing enterprise platforms. DIT will formalize its strategy for conveying the new Teradata operating system and database management system release information to database administrators. Lastly, as noted in the audit report, DIT has completed and successfully tested a disaster recovery plan for the Data Warehouse. DIT will work to achieve full compliance by December 31, 2005.

FINDING

2. Operating System Security

DIT had not effectively secured the operating systems of the Data Warehouse servers. As a result, DIT cannot ensure that data residing on the servers is protected from unauthorized modification, loss, or disclosure.

COBIT recommends that system administrators securely configure operating systems to ensure that access to systems, data, and programs is restricted to authorized users. In addition, system administrators should grant only authorized users the minimum privileges required to perform their jobs.

Our review of operating system configurations for 12 Data Warehouse servers disclosed:

a. DIT had not assigned unique user codes to privileged users for 11 of the 12 servers. Data Center Operations staff use privileged accounts* to perform certain job responsibilities, such as installing software, resetting passwords, and configuring the operating system. To maintain accountability, the sharing of privileged accounts with identical user codes should be prohibited.

b. DIT did not lock or remove default system accounts for 9 of the 12 servers. An unauthorized person may attempt to access the operating system through a default system account. The locking or removal of unnecessary default system accounts by the system administrator reduces the vulnerability of the operating system from unauthorized access.

c. DIT did not completely restrict access for critical operating system configuration files for any of the 12 servers. Configuration files contain sensitive information that the operating system uses to perform tasks such as storing user passwords and running server applications and network services. Typically, ordinary users do not need access to these files. As such, DIT should restrict access to critical operating system configuration files to prevent unauthorized modification or access to the operating system configuration.

d. DIT had not implemented strong password rules for operating system user accounts on any of the 12 servers. The implementation of strong password rules for user accounts reduces the risk of unauthorized access to the operating system.

e. DIT did not completely lock or remove unnecessary operating system services on any of the 12 servers. The locking or removal of unnecessary operating system services reduces the risk of unauthorized access to the operating system, unavailability of system services, and the compromise of confidential data residing on the server.

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

f. DIT had not implemented a host-based intrusion detection system* (IDS) on 9 of the 12 servers. DIT procedures require the installation of host-based IDS on all servers connected to the State's network. The installation of a host-based IDS and the active monitoring of IDS activity provide the system administrator with the capability to prevent or detect unauthorized access to the operating system.

RECOMMENDATION

We recommend that DIT effectively secure the operating systems of the Data Warehouse servers.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to work to effectively secure the Data Warehouse operating system security. DIT informed us that it is currently testing new procedures and will continue to review and implement new security features, such as intrusion detection. DIT informed us that, despite the noted risks, DIT is not aware of any instances in which the confidentiality, integrity, and availability of the Data Warehouse were compromised. DIT will work to achieve full compliance by October 31, 2005.

FINDING

3. Database Security

DIT had not established effective security over the Data Warehouse's database. As a result, DIT could not ensure the confidentiality, integrity, or availability of data residing within the Data Warehouse.

Our review of the Data Warehouse's database disclosed:

a. DIT had not implemented strong password rules for database user accounts. Weak password rules increase the risk that an unauthorized person may easily compromise a password.

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

b. DIT had not established unique database administrator (DBA) user accounts. DBAs at Data Center Operations and Agency Services performed work using shared user accounts. To establish accountability and provide management with a means to monitor changes to the database, DIT should assign all users a unique account to perform their work. DIT informed us that it would begin assigning roles to individual users of the DBA user accounts to improve the accountability of those accounts.

c. DIT did not restrict users' access to database tables. In addition, DIT did not remove excessive default permissions granted to users. We sampled user permissions for selected database tables and determined that the DBAs granted permissions to add, change, or delete data to ordinary users. Most data stored on the data warehouse is used primarily for analysis and reporting. Therefore, to reduce the risk of unintentional or unauthorized modifications to the data, the DBAs should ensure that ordinary users have read-only access to database tables.

d. DIT did not monitor the activities of privileged users. Privileged users, such as the DBAs, have access capabilities that allow them to circumvent established controls and directly access and modify data. For some data tables, DIT logged the activities of privileged users. However, DIT had not developed reports or queries to allow for the monitoring of the activities. DIT informed us that it had not fully enabled the audit logging function because audit logging consumes a significant amount of system storage capacity. Recent enhancements to the Data Warehouse's software have provided DIT with the capability to establish system audit trails and monitoring processes without substantially increasing system overhead.

COBIT states that, to ensure system security, DIT should enable access controls to ensure that access to systems, data, and programs is restricted to authorized users.

RECOMMENDATION

We recommend that DIT establish effective security over the Data Warehouse's database.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will continue to work to effectively secure the Data Warehouse database security. DIT informed us that it is currently implementing agency services roles and profiles, creating unique administrator accounts, removing excessive default permissions, and enabling logging and monitoring controls. DIT will work to achieve full compliance by January 31, 2006.

FINDING

4. Database Reconciliations

DIT did not always reconcile data transferred between source systems and the Data Warehouse. Agency DBAs informed us that reconciliations were not performed for all systems. As a result, DIT could not ensure that data was accurately and completely transferred.

Reconciliation procedures may include a comparison of control totals, hash totals*, or record counts between the source system and the data warehouse. Reconciliation procedures may be performed manually or by using automated software tools. Although performing manual reconciliations is preferable to no reconciliation, automating the reconciliation process would help DIT ensure that reconciliations are performed on a timely and consistent basis.

COBIT recommends that organizations ensure that data entered into a system is checked for accuracy, completeness, and validity. Routine reconciliation of data transferred from source systems to the data warehouse is necessary to ensure the accuracy, completeness, and validity of data in the data warehouse. DIT informed us that the Data Warehouse has special utilities that can assist in the data reconciliation process. As such, DIT should establish procedures to verify that data from source systems matches data loaded onto the Data Warehouse.

RECOMMENDATION

We recommend that DIT reconcile data transferred between source systems and the Data Warehouse.

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

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding and will ensure that all data transferred between source systems and the Data Warehouse is reconciled. All new implementations will establish adequate reconciliation procedures and all existing implementations within the Department of Community Health and the Department of Human Services will be modified to include adequate reconciliations as part of the new base system implementations by October 2007. DIT expects all other implementations to be completed by January 2008.

FINDING

5. Strategic Planning

DIT's strategic plan did not include detailed strategic planning requirements for the Data Warehouse. As such, DIT cannot ensure that the State is utilizing its enterprisewide IT resources in the most efficient and cost-effective manner.

Executive Order No. 2001-3 directed DIT to lead State efforts to re-engineer the State's IT infrastructure with the goal of achieving the use of common technology across the executive branch. In response, DIT developed *Michigan's Information Technology Strategic Plan* to set the direction for IT in Michigan. In its strategic plan, DIT recognized the need to develop enterprisewide technology solutions to enable the State to standardize, consolidate, and coordinate IT resources among the various State agencies. Developing a detailed IT strategic plan specific to the Data Warehouse, would help DIT identify and address Data Warehouse issues affecting all State agencies, such as legal requirements, data management standards, and capacity planning.

In addition, to help ensure that the State achieves the long-term goals of the strategic plan, DIT needs to develop short-term operational plans to address issues affecting daily data warehouse operations, such as application development and security, operating system, and database configuration. COBIT recommends that the senior management of an organization assess IT issues and opportunities and develop long-term and short-term plans as part of a comprehensive strategic IT plan.

RECOMMENDATION

We recommend that DIT include in its strategic plan detailed strategic planning requirements for the Data Warehouse.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding. DIT informed us that it included the establishment of an enterprise data warehouse strategy as part of its strategic plan. DIT will work to achieve full compliance by September 30, 2006.

6. Privacy Framework

DIT had not established a Statewide privacy framework to govern the use of confidential and sensitive data maintained in information systems, such as the Data Warehouse. In addition, DIT had not established standards for data-sharing agreements between users of State data. Without an established privacy framework that includes standards for data-sharing agreements, the State cannot ensure that its agencies are properly protecting confidential and sensitive data from improper disclosure.

DIT's *Secure Michigan Initiative* identified protecting the privacy of data as a critical security mandate for State agencies that collect and retain sensitive data. *Secure Michigan Initiative* recommends that DIT implement policies and procedural safeguards that protect the privacy of sensitive information. Our review of DIT's data privacy efforts disclosed:

a. DIT had not established a framework for developing Statewide privacy policies and standards for the collection, use, and sharing of data. A privacy framework should address principles such as data collection, limitations on secondary uses of data, accountability, and computer security. In addition, the framework should provide guidance to State agencies for developing policies to address unique privacy requirements of data collected by those agencies.

b. DIT and agency management had not identified individuals to act as agency privacy officers. In addition, DIT and the agencies had not formally defined the roles and responsibilities of the agency privacy officer. According to the *Secure Michigan Initiative,* the agency privacy officer would be responsible for understanding how internal and external users use data the agencies maintain in their systems. In addition, the agency privacy officers would be responsible for assisting the agencies in classifying data according to its sensitivity and its importance to the agencies and other users of the data. Agency privacy officers should coordinate their activities with security administrators to ensure that data is properly secured.

c. DIT had not established standards for data-sharing agreements. Developing a model data-sharing agreement with required elements and criteria would help ensure that data-sharing agreements are consistent and in compliance with established policies and procedures.

We reviewed data-sharing agreements between two agencies that allowed for the exchange of sensitive data elements. We determined that these data-sharing agreements were not consistent in their content. For example, the data-sharing agreements did not consistently include provisions specifying how State agencies would notify individuals as to the use and disclosure of their personal information, how the agencies would share personal information, how the agencies would handle requests for data correction, and how long the agencies would retain information in the system. In addition, we noted that the agencies had not updated the data-sharing agreements to reflect subsequent changes in the agencies' organizational structures and personnel.

The DIT Office of Enterprise Security informed us that, in conjunction with Michigan State University, it has started a joint project on data privacy. DIT anticipates that the project will result in a privacy framework for the State.

RECOMMENDATIONS

We recommend that DIT establish a Statewide privacy framework to govern the use of confidential and sensitive data maintained in information systems, such as the Data Warehouse.

We also recommend that DIT establish standards for data-sharing agreements between users of State data.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding. DIT will establish a framework for developing Statewide privacy policies and standards for the collection, use, and sharing of data by October 1, 2006. In addition, DIT will continue to work with the agencies to establish privacy officers. DIT informed us that standards for data sharing agreements are an integral part of DIT's overall Data Warehouse strategy. As such, DIT will develop data sharing standards as part of the Data Warehouse strategy. The standards will include provisions regarding the use and disclosure of personal information and information retention. DIT expects data sharing standards to be defined and developed in fiscal year 2005-06 and to be implemented in fiscal year 2006-07.

FINDING

7. Data Management Standards

DIT had not established data management standards. Establishing data management standards will help ensure the quality and reliability of information produced by users. In addition, establishing data management standards will result in more efficient and secure application development by improving data security, reducing data redundancy, and easing exchanges of data between applications. Data management standards are especially important for information systems designed specifically for the purpose of sharing information, such as the Data Warehouse.

According to Executive Order No. 2001-3, the creation of DIT was expected to bring about improved information management and data sharing. The executive order requires DIT to determine and implement Statewide efforts to standardize data elements among the executive departments and agencies. Specifically:

a. DIT should ensure that data management standards include a metadata* model for the State's data warehouses. To be effective, the metadata model should specify the minimum required metadata elements and allow departments to extend the metadata elements specific to their unique requirements.

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

Reliable metadata is critical to the successful use of the Data Warehouse. It allows users to have more confidence in the data used to support business decisions. Metadata tells users information about data, e.g., the source of the data, how the data was transformed, and how to interpret the data. Inadequate metadata may create a number of data management problems, e.g., it may be difficult to identify the official record if multiple copies exist, to determine who should have access to a record, and to ensure the proper disposition of a record at the end of its retention period.

Although some DIT agencies and State departments have initiated projects to begin classifying data and developing metadata dictionaries, their efforts have not been guided by a common standard.

b. DIT should ensure that data management standards require the development of standard data elements. Standard data elements are individual pieces of data where the meaning and the format of the data have been formally defined and adopted by the State. The standardization of data elements will allow DIT to improve the integration and exchange of data between information systems.

Standardized data will ensure a common understanding by those who use the data. Standardized data increases the value of the data to users by improving the reliability, consistency, and completeness of the data. In addition, consistent use of standard data elements may help reduce the cost of application development by allowing for the reuse or linking of data elements and by decreasing the costs associated with the conversion and transformation of interfaced data.

COBIT suggests that data management standards include a data model, data dictionary and data syntax rules, a data classification scheme, and data security levels. To be the most effective, data management standards should be developed and implemented as new systems are being developed or during major upgrades of existing systems. In addition, to avoid duplication of efforts, DIT should consider using existing national data standards, wherever possible.

RECOMMENDATION

We recommend that DIT establish data management standards.

AGENCY PRELIMINARY RESPONSE

DIT agrees with the finding. DIT informed us that one of the goals in its 2006 strategic plan is to develop an information management strategy that includes identifying data within the State that may be leveraged and shared across agencies. The outcome of DIT's efforts regarding this strategy will include data management standards that will ease the exchanges of data between applications. DIT expects data management standards to be defined and developed in fiscal year 2005-06 and to be implemented in fiscal year 2006-07.

GLOSSARY

Glossary of Acronyms and Terms

Control Objectives for Information and Related Technology framework (COBIT)

In April 1996, the Information Systems Audit and Control Foundation (ISACF) developed an internal control framework to manage, use, and audit information technology. The framework (referred to as COBIT) consists of 34 high-level control objectives associated with primary information technology processes, grouped into four domains. The four domains are planning and organization, acquisition and implementation, delivery and support, and monitoring.

The basic philosophy of COBIT is to center the need for internal controls over information technology processes according to a natural grouping of common information technology processes. COBIT is based on the concept that management must first achieve a complete understanding of the department's business processes before it can effectively develop, manage, and audit the processes for implementing information and related technology solutions. COBIT is based on the underlying assumption that a department's core business processes drive the need for implementing information and related technology. Control objectives define the criteria that must be met to ensure delivery of technology solutions that meet the department's business requirements.

database

A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer.

data warehouse

A very large database designed for fast processing of queries, projections, and data summaries, normally used by a large organization. In this report, "Data Warehouse" refers to the State's Teradata data warehouse.

DBA
database administrator.

DCH
Department of Community Health.

DIT
Department of Information Technology.

effectiveness
Program success in achieving mission and goals.

hash total
A number generated from a series of characters of text. The hash total is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hash totals play a role in security systems where they are used to ensure that transmitted data has not been tampered with.

internal control
The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.

intrusion detection system (IDS)
Software installed on a system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise the system.

IT
information technology.

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.

metadata

Information about data within the data warehouse. This includes descriptions of the sources for the data; the description of each field; the procedures required to move the data from operational systems to the warehouse; and other operational information, such as the history of the migrated data, what organizational unit is responsible for a given field, what happens to the data during migration, what data has been purged, what data is due to be purged, and who is using the data and how they are using it.

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.

operating system

The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.

performance audit

An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.

privileged account

A system account that provides extensive access capabilities. This account is considered high risk and must be controlled and monitored by management.

relational database management system

A database management system with the ability to access data organized in tabular files that may be related by a common item. A relational database management system has the capability to recombine the data files from different files, providing powerful tools for data usage.

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.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL