MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

DATA PRIVACY

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

June 2010

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

084-0570-08

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

Data Privacy

Department of Technology, Management & Budget

Report Number:
084-0570-08

Released:
June 2010

State agencies collect personal information, such as name, social security number, and medical condition, on residents, State employees, and other individuals in the course of providing governmental services. Data privacy relates to how the State collects, stores, uses, disseminates, and disposes of citizens' personal information. The Department of Technology, Management & Budget's (DTMB's) Privacy Project was established to define and create appropriate protection for the personal information collected or maintained by the State of Michigan.

Audit Objective:
To assess the effectiveness of DTMB's efforts to implement a Statewide data privacy program to protect the privacy of personal information.

Audit Conclusion:
DTMB's efforts to implement a Statewide data privacy program to protect the privacy of personal information were moderately effective. We noted one reportable condition (Finding 1).

Reportable Condition:
DTMB should work with the chief privacy officer (CPO) and the Information Privacy Protection Council to implement the State's privacy framework (Finding 1).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DTMB's efforts to incorporate generally accepted privacy principles into the State's privacy framework.

Audit Conclusion:
DTMB's efforts to incorporate generally accepted privacy principles into the State's privacy framework were moderately effective. We noted one reportable condition (Finding 2).

Reportable Condition:
DTMB should work with the CPO and the Information Privacy Protection Council to ensure that the State's privacy framework fully incorporates generally accepted privacy principles (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To analyze and provide data regarding State agencies' practices to protect the privacy of personal information.

Audit Conclusion:
We analyzed and provided data regarding State agencies' practices to protect the privacy of personal information. Our report includes 7 observations and 1 exhibit

(Exhibit 1), presented as supplemental information, related to this audit objective. The purpose of the observations and supplemental information was not to express a conclusion; therefore, we do not.

Observations:

We provided commentary that highlights certain details or events that may be of interest to users of the report. Based on our analysis of State agencies' responses to our privacy questionnaire, we developed observations related to responsibility and accountability for data privacy, collection of personal information, privacy practices, data sharing and safeguards, policies and procedures, agencies' opinions, and privacy risk assessment (Observations 1 through 7).

Supplemental Information:

We provided information related to personal information categories by department (Exhibit 1). We also provided information related to Privacy Project goals and objectives for the Michigan executive branch, proposed initiatives for the Privacy Project, generally accepted privacy principles, principles of fair information practices, and personal information categories (Exhibits 2 through 6).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 2 findings and 2 corresponding recommendations. DTMB's preliminary response indicates that it agrees with both of the recommendations and has 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

June 15, 2010

Mr. Kenneth D. Theis, Director
Department of Technology, Management & Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Theis:

This is our report on the performance audit of Data Privacy, Department of Technology, Management & Budget.

This report contains our report summary; description of agency; audit objectives, scope, and methodology and agency responses and prior audit follow-up; comments, findings, recommendations, and agency preliminary responses; observations; various 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.

AUDITOR GENERAL

This Page Left Intentionally Blank

TABLE OF CONTENTS

DATA PRIVACY

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET

SUPPLEMENTAL INFORMATION

GLOSSARY

Description of Agency

Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of the Michigan Department of Information Technology (MDIT) to DTMB by a Type III transfer and abolished MDIT.

State agencies collect personal information* on residents, State employees, and other individuals in the course of providing governmental services. For example, individuals applying for medical assistance, filing tax returns, seeking a driver's license, or applying for State employment are required to provide personal information to the State in order to obtain services, benefits, or employment. Personal information collected includes name, social security number, date of birth, address, medical conditions, driver's license number, credit card number, bank account numbers, and birth records. We surveyed 18 State departments, and 172 respondents within those departments reported that they have collected over 600 instances* of personal information classified into 11 categories (see Exhibit 1).

In its October 2006 research brief entitled *Keeping Citizen Trust: What Can A State CIO Do To Protect Privacy?,* the National Association of State Chief Information Officers (NASCIO) reported that privacy* was a defining issue of the day. The research brief defined privacy as:

> . . . the decisions that are made about when and how states should collect, store, use, disseminate and dispose of citizens' personal information and how policies based upon those decisions should be implemented.

The brief went on to state that:

> It is more important than ever to ensure that citizens' personal information, held by state government, is kept private.

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

In January 2007, MDIT's Office of Enterprise Security (OES) published its strategic plan for 2007 through 2010. The plan stated:

> The State of Michigan has a broad responsibility for the social and legal environment in which private and sensitive information exists.

The strategic plan described, among other security-related efforts, MDIT's Privacy Project for establishing a privacy program* across State government. The purpose of the Privacy Project was to define and create appropriate protection for the personal information collected or maintained by the State of Michigan. The Privacy Project defined 10 goals and objectives related to developing a formal privacy approach for Michigan's executive branch and 7 initiatives for achieving those goals and objectives (see Exhibits 2 and 3).

To establish leadership for data privacy within State government, the Governor issued Executive Order No. 2009-18 in April 2009. This executive order states in part:

> . . . state and federal law require state agencies to collect, display, retain, destroy, and dispose of records that contain personal identifying information of the residents of this state. . .
>
> . . . the collection, display, retention, destruction, and disposal of records containing the personal identifying information of the residents of this state exposes this state and its residents to security risks, including, but not limited to, identify theft and other privacy violations. . .

The executive order states that the Governor shall designate a chief privacy officer within the executive branch, called on each department director to designate an information privacy protection officer, and created the Information Privacy Protection Council. Members of the Council include the chief privacy officer, as chairperson; the chief information security officer; and the department information privacy protection

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

officers. The Council was created within MDIT to act in an advisory capacity to the Governor and is required to do all of the following:

1. Review, develop, and recommend policies and procedures to be implemented by State departments and agencies to ensure compliance with State and federal privacy laws and the promotion of effective information security and privacy protection.

2. Develop and recommend strategies to enhance awareness, education, and understanding of information security best practices and on-line measures intended to protect the personal identifiable information* of the residents of this State.

3. Identify information security and privacy protection risks within State government and develop and recommend risk mitigation strategies, methods, and procedures to be adopted by State departments and agencies to lessen these risks.

4. Monitor and report compliance by State departments and agencies with State information security and privacy protection policies and procedures.

5. Recommend and coordinate a training program for State employees designed to educate, promote, and advance knowledge of information security and privacy protection policies and procedures.

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

Audit Objectives

Our performance audit* of Data Privacy, Department of Technology, Management & Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to implement a Statewide data privacy program to protect the privacy of personal information.

2. To assess the effectiveness of DTMB's efforts to incorporate generally accepted privacy principles into the State's privacy framework.

3. To analyze and provide data regarding State agencies' practices to protect the privacy of personal information.

Audit Scope

Our audit scope was to examine the program and other records related to the Department of Technology, Management and Budget's data privacy efforts. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit procedures, conducted from April through September 2008 and from May through July 2009, generally covered the period January 2007 through July 2009.

Based on our analysis of State agencies' responses to our privacy questionnaire, we provided commentary that highlights certain details or events that may be of interest to users of the report. This commentary is presented as Observations 1 through 7. The purpose of the observations* was not to express a conclusion; therefore, we do not.

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

As part of our audit, we prepared supplemental information that relates to our audit objectives (Exhibits 1 through 6). Our audit was not directed toward expressing a conclusion on this information and, accordingly, we express no conclusion on it.

Audit Methodology

We reviewed DTMB's Office of Enterprise Security Strategic Plan for 2007 through 2010 and the *Michigan IT Strategic Plan* for 2008 through 2012. We reviewed DTMB's Privacy Project, including the goals and objectives for establishing a privacy framework and the seven initiatives required to implement the framework.

We reviewed numerous State and federal laws regarding the privacy of personal information. We reviewed best practices for data privacy, including the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) *Generally Accepted Privacy Principles - A Global Privacy Framework.*

We conducted a preliminary review of the data privacy practices of State agencies. We surveyed State agencies to obtain an understanding of responsibility for privacy, the types of records collected and maintained that contained personal information, entities that State agencies shared personal information with, privacy practices, and issues facing management.

To accomplish our first objective, we reviewed Executive Order No. 2009-18. We interviewed DTMB staff and reviewed Privacy Project documentation to assess the status of Privacy Project initiatives.

To accomplish our second objective, we examined DTMB's privacy framework and compared it to the AICPA and CICA *Generally Accepted Privacy Principles - A Global Privacy Framework*, published in May 2006, to assess the extent to which generally accepted privacy principles criteria were included in DTMB's privacy framework (see Exhibit 4).

To accomplish our third objective, we compiled the responses from the data privacy questionnaire and analyzed the results to create various charts, graphs, and listings for presentation in our report. We sent the questionnaire to 18 executive branch departments. If a department had established departmentwide data privacy policies,

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

procedures, and/or practices, we asked the department to respond for the entire department on a single questionnaire. However, if a department did not have departmentwide data privacy policies, procedures, or practices, we asked the department to complete a questionnaire for each organizational unit within the department. Most departments chose to complete multiple questionnaires. We received 172 responses to our questionnaire:

Department	Number of Responses
Michigan Department of Agriculture	1
Department of Attorney General	1
Department of Civil Rights	1
Department of Community Health	58
Department of Corrections	1
Michigan Department of Education	3
Department of Energy, Labor & Economic Growth	37
Department of Environmental Quality*	2
Department of History, Arts and Libraries*	2
Department of Human Services	20
Michigan Department of Information Technology*	1
Department of Management and Budget*	17
Department of Military and Veterans Affairs	6
Department of Natural Resources*	7
Department of State	1
Michigan Department of State Police	5
Michigan Department of Transportation	1
Department of Treasury	8
Total	172

We also made observations based on our analysis of the data.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement

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

as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

Agency Responses and Prior Audit Follow-Up

Our audit report contains 2 findings and 2 corresponding recommendations. DTMB's preliminary response indicates that it agrees with both of the recommendations and has 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 the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DTMB to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

We released our prior performance audit of the Teradata Data Warehouse, Michigan Department of Information Technology (MDIT) (50-520-04), in November 2005. Within the scope of this audit, we followed up 1 of the 8 prior audit recommendations. MDIT partially complied with the prior audit recommendation.

Background

The Department of Technology, Management & Budget's (DTMB's) privacy initiatives are intended to protect Michigan citizens' and State employees' personal information collected, maintained, and shared by State agencies.

The Michigan Department of Information Technology (MDIT) established the Privacy Project in the Office of Enterprise Security (OES) Strategic Plan for 2007 through 2010 to define and create appropriate protection for personal information collected or maintained by the State of Michigan. The Privacy Project included seven initiatives that MDIT developed to facilitate the implementation of generally accepted privacy principles (see Exhibit 3).

The following table shows the time line established for each initiative in the OES Strategic Plan for 2007 through 2010:

Privacy Project Initiatives
Summary of Expected Completion Dates by Fiscal Year

Initiative	Initial Expectation as of January 2007	Revised Expectation as of May 2008	Status as of July 31, 2009
Information privacy protection officer Installation	2006-07	2007-08	Substantially complete
State of Michigan privacy office creation	2006-07	2007-08	Not completed
Guideline development and dissemination	2006-07	2007-08	Not completed
Privacy office policy and procedure development	2006-07	No time line given	Not completed
Data identification and documentation	2007-08	2008-09	Not completed
Privacy policy compliance process	2007-08	2008-09	Not completed
Privacy data electronic management	Ongoing (Starting fiscal year 2008-09)	Ongoing (Starting fiscal year 2009-10)	Not completed

Prior to the appointment of the chief privacy officer (CPO), DTMB informed us that the CPO's leadership was needed for the initiatives of the Privacy Project to move forward. DTMB also informed us that revised completion dates for the initiatives would be determined by the CPO.

MDIT recommended in its 2003 *Secure Michigan Initiative**, and again in its 2007 Privacy Project, that each agency designate an individual to be the information privacy protection officer, who would be accountable for ensuring the security and privacy of agency information. By February 2008, only a few departments had designated information privacy protection officers.

In April 2009, Executive Order No. 2009-18 addressed the first initiative of the Privacy Project by establishing the CPO function to be designated by the Governor and requiring each department director to designate an information privacy protection officer for his/her department. As shown in the following table, by July 2009, 12 of 18 departments responded to our questionnaire that they had designated information privacy protection officers in response to the executive order:

Department	Information Privacy Protection Officer
Michigan Department of Agriculture	Yes
Department of Attorney General	Yes
Department of Civil Rights	Yes
Department of Community Health	Yes
Department of Corrections	No Response
Michigan Department of Education	Yes
Department of Energy, Labor & Economic Growth	Yes
Department of Environmental Quality*	No Response
Department of History, Arts and Libraries*	No
Department of Human Services	No Response
Michigan Department of Information Technology*	Yes
Department of Management and Budget*	Yes
Department of Military and Veterans Affairs	No
Department of Natural Resources*	Yes
Department of State	Yes
Michigan Department of State Police	Yes
Michigan Department of Transportation	Yes
Department of Treasury	No Response

In April 2009, MDIT informed the departments that more specific direction for selecting their information privacy protection officer would be provided after the CPO was designated by the Governor.

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

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO IMPLEMENT A STATEWIDE DATA PRIVACY PROGRAM

Audit Objective: To assess the effectiveness of the Department of Technology, Management & Budget's (DTMB's) efforts to implement a Statewide data privacy program to protect the privacy of personal information.

Audit Conclusion: DTMB's efforts to implement a Statewide data privacy program to protect the privacy of personal information were moderately effective. Our assessment disclosed one reportable condition* related to implementation of the State's privacy framework (Finding 1).

DTMB informed us that leadership from a chief privacy officer (CPO) is needed before the initiatives of the Privacy Project can move forward. In August 2009, the Governor designated the legal counsel to the Governor as the CPO.

FINDING

1. Implementation of the State's Privacy Framework

   DTMB should work with the CPO and the Information Privacy Protection Council to implement the State's privacy framework. Without implementation of the State's privacy framework, agencies will not have the requirements or guidance to protect the privacy of citizens and individuals conducting business with the State.

   DTMB's proposed privacy framework was not published as a Statewide policy in the DTMB Administrative Guide. Consequently, Michigan residents must rely on a patchwork of State and federal sector-specific laws, such as financial, medical, education, and criminal, to protect the privacy of personal information collected and maintained by State agencies.

   Although Executive Order No. 2009-18 primarily focuses on compliance with existing State and federal privacy laws and regulations, it did not address the implementation of DTMB's proposed privacy framework.

   The State of Michigan does not have an all-encompassing privacy statute that embodies generally accepted privacy principles or individual State privacy laws that sufficiently address generally accepted privacy principles. The State laws focus primarily on the privacy principle of disclosure and not on the generally accepted

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

privacy principles of management, notice, choice and consent, and monitoring and enforcement.

For federal government agencies, the Privacy Act of 1974, Public Law 93-579, Title 5, section 552a of the *United States Code (USC)*, was created in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy through the creation of four procedural and substantive rights in personal data. First, it requires federal government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called fair information practices, when gathering and handling personal data (see Exhibit 5). Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth, it allows individuals to sue the federal government for violating its provisions.

Although the executive order specifically identifies two key federal laws, the Privacy Act of 1974 and the Right to Financial Privacy Act of 1978, Public Law 95-630, 12 *USC* 3401, these laws do not apply to State governmental agencies.

DTMB stated in its Privacy Project that, in order to implement a privacy framework, it is imperative that a Statewide policy be created and published in the DTMB Administrative Guide to establish agency responsibility for personal information. A Statewide policy would establish agency accountability and build a sustainable privacy program.

RECOMMENDATION

We recommend that DTMB work with the CPO and the Information Privacy Protection Council to implement the State's privacy framework.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has already taken steps toward compliance. Executive Order No. 2009-18 established the Council and created the position of CPO for the State of Michigan. One objective of the Council is to recommend Statewide policy and procedure to help ensure compliance with State and federal privacy laws and the promotion of effective information security and privacy protection. As a member of the Council, DTMB stated that it will continue to work with the State's CPO and other department information privacy protection officers

to implement a comprehensive privacy framework, based on generally accepted privacy principles.

EFFECTIVENESS OF EFFORTS TO INCORPORATE GENERALLY ACCEPTED PRIVACY PRINCIPLES INTO THE STATE'S PRIVACY FRAMEWORK

COMMENT

Background: In May 2006, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) published *Generally Accepted Privacy Principles - A Global Privacy Framework.* Generally accepted privacy principles are essential to the proper protection and management of personal information. They are based on internationally known principles of fair information practices included in many privacy laws and regulations of various jurisdictions around the world and are recognized as good privacy practices. There are 10 generally accepted privacy principles (see Exhibit 4), each supported by objective and measurable criteria for creating an effective privacy program.

Audit Objective: To assess the effectiveness of DTMB's efforts to incorporate generally accepted privacy principles into the State's privacy framework.

Audit Conclusion: DTMB's efforts to incorporate generally accepted privacy principles into the State's privacy framework were moderately effective. Our assessment disclosed one reportable condition related to DTMB's privacy framework (Finding 2).

FINDING

2. Privacy Framework

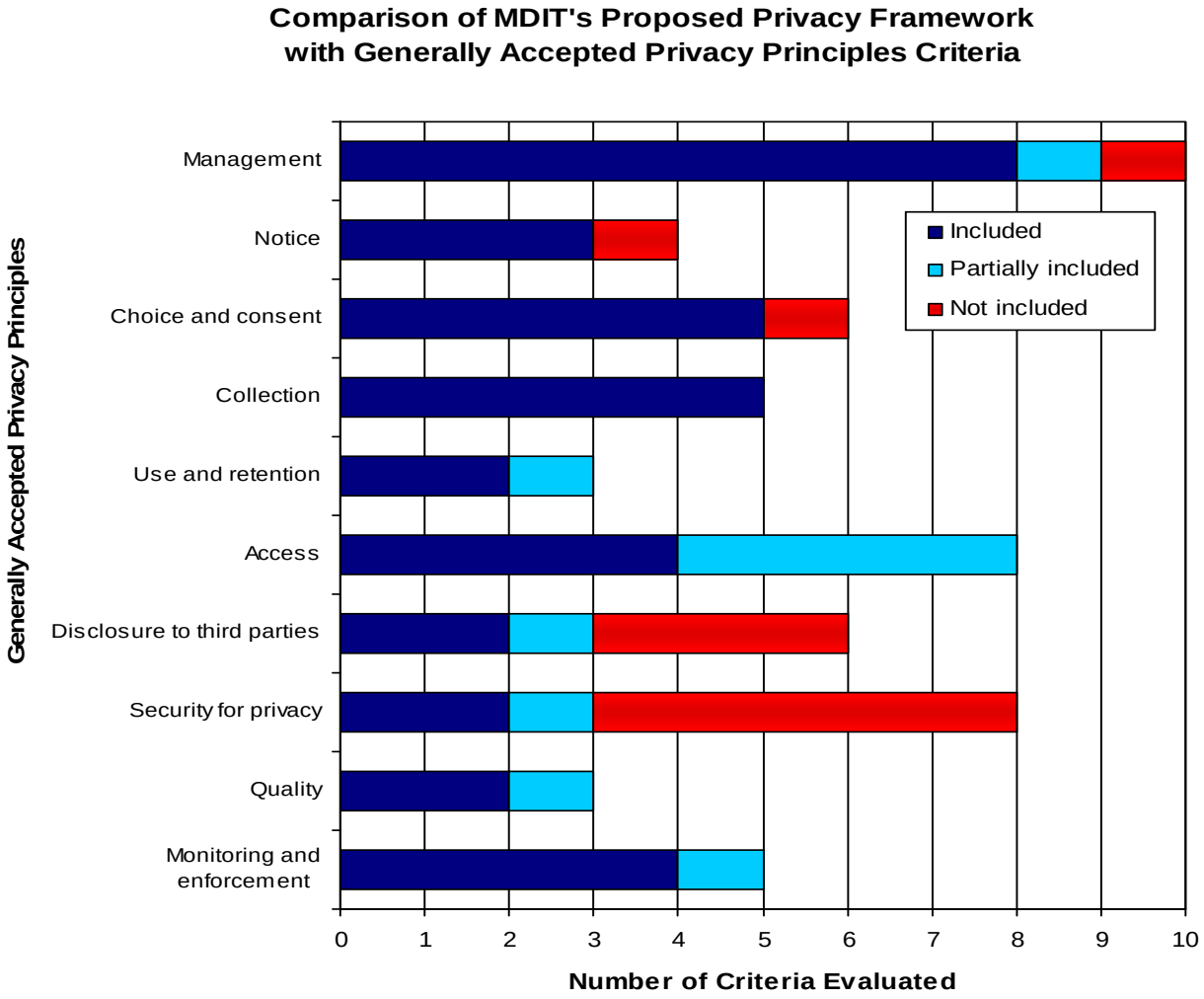
DTMB should work with the CPO and the Information Privacy Protection Council to ensure that the State's privacy framework fully incorporates generally accepted privacy principles. The omission of critical criteria from DTMB's proposed privacy framework could hinder State agencies' efforts to establish effective protection of personal information.

In our performance audit of the Teradata Data Warehouse, released in November 2005, we recommended that the Michigan Department of Information Technology (MDIT) establish a Statewide privacy framework to govern the use of confidential

and sensitive data maintained in information systems. In its response, MDIT agreed to establish a framework for developing Statewide privacy policies and standards for the collection, use, and sharing of data by October 1, 2006.

We compared DTMB's proposed privacy framework with the 10 generally accepted privacy principles and the 58 objective and measurable criteria associated with the generally accepted privacy principles.

Our review indicated that DTMB's proposed privacy framework included 37 of the 58 criteria and partially included 10 of the 58 criteria, representing 47 (81%) of the 58 total criteria. However, the proposed framework did not include 11 (19%) of the 58 generally accepted privacy principles criteria. Each of the 10 generally accepted privacy principles had between 3 and 10 objective and measurable criteria. The chart that follows summarizes our analysis:



Several of the criteria omitted from DTMB's proposed privacy framework include: providing human capital and financial resources to support a privacy program (management principle), obtaining the consent of an individual prior to using his or her personal information for a new purpose (choice and consent principle), and disclosing personal information only to third parties that have privacy protections consistent with the State's privacy practices (disclosure to third parties principle). Although DTMB did not include 5 security-related criteria in its proposed privacy framework, it has established enterprise-wide policy to address most of these security-related criteria.

Fully incorporating all generally accepted privacy principles criteria into DTMB's proposed privacy framework will provide a solid foundation from which State agencies can create their privacy programs and demonstrate their intention to protect the privacy of citizen and employee personal information. By involving the CPO and the Council in this effort, DTMB will help State agencies take ownership of the privacy framework.

RECOMMENDATION

We recommend that DTMB work with the CPO and the Information Privacy Protection Council to ensure that the State's privacy framework fully incorporates generally accepted privacy principles.

AGENCY PRELIMINARY RESPONSE

DTMB agrees and informed us that it has complied. DTMB agrees that generally accepted privacy principles should be fully incorporated into the State's data privacy framework and, as a member of the Council, participated in the recent adoption of Statewide privacy principles based on the AICPA and CICA published *Generally Accepted Privacy Principles - A Global Privacy Framework*. DTMB also informed us that State agencies will next develop and implement procedures that address these privacy principles consistent with the agencies' mission, business practices, and organization.

ANALYSIS OF
STATE AGENCIES' PRIVACY PRACTICES

COMMENT

Background: We developed a questionnaire to request information about the data privacy practices in place throughout executive branch departments.

The questionnaire inquired about the following categories of personal information:

- vital record information
- health information
- tax information
- education information
- personnel information
- driver record information
- bank and financial information
- children's information
- library information
- privileged information
- criminal record information

For each category, we asked what specific types of personal information was collected (such as name, social security number, and bank account number); whether the information was shared; what privacy practices were in place to protect the information; and the respondents' opinions about data privacy within each department.

We used the information obtained from the questionnaires to develop the observations for this objective.

Audit Objective: To analyze and provide data regarding State agencies' practices to protect the privacy of personal information.

Audit Conclusion: We analyzed and provided data regarding State agencies' practices to protect the privacy of personal information. Our summary of responses to the privacy questionnaire is provided in Exhibit 1, presented as supplemental information. In addition, our analysis resulted in observations, which include data from the privacy questionnaires, related to responsibility and accountability

for data privacy, collection of personal information, privacy practices, data sharing and safeguards, policies and procedures, agencies' opinions, and privacy risk assessment (Observations 1 through 7). The purpose of the observations and supplemental information was not to express a conclusion; therefore, we do not.

OBSERVATIONS

OBSERVATION

1. Responsibility and Accountability for Data Privacy

The generally accepted privacy principle of management notes the importance of assigning responsibility and accountability for data privacy to an individual or group within the organization. At the time we surveyed agencies in August 2008, prior to the Governor's April 2009 Executive Order No. 2009-18, only two departments had formally designated information privacy protection officers. To understand the extent to which individuals responding to our questionnaire had been assigned responsibility for data privacy, we asked, "Are you responsible for data privacy in your department?"

We received the following responses:

	Number of Responses	Percentage of Responses
Yes	81	47%
No	87	51%
No response	4	2%
Total	172	100%

The questionnaire responses indicated that just over half, or 87 (51%), of the 172 respondents did not have responsibility for data privacy within the agency or department that they represented.

All departments had designated at least one individual with responsibility for data privacy except the Departments of Corrections, Environmental Quality, Information Technology, Natural Resources, and Transportation.

The first goal of DTMB's Privacy Project requires agencies to assign responsibility to an individual for data privacy (see Exhibit 2). Formal assignment (through the use of a position description) is one of the best ways to ensure that the roles and responsibilities of this position are known and understood. For the 81 (47%) respondents who indicated that they were responsible for data privacy, we also asked, "How are data privacy responsibilities formally assigned within your department?"

The following table summarizes how data privacy responsibilities were assigned:

	Number of Respondents	Percentage of Respondents
Position description	24	30%
Not formally assigned or assigned by other means	52	64%
Not sure how privacy responsibility was assigned	5	6%
Total	81	100%

Only 24 (30%) of the respondents indicated that data privacy responsibilities were formally assigned through position description and 52 (64%) of the respondents reported that their responsibilities were assigned informally (without the use of a position description). The remaining 5 (6%) respondents responsible for data privacy were not sure how their responsibilities were assigned.

Executive Order No. 2009-18 and DTMB's proposed privacy framework recognize the need for agency information privacy protection officers, with the privacy framework calling for agencies to assign privacy responsibility, accountability, and authority to their information privacy protection officers.

OBSERVATION

2. Collection of Personal Information

State agencies responded to our privacy questionnaire that they collected and maintained 664 instances of personal information. See Exhibit 1 for a summary of the number of instances reported along with the number of responses by department.

Of the 11 personal information categories (see Exhibit 6), respondents indicated the number of personal information categories in which they collected, maintained, or disclosed information:

	Number of Personal Information Categories
Department of Community Health	11
Department of Attorney General	10
Department of Energy, Labor & Economic Growth	10
Department of Human Services	10
Department of Management and Budget*	10
Department of Military and Veterans Affairs	10
Department of Natural Resources*	10
Department of Treasury	10
Department of Environmental Quality*	8
Department of History, Arts and Libraries*	8
Michigan Department of State Police	8
Department of Corrections	6
Michigan Department of Education	6
Department of Civil Rights	5
Department of State	5
Michigan Department of Agriculture	3
Michigan Department of Information Technology*	3
Michigan Department of Transportation	1

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

We summarized questionnaire responses by the 11 personal information categories to determine the extent to which data in each category of personal information was collected, maintained, or disclosed:

Personal Information Category	Reported Instances
Health information	95
Personnel information	94
Vital record information	75
Tax information	73
Criminal record information	63
Children's information	62
Education information	60
Bank and financial information	55
Driver record information	51
Privileged information	33
Library information	3
Total	664

We summarized the frequency at which certain data was collected by departments in the following table:

Data Collected by Departments	Reported Instances
Date of birth	512
Social security number	489
Signature	356
Driver's license number	154
Bank account number	45
Credit card number	25

Our analysis of questionnaire responses shows that most departments collect, maintain, and disclose many different categories of personal information. The extensive amount of personal information collected by State agencies supports the need for implementing DTMB's Privacy Project and proposed privacy framework.

OBSERVATION

3. Privacy Practices

Privacy practices are essential to the protection and management of personal information. For each information category, we requested that respondents "Please indicate the extent to which the following privacy practices are in place within your department." Of the 664 reported instances of personal information, we summarized the security-related practices and responses as follows:

Security-Related Practices	Always		Sometimes		Never		No Response	
Limits access based on business need.	471	71%	95	14%	18	3%	80	12%
Limits electronic access to the data.	457	69%	84	13%	18	3%	105	16%
Limits physical access to the data.	474	71%	96	14%	9	1%	85	13%
Trains staff on proper handling of the data.	445	67%	118	18%	8	1%	93	14%
Monitors disposal of the data in electronic files.	281	42%	122	18%	90	14%	171	26%
Monitors disposal of the data in paper documents.	376	57%	128	19%	35	5%	125	19%

Regarding the six security-related privacy practices, between 42% and 71%, or an average of 63%, of our questionnaire respondents said that privacy practices were always in place at their department and only 1% to 14%, or an average of 5%, of respondents said privacy practices were never in place. Of the 664 reported instances of personal information, we summarized the nonsecurity-related practices and responses as follows:

Nonsecurity-Related Practices	Always		Sometimes		Never		No Response	
Allows individuals to review their data.	284	43%	136	20%	91	14%	153	23%
Classifies data (private, confidential, public)	287	43%	107	16%	113	17%	157	24%
Corrects data upon individuals' request.	304	46%	134	20%	77	12%	149	22%
Inventories data.	240	36%	106	16%	143	22%	175	26%
Limits data collection to necessary data.	447	67%	97	15%	22	3%	98	15%
Notifies individuals if their data is disclosed.	178	27%	140	21%	172	26%	174	26%

Regarding the six nonsecurity-related privacy practices, between 27% and 67%, or an average of 44%, of our questionnaire respondents said that privacy practices were always in place at their department and only 3% to 26%, or an average of

16%, of respondents said privacy practices were never in place. Several factors may have contributed to the higher rate of security-related controls being in place throughout the State. These include DTMB's implementation of policies and procedures in the DTMB Administrative Guide and our recent information technology audit recommendations for the improvement of data security practices.

Although the nonsecurity-related privacy practices were less likely to be in place than the security-related privacy practices, DTMB Administrative Guide policy 1340 Information Technology Information Security, issued in April 2007, requires agencies to identify (inventory) and classify agency information based on sensitivity, criticality, and risk. As illustrated by the preceding table, 36% of the respondents indicated that data inventories were "always" performed and the practice of classifying data was "always" performed 43% of the time. The lower level of compliance with this Statewide policy may, in part, be due to the lack of agency policies and procedures that implement DTMB Administrative Guide policy 1340. Based on the results of our questionnaire, 23% and 34% of respondents indicated that written policies and procedures were in place for inventory of data and classification of data, respectively (see Observation 5).

Overall, the pattern of security-related practices occurring at a higher rate than nonsecurity-related privacy practices was relatively consistent for each personal information category included in the questionnaire. The two categories that fell slightly outside this pattern were library information and criminal record information. There were only three responses for library information so it was difficult to determine whether they followed the same trends as other categories. Criminal record information followed the same general patterns as other personal information categories in which security-related practices were in place more often than nonsecurity-related privacy practices; however, there was a much higher rate of nonresponses than in the other personal information categories.

Regardless of the type of data being evaluated, generally accepted privacy principles require that both security-related and nonsecurity-related privacy practices be in place as part of an effective data privacy program.

OBSERVATION

4. Data Sharing and Safeguards

We asked each questionnaire respondent, "With whom does your department share personal information?" The following table summarizes with whom State departments are sharing the personal information that they collect:

Entity	Percentage of Shared Instances
Other State of Michigan departments or agencies	60%
Federal government agencies	36%
Contracted service providers	36%
Local governments	27%
Individuals when FOIA requests were submitted	24%
Other state and local governments	23%
Private businesses	11%
Researchers	11%
Individuals when a FOIA request was not submitted	5%
Other entities	1%
Not sure if the record was shared	18%

Of the 664 instances of records containing personal information, respondents indicated that 551 (83%) instances were shared with one or more other entities. Library information and personnel information were the personal information categories that were shared the least (33% and 60%, respectively). The remaining nine personal information categories shared between 78% and 100% of the

personal information with other entities. We summarized the personal information categories and the number of instances shared as follows:

	Number of Instances			Percentage
	Shared	Not Shared	Total	Shared
Privileged information	33	0	33	100%
Health information	85	10	95	90%
Vital record information	66	9	75	88%
Tax information	64	9	73	88%
Driver record information	45	6	51	88%
Bank and financial information	48	7	55	87%
Children's information	53	9	62	86%
Education information	51	9	60	85%
Criminal record information	49	14	63	78%
Personnel information	56	38	94	60%
Library information	1	2	3	33%
Total	551	113	664	
Percentage of Total	83%	17%		

We also asked respondents which safeguards were in place to protect shared personal information. We obtained the following responses:

Safeguards	Number of Shared Instances	Percentage of Total Instances Shared
Requires signed confidentiality agreements.	245	44%
Monitors third party access to the State's data.	211	38%
Has policies and procedures for data sharing.	407	74%
Has no safeguards in place to protect shared data.	9	2%
Is not sure what safeguards are in place.	11	2%
Other.	142	26%

Respondents indicated that 407 (74%) of the 551 instances of personnel information shared were covered by data sharing policies and procedures. Although we did not review agency policies, we did review several State laws regarding data sharing. These laws focused on disclosure of data, with whom the

data could be shared, and under what circumstances the data could be shared. The laws we reviewed did not specify the safeguards that should be in place when data is shared with other entities.

Agencies may protect personal information with safeguards in addition to policies and procedures. Safeguards such as signed confidentiality agreements could be used to ensure that the third party protected the personal data it received according to agency requirements. Agencies may also monitor third party access to ensure that data was used in accordance with signed agreements. We summarized the responses to determine the extent to which respondents supplemented their policies and procedures with confidentiality agreements and monitoring to protect personal data shared with third parties:

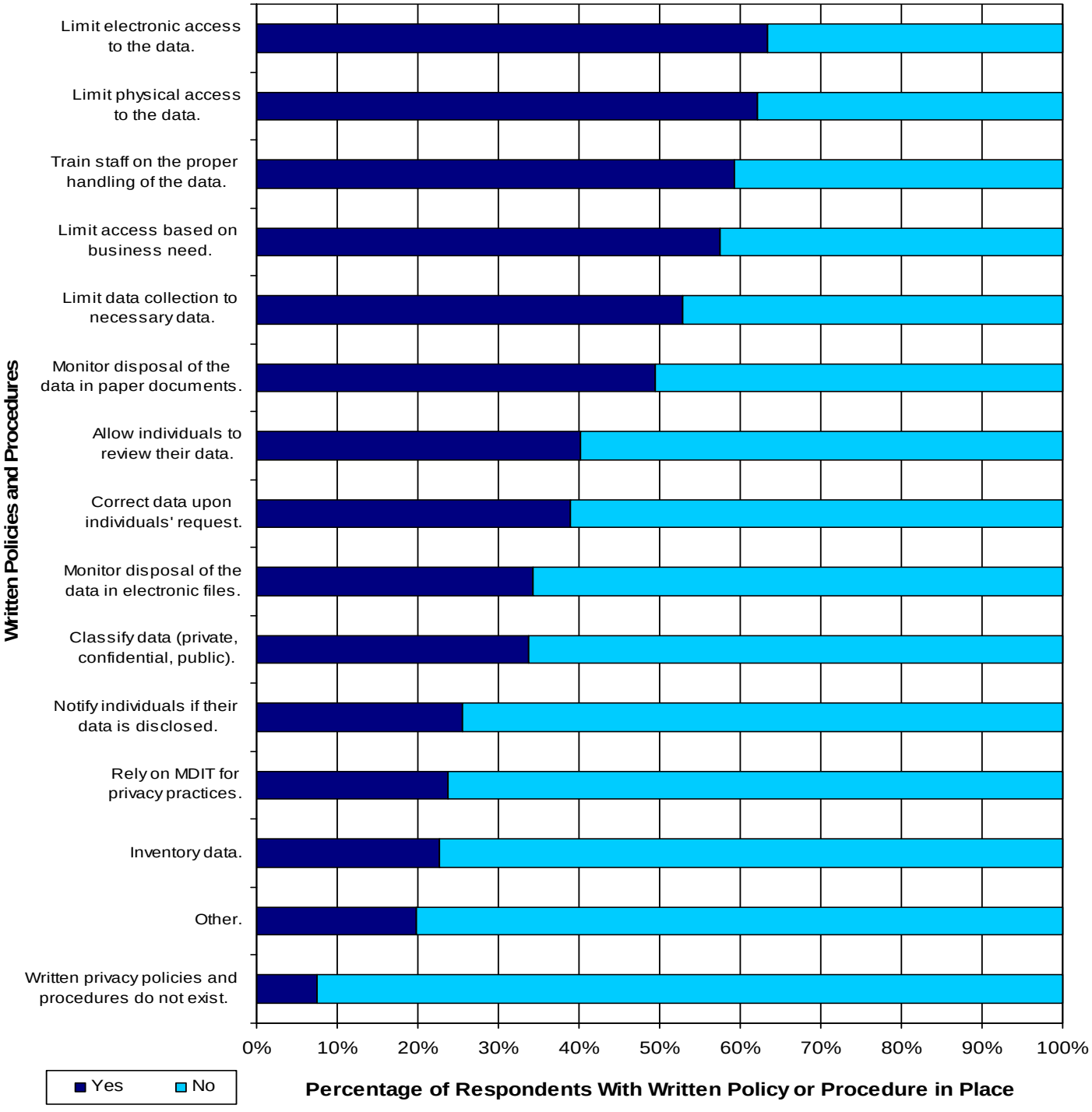
	Number of Shared Instances	Percentage of Shared Instances
Requires signed confidentiality agreements.	76	14%
Monitors third party access to State's data.	47	9%
Requires signed confidentiality agreements and monitors third party access to State's data.	139	25%
Total	262	48%

This summary shows that 48% of the 551 instances of personal information shared with third parties was protected by policies, procedures, and some other specific safeguard. Agencies having policies and procedures along with signed confidentiality agreements and monitoring practices are better positioned to protect the privacy of individuals as soon as their personal information is passed on to third parties.

OBSERVATION

5. Policies and Procedures

We asked each questionnaire respondent to "Please indicate the privacy practices that have been established in written policy or procedure within your department." The responses were as follows:



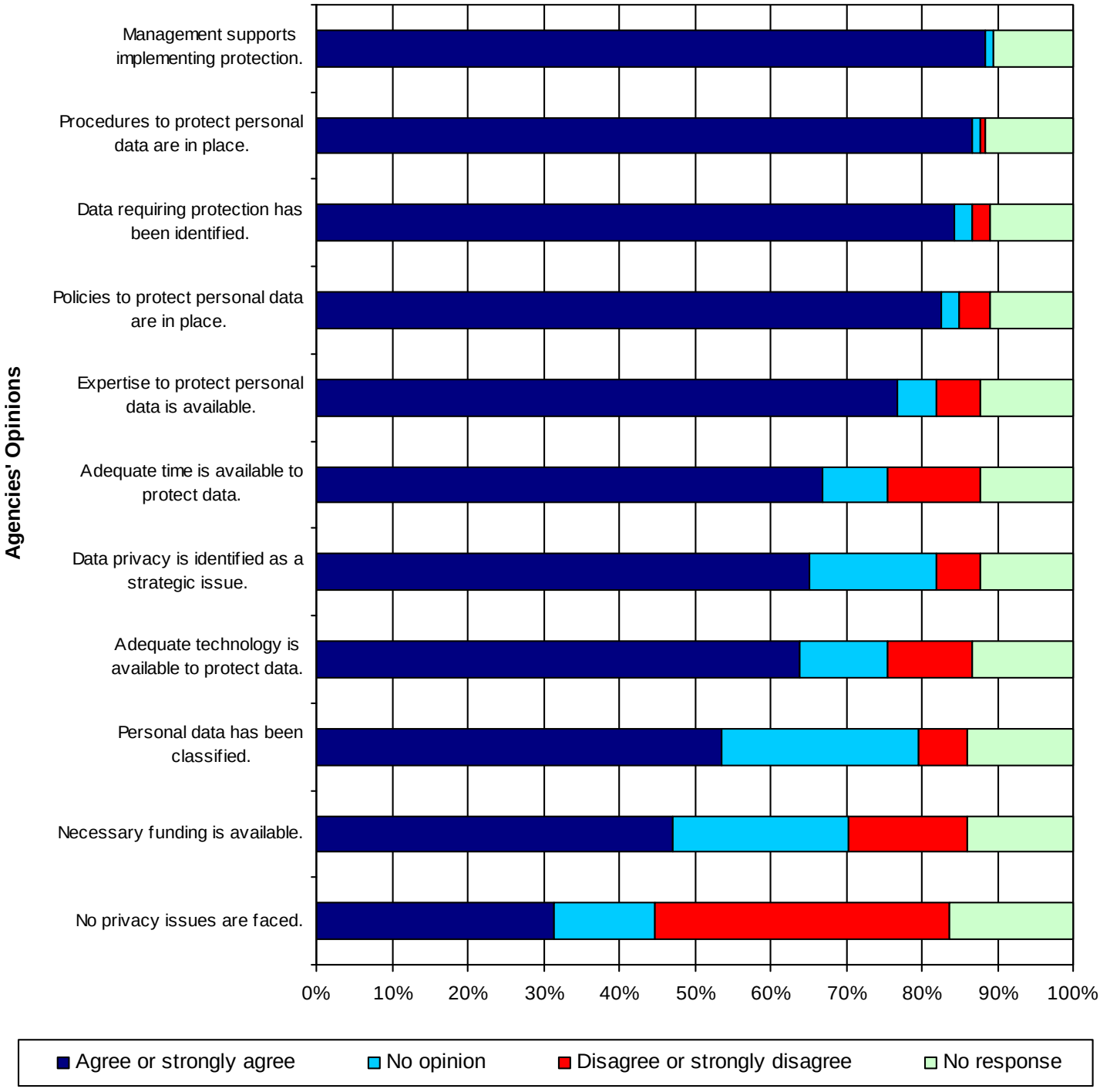
Questionnaire responses indicate that written policies and procedures are in place more frequently to address the security principle; for example, 63% limit electronic access to the data, 62% limit physical access to the data, 59% train staff on the proper handling of data, and 58% limit access based on business need. This is consistent with Observation 3, which noted that security-related practices were more likely to have been implemented than nonsecurity-related privacy practices such as notification of disclosure.

DTMB Administrative Guide policy 1340, Information Technology Information Security, states that information is not limited only to electronic documents and is to be inventoried and classified by the agency based on sensitivity, criticality, and risk. Despite DTMB's guidance, agencies' written policies and procedures to inventory data and classify information were limited. Only 23% of the agencies responded that they had written policies and procedures in place to inventory the information they collected and maintained, and only 34% had written policies and procedures in place to classify the information they collected and maintained.

OBSERVATION

6. Agencies' Opinions

We requested that respondents "Please specify the extent to which you agree with each of the following statements related to privacy practices within your department." The responses we received are shown below:



We noted that 88% of the respondents agree or strongly agree with the statement that management supports implementing protection for data privacy, 83% agree or strongly agree that policies to protect personal data were in place, and 87% agree or strongly agree that procedures to protect personal data were in place. However, based on the information in Observations 3 and 5, it does not appear that privacy practices, policies, or procedures are in place throughout the State to protect personal information.

Questionnaire responses indicated that 84% agree or strongly agree with the statement that data requiring protection had been identified. However, in actual practice, this may not necessarily be the case. Observation 3 shows that 52% of respondents indicated that they "always" (36%) or "sometimes" (16%) inventoried personal information. To a lesser extent, Observation 5 shows that only 23% of respondents indicated that they had written policies and procedures that required their department to inventory data.

Questionnaire responses indicated that 54% agree or strongly agree with the statement that personal data has been classified. This is consistent with Observation 3, in which 59% of the respondents indicated that they "always" (43%) or "sometimes" (16%) classified data. However, questionnaire responses shown in Observation 5 indicate that only 34% had written policies and procedures for classifying data. Classifying data consists of determining whether the data is private, confidential, or public. In order to know if all the data that needed protection had been identified, the data would also need to be classified.

Only 47% of respondents agree or strongly agree with the statement that the necessary funding is available to implement data privacy practices. Given the budget constraints that the State has faced in the last few years, this is understandable. No specific appropriations have been made to implement generally accepted privacy principles outlined in DTMB's Privacy Project.

We noted that 31% of the respondents agree or strongly agree that no privacy issues were faced. We also noted that 13% of the respondents had no opinion on this statement, 39% disagree or strongly disagree, and 16% did not provide a response. Having a higher percentage of respondents disagree with this statement than agree with it suggests that there is some level of awareness that there are privacy related issues that need to be addressed.

OBSERVATION

7. Privacy Risk Assessment

Because of the vast amount of personal information collected by the State, the risk to personal privacy is a concern that should be addressed. We asked each respondent, "Has your department assessed the risks posed by data privacy?"

We obtained the following responses:

	Percentage
Risk assessment to assess the risk posed by data privacy had been performed	58%
No risk assessment had been performed	23%
Did not respond to the question	19%

Of the respondents, 42% asserted that a risk assessment had not been done or they did not respond to the question. These respondents account for 273 (41%) of the 664 total instances of personal information collected and maintained and 227 (41%) of the 551 instances shared throughout the State.

The following table shows the individual responses, by department, to the question:

Department	Yes	No	No Response
Michigan Department of Agriculture	1	0	0
Department of Attorney General	1	0	0
Department of Civil Rights	1	0	0
Department of Community Health	40	8	10
Department of Corrections	0	1	0
Michigan Department of Education	2	1	0
Department of Energy, Labor & Economic Growth	14	14	9
Department of Environmental Quality*	0	2	0
Department of History, Arts and Libraries*	2	0	0
Department of Human Services	9	6	5
Michigan Department of Information Technology*	1	0	0
Department of Management and Budget*	14	1	2
Department of Military and Veterans Affairs	4	0	2
Department of Natural Resources*	4	3	0
Department of State	1	0	0
Michigan Department of State Police	2	1	2
Michigan Department of Transportation	0	1	0
Department of Treasury	4	1	3
Total	100	39	33

All of the respondents from the Departments of Agriculture; Attorney General; Civil Rights; History, Arts and Libraries; Information Technology; and State asserted in their responses that they completed risk assessments related to data privacy. However, respondents from the Departments of Corrections, Environmental Quality, and Transportation asserted that they had not completed a risk assessment. Respondents from the remaining 9 departments had varied responses indicating that risk assessments may have been conducted for some areas of their department but not for others.

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

There are risks associated with collecting personal information. These risks need to be assessed in order to ensure that adequate privacy protection is provided.

The federal government addressed the assessment of privacy risks with the passage of the E-Government Act of 2002. Federal agencies are required to complete privacy impact assessments for new information systems, systems under development, or systems undergoing major modifications. A privacy impact assessment is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collection; to maintain and disseminate information in an identifiable form in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

State agencies operate without comparable privacy requirements or guidance. Adopting practices similar to the federal government's privacy impact assessment would assist State agencies' efforts to assess data privacy risks in a consistent manner and ensure the protection of an individual's personal information.

SUPPLEMENTAL INFORMATION

DATA PRIVACY

Department of Technology, Management & Budget

Personal Information Categories by Department

Department	Vital Record	Health	Tax	Education	Personnel	Driver Record	Bank and Financial
Michigan Department of Agriculture	0	0	1	0	0	1	0
Department of Attorney General	1	1	1	1	1	1	1
Department of Civil Rights	1	1	0	1	0	1	0
Department of Community Health	21	45	12	12	23	5	6
Department of Corrections	1	1	1	1	0	0	0
Michigan Department of Education	2	0	1	2	3	0	0
Department of Energy, Labor & Economic Growth	12	11	20	14	18	8	12
Department of Environmental Quality	2	1	2	1	2	2	2
Department of History, Arts and Libraries	1	1	2	1	0	0	2
Department of Human Services	11	14	6	10	12	6	5
Michigan Department of Information Technology	0	0	0	0	1	1	0
Department of Management and Budget	8	8	12	7	14	10	9
Department of Military and Veterans Affairs	6	6	5	5	5	3	5
Department of Natural Resources	1	3	2	1	6	3	3
Department of State	0	0	0	1	1	1	1
Michigan Department of State Police	1	1	1	0	3	3	2
Michigan Department of Transportation	0	0	0	0	0	0	1
Department of Treasury	7	2	7	3	5	6	6
Totals	75	95	73	60	94	51	55

Source: Office of the Auditor General analysis of data reported by agencies in privacy questionnaire.

Children's	Library	Privileged	Criminal Record	Total Instances Reported	Number of Different Categories of Data	Total Questionnaires Submitted
0	0	1	0	3	3	1
1	0	1	1	10	10	1
1	0	0	0	5	5	1
20	1	9	14	168	11	58
1	0	0	1	6	6	1
0	0	1	1	10	6	3
8	0	7	11	121	10	37
0	0	2	0	14	8	2
1	1	0	1	10	8	2
12	0	3	9	88	10	20
0	0	0	1	3	3	1
6	0	4	5	83	10	17
4	0	2	4	45	10	6
2	1	0	3	25	10	7
0	0	0	1	5	5	1
2	0	0	4	17	8	5
0	0	0	0	1	1	1
4	0	3	7	50	10	8
62	3	33	63	664		172

Exhibit 2

DATA PRIVACY

Department of Technology, Management & Budget

Privacy Project Goals and Objectives for the Michigan Executive Branch

1. Enhance Agency-Level Accountability. Each agency must be responsible for managing personal information under its control as well as the assignment of responsibilities to its staff.

2. Improve Notice Information. Each agency must identify what personal information is gathered and the purpose for usage of that information. Whenever possible, a notice with this information should be given to the individual.

3. Improve Consent Procedures. If at all possible, consent should be obtained before data collection, storage, and use. Sensitive information should always be gathered with explicit consent of the individual.

4. Minimize Information Collection. Agencies must only gather information necessary for purposes in support of their department.

5. Reduce Information Retained. Information should only be retained as required and must include a set of guidelines for removal. Only the media approved by the agency may be used.

6. Improve Accuracy. Information must be as accurate as possible.

7. Meet or Exceed Privacy Regulations. Appropriate controls must be in place to meet or exceed State and federal privacy regulations or laws.

8. Make Disclosure More Readily Accessible. The privacy policies and procedures should be readily available for public review when required. The policies must be updated when needed and communicated to internal personnel at least annually.

9. Increase Information Access. Upon request, individuals' access to their private information may be allowed. The agency should also provide the individuals the ability to address inaccuracies.

10. Facilitate Challenges. An individual may have the right to challenge an agency's compliance with the principles outlined in these goals. A venue must be in place for these challenges to take place.

Source: Office of Enterprise Security Strategic Plan 2007 through 2010.

Exhibit 3

DATA PRIVACY

Department of Technology, Management & Budget

Proposed Initiatives for the Privacy Project

Below are the specific initiatives that the State is undertaking in order to move the Privacy Project forward:

Initiative 1: Privacy Officer Installation
The Michigan Department of Information Technology (MDIT) will work with agencies to establish the privacy officer roles and responsibilities.

Initiative 2: State of Michigan Privacy Office Creation
In an effort to create a State of Michigan privacy office, we will begin by defining the requirements and then assist with its establishment.

Initiative 3: Guideline Development and Dissemination
Guidelines are needed for the agency's privacy policy and procedures. MDIT will work to develop the guidelines and make agencies aware of them.

Initiative 4: Privacy Office Policy and Procedure Development
MDIT will provide guidelines for the privacy office's policy and procedures.

Initiative 5: Data Identification and Documentation
It is necessary for the agencies and MDIT to identify and document where all State of Michigan privacy data are collected, used, displayed, and retained.

Initiative 6: Privacy Policy Compliance Process
To ensure compliance with privacy policies, MDIT and the agencies will create and implement an agreed-upon process.

Initiative 7: Privacy Data Electronic Management

The responsibility for the initiatives related to this privacy framework development and implementation falls within three areas of State government: 1) the parent agencies where the data is needed to perform duties as assigned by State or federal laws or regulations; 2) MDIT as custodian of the electronic data; and 3) a new public facing privacy group referred to in this plan as the State of Michigan Privacy Office.

Source: Office of Enterprise Security Strategic Plan 2007 through 2010.

Exhibit 4

DATA PRIVACY

Department of Technology, Management & Budget

Generally Accepted Privacy Principles

Generally accepted privacy principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

The following are the 10 generally accepted privacy principles:

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. Choice and Consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. Collection. The entity collects personal information only for the purposes identified in the notice.

5. Use and Retention. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.

6. Access. The entity provides individuals with access to their personal information for review and update.

7. Disclosure to Third Parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for Privacy. The entity protects personal information against unauthorized access (both physical and logical).

9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. Monitoring and Enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Source: American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants *Generally Accepted Privacy Principles - A Global Privacy Framework.*

Exhibit 5

DATA PRIVACY

Department of Technology, Management & Budget

Principles of Fair Information Practices

In 1973, the U.S. Department of Health, Education, and Welfare issued a report entitled *Records, Computers, and the Rights of Citizens.* This report recommended that Congress enact legislation adopting a code of fair information practices for automated personal data systems. This code would adhere to the following principles:

1. There must be no personal-data recordkeeping systems whose very existence is secret.

2. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

These principles should govern the conduct of all personal-data recordkeeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law.

Source: U.S. Department of Health, Education, and Welfare Report of the Secretary's Advisory Committee on Automated Personal Data Systems entitled *Records, Computers, and the Rights of Citizens*, July 1973.

DATA PRIVACY
Department of Technology, Management & Budget

Personal Information Categories

Personal information categories include:

Vital Record Information:
- Birth certificate information
- Death certificate information
- Marriage certificate information
- Divorce certificate information

Health Information:
- Diagnosis information
- Prognosis information
- Treatment information
- Medical record information
- Psychotherapy notes
- Health identification number
- Health insurance identification number
- Doctor/psychologist-patient privileged information
- Physical or mental condition information
- Disability information

Tax Information:
- Taxpayer identification number
- Federal employer identification number
- Taxpayer adjusted gross income
- Exemption information
- Dependent information
- Individual's tax liability
- Nature, source, or amount of income
- Nature, source, or amount of fines
- Nature, source, or amount of penalties
- Other information on tax return
- Other information collected when return was filed

Education Information:
- Student identification number or other identifier
- List of student's characteristics
- Other personally identifiable information
- Academic information
- Financial information
- Admission information

Personnel Information:
- College transcript information
- Evaluation information
- Disciplinary information
- Employee identification number

Driver Record Information:
- Passport number
- Individual's photograph
- Medical information
- Disability information

Bank and Financial Information:
- Bank account numbers
- Personal identification numbers
- Credit card numbers
- Stock or security certificate numbers

Children's Information:
- E-mail address

Library Information:
- Materials requested
- Materials checked out

Privileged Information:
- Attorney-client privilege information
- Clergy-parishioner privilege information

Criminal Record Information:
- DNA (Deoxyribonucleic acid)
- Photographs of the individual
- Arrest or conviction histories
- Physical identifying marks (tattoos, scars, etc.)
- Crime victim information
- Witness information
- Fingerprint

Personal identifying information common to two or more categories include:

- Date of birth
- Driver's license number
- Home address
- Mother's maiden name
- Name
- Signature
- Social security number
- Telephone number

Source: Office of the Auditor General data privacy questionnaire.

GLOSSARY

AICPA	American Institute of Certified Public Accountants.
CICA	Canadian Institute of Chartered Accountants.
CPO	chief privacy officer.
Department of Environmental Quality	Executive Order No. 2009-45 created the Department of Natural Resources and Environment (DNRE), effective January 17, 2010. It transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and budgetary resources of the Department of Natural Resources (DNR) and the Department of Environmental Quality (DEQ) to DNRE by a Type II transfer and abolished DNR and DEQ.
Department of History, Arts and Libraries	Executive Order No. 2009-36 transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and budgetary resources of the Department of History, Arts and Libraries to various State departments and agencies by Type I, II, and III transfers, effective October 1, 2009, and abolished the Department.
Department of Management and Budget (DMB)	Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and appropriations of the Michigan Department of Information Technology (MDIT) to DTMB by a Type III transfer and abolished MDIT.
Department of Natural Resources	Executive Order No. 2009-45 created the Department of Natural Resources and Environment (DNRE), effective January 17, 2010. It transferred all of the authority, powers,

	duties, functions, responsibilities, records, personnel, property, equipment, and budgetary resources of the Department of Natural Resources (DNR) and the Department of Environmental Quality (DEQ) to DNRE by a Type II transfer and abolished DNR and DEQ.
DTMB	Department of Technology, Management & Budget.
effectiveness	Program success in achieving mission and goals.
FOIA	Freedom of Information Act.
instance	A specific type [category] of personal information that a respondent indicated that his or her agency collected, maintained, or disclosed. These 11 categories included: Vital record information Health information Tax information Education information Personnel information Driver record information Bank and financial information Children's information Library information Privileged information Criminal record information Each agency respondent could indicate that he or she collected, maintained, or disclosed up to 11 different categories of personal information for the questionnaire that he or she submitted.
Michigan Department of Information Technology (MDIT)	Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management & Budget (DTMB), effective March 21, 2010. It also transferred all of the authority, powers, duties, functions,

	responsibilities, records, personnel, property, equipment, and appropriations of the Michigan Department of Information Technology (MDIT) to DTMB by a Type III transfer and abolished MDIT.
observation	A commentary that highlights certain details or events that may be of interest to users of the report. An observation differs from an audit finding in that it may not include the attributes (condition, effect, criteria, cause, and recommendation) that are presented in an audit finding.
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 program operations, to facilitate decision making by parties responsible for overseeing or initiating corrective action, and to improve public accountability.
personal identifiable information	A name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver's license or State personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.
personal information	Information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information collected by an organization

	about an individual is likely to be considered personal information if it can be attributed to an identified individual.
privacy	The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.
privacy program	The policies, procedures, communications, and controls in place to manage and protect personal information in accordance with generally accepted privacy principles and criteria.
reportable condition	A matter that, in the auditor's judgment, falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the objectives of the audit; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
risk assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Secure Michigan Initiative	A self-assessment report conducted by the Michigan Department of Information Technology in 2002 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.
USC	*United States Code.*

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL