MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

DATA EXCHANGE GATEWAY

DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

September 2013

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

071-0592-13

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 Exchange Gateway

Department of Technology, Management, and Budget

Report Number:
071-0592-13

Released:
September 2013

The Data Exchange Gateway (DEG) is an enterprisewide managed file transfer system operated and supported by Data Center Operations, Department of Technology, Management, and Budget (DTMB). The DEG provides for the secure storage and electronic transmission of data between State agencies and external trading partners, such as healthcare companies and providers, banks, and other government agencies. As of June 30, 2013, there were 11 State departments that used the DEG. In fiscal year 2011-12, DTMB billed State agencies $1.9 million for DEG services.

Audit Objective:
To assess the effectiveness of DTMB's efforts to help ensure that State agencies use the DEG or other secure methods for the electronic transfer of data.

Audit Conclusion:
DTMB's efforts to help ensure that State agencies use the DEG or other secure methods for the electronic transfer of data were moderately effective. We noted one reportable condition (Finding 1).

Reportable Condition:
DTMB had not fully established an effective strategy to help ensure that State agencies used the DEG or other secure methods when electronically transferring sensitive data (Finding 1).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DTMB's efforts to implement a secure managed file transfer infrastructure.

Audit Conclusion:
DTMB's efforts to implement a secure managed file transfer infrastructure were moderately effective. We noted one reportable condition (Finding 2).

Reportable Condition:
DTMB had not fully implemented a secure managed file transfer infrastructure (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DTMB's security and access controls over the DEG.

Audit Conclusion:
DTMB's security and access controls over the DEG were moderately effective. We noted three reportable conditions (Findings 3 through 5).

Reportable Conditions:
DTMB had not fully established effective security and access controls over the

operating system for the DEG servers (Finding 3).

DTMB had not fully established effective security and access controls over the DEG database management system (Finding 4).

DTMB had not fully implemented effective baseline security controls for the authentication of users of the DEG (Finding 5).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates that it agrees 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

September 19, 2013

John E. Nixon, C.P.A, Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Mr. Nixon and Mr. Behen:

This is our report on the performance audit of the Data Exchange Gateway, Department of Technology, Management, and Budget.

This report contains our report summary; a description; our audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; a description of survey, a summary of survey responses, and a flow chart of survey questions, 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 response subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

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

This Page Left Intentionally Blank

TABLE OF CONTENTS

DATA EXCHANGE GATEWAY
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Page

INTRODUCTION

Report Summary 1
Report Letter 3
Description 7
Audit Objectives, Scope, and Methodology and Agency Responses 9

COMMENTS, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

Effectiveness of Efforts to Help Ensure Use of the DEG or Other Secure Methods for Electronic Transfer of Data 13
1. Secure Electronic Transfers 14
Effectiveness of Efforts to Implement a Secure Managed File Transfer Infrastructure 16
2. Infrastructure of the DEG 16
Effectiveness of Security and Access Controls Over the DEG 19
3. Operating System Security and Access Controls 19
4. Database Management System Security and Access Controls 20
5. Access Controls Over the DEG 21

SUPPLEMENTAL INFORMATION

Description of Survey 24

Summary of Survey Responses 25

Flow Chart of Survey Questions 30

GLOSSARY

Glossary of Acronyms and Terms 33

Data Exchange Gateway

The Data Exchange Gateway (DEG) is an enterprisewide managed file transfer system operated and supported by Data Center Operations, Department of Technology, Management, and Budget (DTMB). Managed file transfer is a technology solution that provides for the secure electronic transfer of data in an efficient and reliable manner. Managed file transfer provides a single application that handles all file transfers, regardless of the protocol*, and provides auditing, reporting, and password policy features that are needed to comply with various government requirements, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The DEG provides for the secure storage and electronic transmission of data between State agencies and external trading partners. External trading partners include healthcare companies and providers, banks and financial companies, local government agencies, federal government agencies, and other State government agencies. The DEG service began in 1997. As of June 30, 2013, there were 11 State departments that used the DEG. For example, the Department of Human Services uses the DEG to transfer $66 million per month in food stamp funds and $32 million per month in electronic cash assistance benefits to J.P.Morgan. The Department of Human Services also uses the DEG to transfer health information from the Child Support Enforcement System to healthcare providers.

The DEG acts like an electronic post office. Each transfer contains routing information similar to a postal address. The DEG reads the address and transfers files to the correct location. Some transfers have automatic delivery to a specific location, much like the delivery of mail to a home. Other transfers are stored for a short time before pickup, typically 8 days, like a post office box. As of June 30, 2013, there were approximately 2,700 automatic delivery mailboxes for outgoing messages and 6,400 pickup mailboxes.

The DEG service is available 24 hours a day, 7 days a week and is backed up by a disaster recovery* solution that resides in another hosting center.

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

State agencies transfer approximately 300 to 400 gigabytes of data each month through the DEG. Over the last five years, the amount of data transferred through the DEG has increased by 46%. State agencies are charged a rate of $0.00045 per kilobyte per month for DEG file transfer services. In fiscal year 2011-12, DTMB billed State agencies $1.9 million through interagency transfers for DEG services.

Data Center Operations (DCO)

DTMB's DCO is responsible for managing the State's computer hosting centers; supporting the DEG, Teradata data warehouse, and Unisys mainframe computer systems; providing configuration management of all mainframe computer systems, servers, and other devices within the hosting centers; and performing enterprisewide monitoring of all server devices and critical applications on the State's network.

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Data Exchange Gateway (DEG), Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DTMB's efforts to help ensure that State agencies use the DEG or other secure methods for the electronic transfer of data.

2. To assess the effectiveness of DTMB's efforts to implement a secure managed file transfer infrastructure.

3. To assess the effectiveness of DTMB's security and access controls* over the DEG.

Audit Scope

Our audit scope was to examine the information processing and other records related to the Data Exchange Gateway. 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 February through June 2013, generally covered the period October 1, 2011 through June 30, 2013.

Audit Methodology

We conducted a preliminary review of the DEG to establish our audit objectives. We obtained an understanding of DTMB's processes related to the DEG. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

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

To accomplish our first objective, we interviewed DTMB staff and reviewed policies, procedures, and standards related to the overall administration of electronic file transfers. We also reviewed and analyzed information related to unsecured file transfers that had occurred within and outside the State's network. In addition, we surveyed State agencies to gain an understanding of how data was electronically transferred, the types of entities that data was transferred to, and whether the data transferred was private or confidential.

To accomplish our second objective, we interviewed DTMB staff and reviewed the network diagram of the DEG to gain an understanding of the design of the DEG. We also interviewed DTMB staff to determine if service level agreements were established with the State agencies that use the DEG.

To accomplish our third objective, we interviewed DTMB staff to gain an understanding of the security* of the operating system*, database management system*, and access controls over the DEG. We tested the security of the operating system and the database to verify that they were secured in accordance with the Center for Internet Security* benchmarks. We tested access controls over the DEG to ensure that the controls complied with DTMB security standards.

This report summarizes security and access control weaknesses in the DEG. It does not contain detailed examples of the security and access control weaknesses because of their sensitive nature. During the course of the audit, we provided DTMB management with detailed examples of the security and access control weaknesses identified during our audit fieldwork.

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 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.

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

Agency Responses

Our audit report contains 5 findings and 5 corresponding recommendations. DTMB's preliminary response indicates that it agrees 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 the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DTMB to develop a plan to comply with the audit recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO HELP ENSURE USE OF THE DEG OR OTHER SECURE METHODS FOR ELECTRONIC TRANSFER OF DATA

COMMENT

Background: As data files have grown exponentially larger and become increasingly subject to security threats and regulations, transferring data files in a secure manner has become an area of great concern to information technology departments. File transfer protocol* (FTP) is a simple and unsecure method that was developed in the early 1970s to transfer data over a network. FTP continues to be heavily used to exchange data; however, FTP does not have strong security features, cannot handle most failed data transfers, does not offer an automated interface, does not compress data, and cannot be used for the kinds of auditing and compliance rules in effect today. Another insecure method for transferring data is through e-mail. Information technology departments worry that e-mail used in an ad hoc manner cannot be adequately monitored and controlled. Managed file transfer* is a more secure method for transferring data than FTP, e-mail, and other common methods, such as magnetic tapes, USB flash drives, and external hard drives, because of its security and compliance features. Managed file transfer provides the ability to monitor, control, and secure the transfer of data and offers high levels of security, reliability, speed, compliance, and auditability.

Audit Objective: To assess the effectiveness of the Department of Technology, Management, and Budget's (DTMB's) efforts to help ensure that State agencies use the Data Exchange Gateway (DEG) or other secure methods for the electronic transfer of data.

Audit Conclusion: DTMB's efforts to help ensure that State agencies use the DEG or other secure methods for the electronic transfer of data were moderately effective. Our assessment disclosed one reportable condition* related to secure electronic transfers (Finding 1).

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

FINDING

1. Secure Electronic Transfers

   DTMB had not fully established an effective strategy to help ensure that State agencies used the DEG or other secure methods when electronically transferring sensitive data. Without an enterprise strategy, DTMB cannot ensure that State agencies transfer sensitive data securely within the State network and with external entities.

   Executive Order No. 2009-55 requires that DTMB, under the direction and guidance of the State Chief Information Officer, develop and implement processes to replicate information technology best practices and standards throughout the executive branch of State government. In addition, the executive order states that DTMB is focused on promoting a unified approach to information technology management for departments and agencies.

   Our audit procedures and survey of State agencies disclosed:

   a. DTMB did not ensure that State agencies electronically transferred confidential and sensitive data in a secure manner. We surveyed employees from 18 State departments to gain an understanding of their electronic data transfer practices. Of the 113 responses received, 76 (67%) indicated that they transfer confidential or private data (see survey question 4). Forty-one (54%) of the 76 respondents indicated that, although they used some secure methods to transfer data, they also used unsecure methods, such as e-mail and FTP. However, 5 (7%) of the 76 respondents indicated that they used only e-mail or FTP to conduct those transfers. These methods do not provide encryption or security for the data being transferred and increase the risk of sensitive data being disclosed to unauthorized individuals.

   b. DTMB did not ensure that State agencies obtained DTMB approval to use a method other than the DEG to electronically transfer data. In certain limited cases, DTMB Technical Standard 1305.00.02 allows agencies to request exceptions to existing information technology policies, standards, and technology products, such as use of the DEG, when the associated risk and acceptable alternative solutions are identified. We identified approximately 1,600 unsecured outgoing file transfers that occurred over four days in

April 2013 that had not received an approved exception from DTMB. In addition, we noted that several of these transfers were made from State of Michigan servers that supported critical applications, many of which contained confidential data and personal identifiable information*. Without a documented and approved exception, DTMB cannot ensure that it has limited the risk of sensitive or confidential data being exposed.

c. DTMB did not ensure that State agencies were aware of the DEG service. In our survey of State departments, 100 (88%) of the 113 respondents indicated that they electronically transferred data (see survey question 3). However, 36 (36%) of the 100 respondents indicated that they had never used the DEG, with 21 (58%) of the 36 indicating that they did not know that DTMB offered the DEG service (see survey questions 7 and 8).

DEG management informed us that, since 2011, it has made presentations to one State department and two divisions of DTMB to promote the benefits of using the DEG service.

DTMB could increase the use of the DEG by State agencies with improved awareness and communication of the DEG service.

RECOMMENDATION

We recommend that DTMB fully establish an effective strategy to help ensure that State agencies use the DEG or other secure methods when electronically transferring sensitive data.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation.

With regard to part a. of the finding, DTMB informed us that DTMB Cyber Security will use data loss prevention tools to monitor unsecure FTP traffic.

With regard to part b. of the finding, DTMB informed us that it is in the process of developing a data classification standard which is expected to be implemented by

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

December 31, 2015. The data classification standard will require agencies to attest to compliance with federal and State laws and State policies and procedures. To ensure compliance with the newly implemented DTMB Technical Standard 1340.00.11, DTMB informed us that all current exceptions to the standard will be reviewed and compliance dates will be established. In addition, DTMB informed us that DTMB Technical Standard 1305.00.02 will be updated by June 30, 2014 to require compliance within one year.

With regard to part c. of the finding, DTMB informed us that a communication plan will be developed by March 31, 2014 to inform agencies of the newly published standard, the benefits of using the DEG, and the proper procedures for using the DEG.

EFFECTIVENESS OF EFFORTS TO IMPLEMENT A SECURE MANAGED FILE TRANSFER INFRASTRUCTURE

COMMENT

Audit Objective: To assess the effectiveness of DTMB's efforts to implement a secure managed file transfer infrastructure.

Audit Conclusion: DTMB's efforts to implement a secure managed file transfer infrastructure were moderately effective. Our assessment disclosed one reportable condition related to infrastructure of the DEG (Finding 2).

FINDING

2. Infrastructure of the DEG

DTMB had not fully implemented a secure managed file transfer infrastructure. Without a secure infrastructure, DTMB cannot ensure the integrity and confidentiality of data being transferred within the State's network and over the Internet.

The purpose of the DEG is to promote the receipt of safe, virus-free, electronic file transfers from State of Michigan business partners and other external entities.

Our review of the DEG infrastructure disclosed:

a. DTMB did not enable virus scanning software to check files being transferred to or from the State's network for viruses. DTMB informed us that virus scanning is a configurable setting on the DEG; however, DTMB had not yet configured the DEG software to use this feature. Without virus scanning software, DTMB cannot ensure that files entering the State's network through the DEG are free of viruses that could infect the State's network. Viruses entering the State's network through the DEG could spread across the network and affect the availability of other State resources and services.

   The Federal Information System Controls Audit Manual* (FISCAM) states that virus scanning software should be provided at critical entry points. The DEG represents a critical entry point into the State of Michigan network.

b. DTMB had not established service level agreements with the 11 State departments that used the DEG for file transfers. As a result, misunderstandings could occur between DTMB and the various State departments using the file transfer services provided by DTMB.

   Executive Order No. 2009-55 requires DTMB to develop and periodically update service level agreements with executive branch departments and agencies to ensure that it delivers quality information technology services. According to Control Objectives for Information and Related Technology* (COBIT), the purpose of a service level agreement is to establish the roles, responsibilities, customer commitment, and performance expectations for information technology services provided. For the DEG, this would include such items as how often the file transfer service will be available and response times for various classes of problems.

c. DTMB did not restrict State agencies from using an unsecured FTP for data transfers through the DEG within the State's network. Without additional control, confidential and sensitive data is at an increased risk of being disclosed to unauthorized persons as it is transferred within the State's network using the DEG.

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

FISCAM states that information systems should be reviewed to identify and eliminate unnecessary services and that the purpose of services should be documented and approved by management.

DTMB configured the DEG to prevent data from entering or leaving the State's network using an unsecured FTP unless an approved request was received from an authorized requestor. However, DTMB did not have these controls in place for transfers within the State's network. Data transferred via FTP is transmitted in plain text, which can be viewed as it is passed over the network.

The security risk increases if a State agency includes passwords or other confidential information in the data being transmitted. DTMB relies on State agencies to determine and use the appropriate transfer method when transferring data to and receiving data from other agencies using the DEG.

DTMB should limit the risk of State agencies using FTP to send sensitive and confidential data by requiring agencies to submit a request that documents the need to use FTP for transfers via the DEG within the State's network.

RECOMMENDATION

We recommend that DTMB fully implement a secure managed file transfer infrastructure.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation.

With regard to part a. and part c. of the finding, DTMB informed us that it will perform a hardware and software migration of the DEG platform by December 31, 2013, which will include the implementation of virus scanning and provide DTMB with the ability to restrict the use of unsecured FTP through the DEG within the State's network.

With regard to part b. of the finding, DTMB informed us that it has developed a service catalog for the DEG service that includes terms of use and service levels that will be reviewed annually to ensure accuracy.

EFFECTIVENESS OF
SECURITY AND ACCESS CONTROLS OVER THE DEG

COMMENT

Audit Objective: To assess the effectiveness of DTMB's security and access controls over the DEG.

Audit Conclusion: DTMB's security and access controls over the DEG were moderately effective. Our assessment disclosed three reportable conditions related to operating system security and access controls, database management system security and access controls, and access controls over the DEG (Findings 3 through 5).

FINDING

3. Operating System Security and Access Controls

DTMB had not fully established effective security and access controls over the operating system for the DEG servers. As a result, DTMB cannot ensure that DEG data is protected from unauthorized modification, loss, or disclosure.

DTMB Technical Standard 1340.00.03 requires secure establishment, maintenance, and administration of servers, including operating system software and data residing on the servers. To achieve a secure operating system, the standard requires that controls be established to protect information and resources from unauthorized access. In addition, it requires that the operating system be installed with a minimal service configuration to reduce the risk of network intrusion or exploitation of well-known operating system vulnerabilities*.

We assessed the configuration of six servers used for the DEG using the Center for Internet Security benchmarks for a secure operating system configuration. Our review disclosed potentially vulnerable operating system configurations on all six servers. Because of the confidentiality of operating system configurations, we summarized our testing results for presentation in this finding and provided the detailed results to DTMB.

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

RECOMMENDATION

We recommend that DTMB fully establish effective security and access controls over the operating system for the DEG servers.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation and informed us that it will implement a Lightweight Directory Access Protocol by September 30, 2014, which will improve security and access controls. In addition, DTMB informed us that it will implement an automated configuration management tool by March 31, 2014, which will assist in rapidly deploying, maintaining, and auditing operating system security and access controls. The tool will also prevent changes from the required minimal service configurations and deviations from approved initial operating system configuration settings.

FINDING

4. Database Management System Security and Access Controls

DTMB had not fully established effective security and access controls over the DEG database management system. Fully establishing database management system security and access controls would help prevent the unauthorized modification of database configurations and settings. Unauthorized modification of database configurations and settings could prevent State agencies from being able to send and receive messages through the DEG application.

Data files transferred using the DEG are called messages. The messages transferred by the DEG are stored in an encrypted storage area network and not in the DEG database. However, security and access controls over the DEG database are important because the DEG database contains the configurations and settings necessary for the secure operation of the DEG application.

National Institute of Standards and Technology* (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, recommends that an organization establish, document, and implement mandatory configuration settings for a given information technology

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

platform using a security configuration checklist, also referred to as a hardening guide, security guide, or benchmark.

Our review disclosed:

a. DTMB had not established procedures for hardening the DEG database management system and maintaining a secure database configuration. Proper configuration of database security settings helps to prevent unauthorized access and ensure the integrity of data within the database.

b. DTMB had not fully implemented effective security configurations over the DEG database management system. We assessed the configuration of the DEG database management system using the Center for Internet Security benchmarks for a secure database configuration. Our review disclosed potentially vulnerable database configurations on the DEG database. Because of the confidentiality of database configurations, we summarized our testing results for presentation in this finding and provided the detailed results to DTMB.

RECOMMENDATION

We recommend that DTMB fully establish effective security and access controls over the DEG database management system.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation and informed us that it will create internal procedures to document the hardening process for the DEG database and establish effective security and access controls over the DEG database by June 30, 2014 as defined by best practices from the Center for Internet Security.

FINDING

5. Access Controls Over the DEG

DTMB had not fully implemented effective baseline security controls for the authentication of users of the DEG. As a result, DTMB cannot ensure that the data transferred via the DEG is protected from disclosure to unauthorized users.

DTMB Technical Standard 1335.00.03 defines the minimum baseline security controls as they relate to identification, authentication, and access controls for the State of Michigan information systems. The standard applies to all executive branch networks, systems, computers, data, databases, and applications. Effective access controls, such as requiring unique user codes and strong passwords, regularly changing passwords, and limiting invalid log-on attempts, help mitigate inappropriate access to computer resources, thereby protecting those resources from unauthorized modification, loss, and disclosure.

Our review disclosed that DTMB did not implement authentication controls over user access to the DEG in accordance with DTMB Technical Standard 1335.00.03. We determined that baseline security controls were not in place related to the frequency for changing passwords, the requirements for complex passwords, and the number of invalid log-on attempts before the user code is locked out. As a result, DTMB cannot ensure that it reduced the risk of unauthorized users gaining access to sensitive or confidential data in a DEG mailbox not assigned to them.

RECOMMENDATION

We recommend that DTMB fully implement effective baseline security controls for the authentication of users of the DEG.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation and informed us that it will perform a hardware and software migration of the DEG platform by December 31, 2013. The migration will allow DTMB to implement effective authentication security controls for the DEG and comply with DTMB Technical Standard 1335.00.03. However, DTMB anticipates significant challenges related to mandating password expirations for some external trading partners.

SUPPLEMENTAL INFORMATION

Description of Survey

We developed a survey to request input from employees in State departments regarding the electronic file transfer practices used to transfer data.

With the assistance of the Department of Technology, Management, and Budget, we e-mailed 132 employees from 18 State departments and provided them with a link to complete the survey on-line. We received responses from 113 State employees, a response rate of 86%.

Of the 100 respondents who indicated that they electronically transfer data, 76 (76%) responded that the data transferred included confidential or private data. Of those 76 respondents, 47 (62%) indicated that they used the DEG to transfer this data, whereas the remaining 29 (38%) responded that they did not use the DEG to transfer the data.

Of the 100 respondents who indicated that they electronically transferred data, 63 (63%) indicated that they currently use the DEG. Of those 63 respondents, 52 (83%) responded that they were either satisfied or very satisfied with the DEG service. In addition, 43% of the respondents indicated that they had not experienced any problems with the DEG service in the past two years. Those respondents who indicated that they had experienced some problems using the DEG service reported that the problems were infrequent and all were satisfactorily resolved.

Following is a summary of the survey responses, including the number and percentage of responses received for each question. The total number of responses for each question may not equal 113 respondents because some respondents were not required to answer all questions. After the summary of the survey responses, a flow chart is provided showing which questions respondents would answer based on the response provided. Also, we did not include comments to survey questions that asked for respondent comments. However, we did include the questions and the number of respondents that had comments.

DATA EXCHANGE GATEWAY
Department of Technology, Management, and Budget

Summary of Survey Responses

1. Please select your department.

Department	Number of Department Response	Number of DTMB Response for Department	Total Number of Responses
Michigan Department of Agriculture and Rural Development	1		1
Department of Attorney General	1		1
Department of Civil Rights	3		3
Michigan Civil Service Commission	1	1	2
Department of Community Health	12	8	20
Department of Corrections	15		15
Michigan Department of Education	2		2
Department of Environmental Quality	1		1
Department of Human Services	1	4	5
Department of Insurance and Financial Services	10		10
Department of Licensing and Regulatory Affairs	4	1	5
Department of Military and Veterans Affairs	2		2
Department of Natural Resources	15		15
Department of State	1		1
Michigan Department of State Police	5		5
Department of Technology, Management, and Budget (DTMB)	8		8
Michigan Department of Transportation	1	1	2
Department of Treasury	15		15
Total	98	15	113
Percent of Total	86.7%	13.3%	100.0%

3. Does your agency electronically transfer data to and/or receive data from other governmental agencies, vendors, organizations, or businesses? (Please select all that apply.) (See Finding 1.)

Answer Options	Response Percent	Response Count
a. Yes, we send data.	77.9%	88
b. Yes, we receive data.	69.9%	79
c. No, we do not send or receive data.	11.5%	13
	answered question	113
	skipped question	0

4. Is any of the data that is electronically transferred confidential or private data (e.g., criminal history information, patient medical information, proprietary data, social security numbers, tax information, or other personal identifiable information)? (See Finding 1.)

Answer Options	Response Percent	Response Count
Yes	76.0%	76
No	24.0%	24
	answered question	100
	skipped question	13

5. With which of the following entities does your agency exchange data? (Please select all that apply.)

Answer Options	Response Percent	Response Count
a. Intra-agency	60.0%	60
b. Other State of Michigan agencies	69.0%	69
c. Federal agencies	53.0%	53
d. Local agencies	34.0%	34
e. Vendors	54.0%	54
f. Other organizations or businesses (please explain)	31.0%	31
	answered question	100
	skipped question	13

6. What method does your agency use to transfer data to or receive data from other entities? (Please select all that apply.)

Answer Options	Response Percent	Response Count
a. E-mail	49.0%	49
b. Data Exchange Gateway services	54.0%	54
c. FTP	35.0%	35
d. FTPS (FTP/SSL)	21.0%	21
e. SFTP (SSH)	21.0%	21
f. Web Client HTTPS	20.0%	20
g. I am not sure.	19.0%	19
h. Other (please describe)	21.0%	21
	answered question	100
	skipped question	13

7. Please select the statement that best describes your agency's use of the Department of Technology, Management, and Budget's Data Exchange Gateway (DEG). (See Finding 1.)

Answer Options	Response Percent	Response Count
a. We currently use the DEG.	63.0%	63
b. We have previously used the DEG but are not currently using it.	1.0%	1
c. We have never used the DEG.	36.0%	36
	answered question	100
	skipped question	13

8. Please select the statement that best describes the reason your agency does not use the DEG. (Please select all that apply.) (See Finding 1.)

Answer Options	Response Percent	Response Count
a. We did not know about the DEG service.	56.8%	21
b. The DEG service is too costly.	0.0%	0
c. The DEG is difficult to use.	0.0%	0
d. The DEG method of transfers is not compatible with our agency systems.	8.1%	3
e. We have an agency system that performs the same task.	8.1%	3
f. We have experienced problems using the DEG in the past.	5.4%	2
g. Other (please explain)	40.5%	15
	answered question	37
	skipped question	76

9. What method does your agency use for transferring data through the DEG? (Please select all that apply.)

Answer Options	Response Percent	Response Count
a. SoM DEG Web page (HTTPS)	34.9%	22
b. FTP	28.6%	18
c. FTPS (FTP/SSL)	19.0%	12
d. SFTP (SSH)	22.2%	14
e. I am not sure.	39.7%	25
	answered question	63
	skipped question	50

10. Does your agency use the DEG for all data transfers?

Answer Options	Response Percent	Response Count
a. Yes	11.1%	7
b. No	50.8%	32
c. I am not sure.	38.1%	24
	answered question	63
	skipped question	50

11. Please select the statement that best describes the reason your agency does not use the DEG for all data transfers. (Please select all that apply.)

Answer Options	Response Percent	Response Count
a. We did not know about the DEG service.	0.0%	0
b. The DEG service is too costly.	10.7%	6
c. The DEG is difficult to use.	8.9%	5
d. The DEG method of transferring data is not compatible with our agency systems.	5.4%	3
e. We have an agency system that performs the same task.	17.9%	10
f. We have experienced problems using the DEG in the past.	1.8%	1
g. I am not sure.	44.6%	25
h. Other (please explain)	41.1%	23
	answered question	56
	skipped question	57

12. How frequently has your agency experienced problems with the DEG within the past two years?

Answer Options	Response Percent	Response Count
a. Daily	1.6%	1
b. Weekly	1.6%	1
c. Monthly	11.1%	7
d. Once per year	42.9%	27
e. Never	42.9%	27
	answered question	63
	skipped question	50

13. Please select the statement(s) that best describe the problems you have experienced with using the DEG. (Please select all that apply.)

Answer Options	Response Percent	Response Count
a. Some files were not received from sender.	50.0%	18
b. Some files were not sent to recipient.	44.4%	16
c. We were unable to access one or more of our mailboxes.	19.4%	7
d. Data was corrupt when it was received or sent.	2.8%	1
e. Other (please describe)	27.8%	10
answered question		36
skipped question		77

14. Were the problems you experienced using the DEG resolved in a satisfactory manner?

Answer Options	Response Percent	Response Count
a. Yes	100.0%	36
b. No	0.0%	0
answered question		36
skipped question		77

15. Please provide a brief description of the DEG data transfer problems that were not satisfactorily resolved.

Answer Options		Response Count
		0
answered question		0
skipped question		113

16. Please rate your overall satisfaction with the DEG.

Answer Options		Response Count
Very satisfied		23
Satisfied		29
Not satisfied but not unsatisfied		9
Unsatisfied		1
Very unsatisfied		1
answered question		63
skipped question		50

17. In what ways could the DEG be improved to better serve your agency's data transfer needs?

Answer Options		Response Count
		25
answered question		25
skipped question		88

18. Please provide any other information you would like us to know about your experience using the DEG.

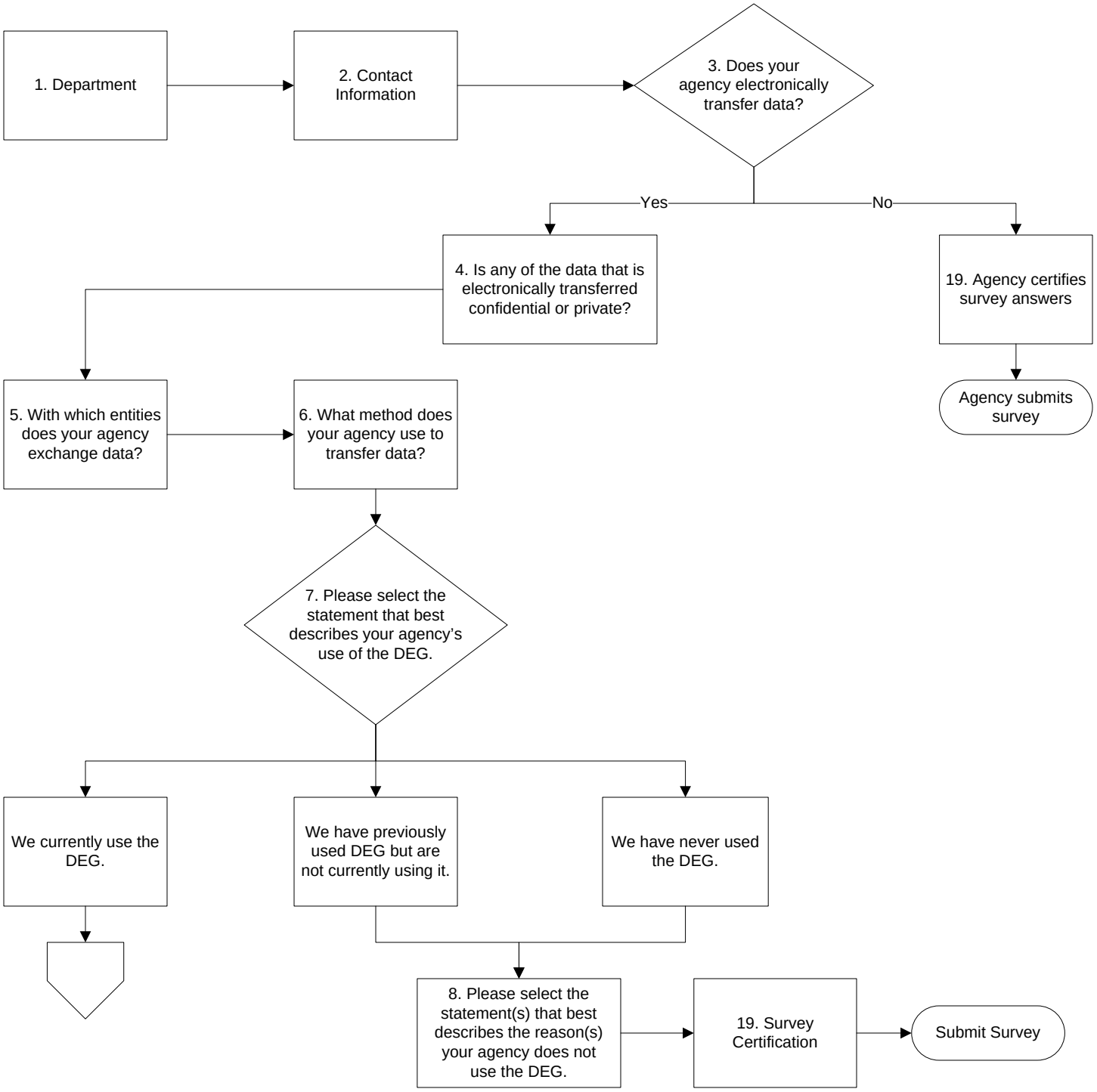
Answer Options		Response Count
		18
	answered question	18
	skipped question	95

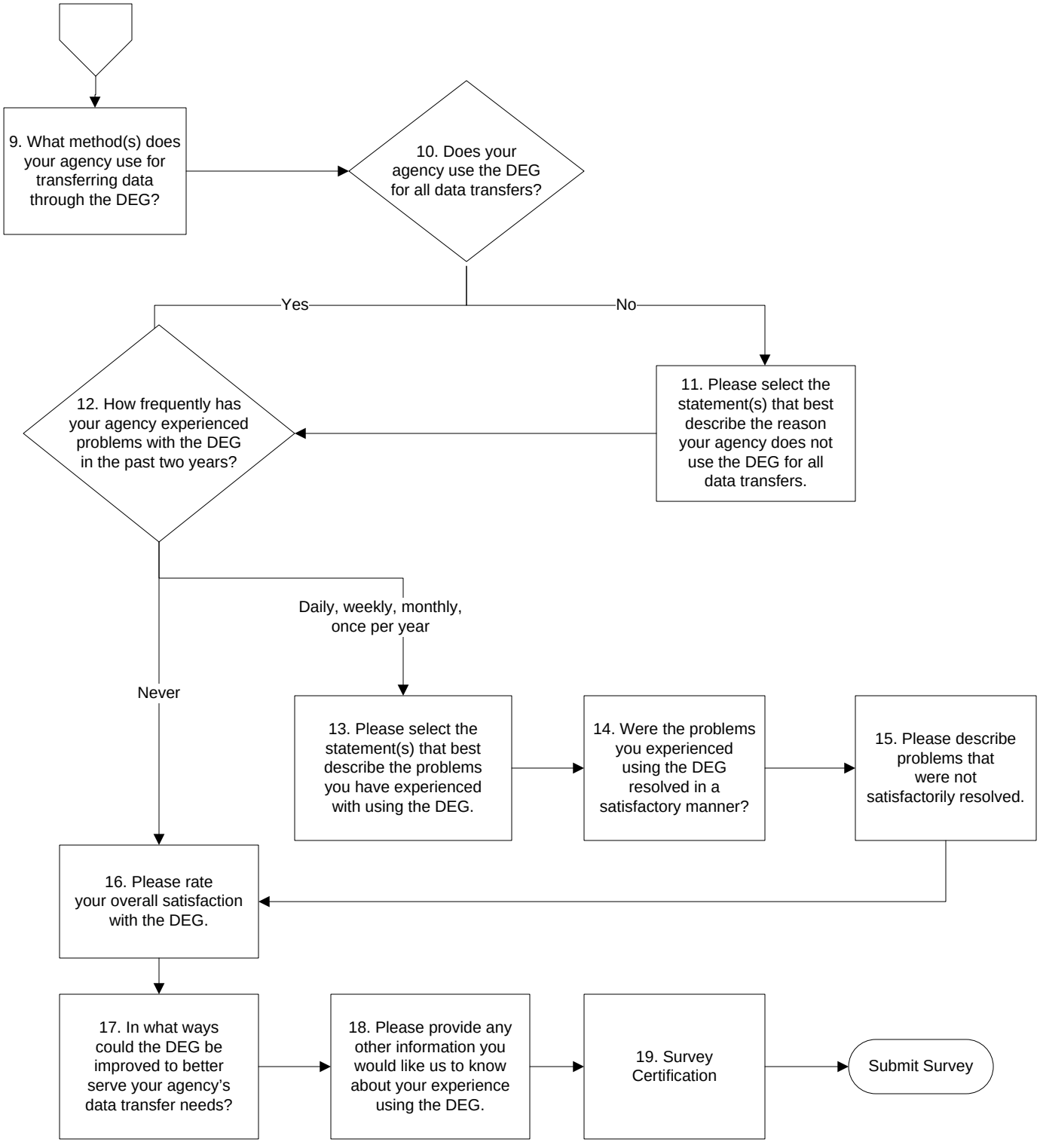
19. Survey Certification

Answer Options	Response Percent	Response Count
By checking this box, I certify that, to the best of my knowledge, the preceding information is accurate.	100.0%	113
	answered question	113
	skipped question	0

DATA EXCHANGE GATEWAY (DEG)
Department of Technology, Management, and Budget

Flow Chart of Survey Questions





Source: Office of the Auditor General analysis of data reported in DEG survey.

GLOSSARY

Glossary of Acronyms and Terms

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
Center for Internet Security	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.
database management system	A software product that aids in controlling and using the data needed by application programs. Database management systems organize data in a database; manage all requests for database actions, such as queries or updates from users; and permit centralized control of security and data integrity.
DCO	Data Center Operations.
DEG	Data Exchange Gateway.
disaster recovery	The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.

Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.
file transfer protocol (FTP)	A protocol used to transfer files over a Transmission Control Protocol/Internet Protocol (TCP/IP) network, such as the Internet.
managed file transfer	A technology solution that provides for the secure electronic transfer of data in an efficient and reliable manner; handles all file transfers, regardless of the protocol; and provides auditing, reporting, and password policy features that are needed to comply with various government requirements.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
personal identifiable information	Any information that permits the identity of an individual to be directly or indirectly inferred. This may include first name or

	initial and last name, address, or telephone number in conjunction with social security number, driver's license number, credit card number, or health and medical information.
protocol	In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and 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 audit objectives; 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.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL