MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

MICHIGAN WOMEN, INFANTS, AND CHILDREN INFORMATION SYSTEM (MI-WIC)

DEPARTMENT OF COMMUNITY HEALTH AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

January 2012

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

391-0592-11

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

Michigan Women, Infants, and Children Information System (MI-WIC)

Department of Community Health (DCH) and Department of Technology, Management, and Budget (DTMB)

Report Number:
391-0592-11

Released:
January 2012

MI-WIC is an automated information system developed by a third party vendor that DCH and authorized local agencies use to process participant data, determine eligibility, and issue benefits for the Women, Infants, and Children (WIC) Program. The WIC Program is a 100% federally funded food and nutrition program for improving health outcomes and the quality of life for eligible women, infants, and children. DTMB provides information technology support services to DCH for MI-WIC, such as operating system configuration and database administration.

Audit Objective:
To assess the effectiveness of DCH and DTMB's security and access controls over the MI-WIC database.

Audit Conclusion:
We concluded that DCH and DTMB's security and access controls over the MI-WIC database were moderately effective. We noted one material condition (Finding 1) and two reportable conditions (Findings 2 and 3).

Material Condition:
DCH, in conjunction with DTMB, did not effectively monitor the third party vendor's security configuration of the MI-WIC database (Finding 1).

Reportable Conditions:
DTMB, in conjunction with DCH, had not fully established security controls over the MI-WIC database (Finding 2).

DTMB had not fully established effective security and access controls over the MI-WIC operating system (Finding 3).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DCH's efforts to control high-risk access to MI-WIC.

Audit Conclusion:
We concluded that DCH's efforts to control high-risk access to MI-WIC were effective. However, we noted one reportable condition (Finding 4).

Reportable Condition:
DCH did not document authorization for user access to MI-WIC for selected high-risk State level MI-WIC users (Finding 4).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DCH's efforts to establish application controls over the processing of client data within MI-WIC.

Audit Conclusion:
We concluded that DCH's efforts to establish application controls over the processing of client data within MI-WIC were effective. Our audit report does not include any reportable conditions related to this audit objective.

Noteworthy Accomplishments:
DCH and the third party vendor completed the development and implementation of MI-WIC within the projected time frame. In 2009, the U.S. Department of Agriculture (USDA) approved MI-WIC for administering the WIC Program in Michigan. The USDA has recognized MI-WIC as a model system that can be used by other states for administering their WIC Program. Since 2010, 18 agencies from other states and 5 USDA regional offices have visited Michigan to review MI-WIC for implementation in their home state or region.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 4 findings and 4 corresponding recommendations. DCH and DTMB's preliminary response indicates that they agree with all of the recommendations and have complied or will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

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

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

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

January 18, 2012

Ms. Olga Dazzo, Director
Department of Community Health
Capitol View Building
Lansing, Michigan
and
John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan

Dear Ms. Dazzo and Mr. Nixon:

This is our report on the performance audit of the Michigan Women, Infants, and Children Information System, Department of Community Health and Department of Technology, Management, and Budget.

This report contains our report summary; description of system; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; 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 agencies' response subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies 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 agencies 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

MICHIGAN WOMEN, INFANTS, AND CHILDREN INFORMATION SYSTEM
DEPARTMENT OF COMMUNITY HEALTH AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

Description of System

Michigan Women, Infants, and Children Information System (MI-WIC)

MI-WIC is an automated information system used by the Women, Infants, and Children (WIC) Program, Department of Community Health (DCH), and authorized local health agencies to process participant data, determine eligibility, and issue benefits for the WIC Program. The WIC Program's mission* is to improve health outcomes and quality of life for eligible women, infants, and children by providing nutritious food, nutrition education, breastfeeding promotion and support, and referrals to health and other services. Each month, more than 200,000 women, infants, and children under age 5 receive nutritious foods from the Michigan WIC Program. WIC Program foods are worth $30 to $112 or more per month for each participant. The WIC Program is designed for families with inadequate income that are at special risk with respect to diet and physical and mental health due to inadequate nutrition or health care. The WIC Program is a 100% federally funded food and nutrition program. During fiscal year 2009-10, MI-WIC processed benefits totaling $119 million.

The State contracted with a third party vendor to develop, implement, and support MI-WIC. MI-WIC was implemented in May 2009 and is used by 48 local health agencies with 219 clinics in 83 counties serving approximately 430,000 participants a year. The local health agencies use MI-WIC to verify that potential participants meet program eligibility requirements. Potential participants who meet all categorical, residency, income, and nutritional risk requirements are certified (accepted) into the WIC Program.

MI-WIC is composed of four modules: administration, clinic, nutrition, and vendor. The administration module is used to perform administrative tasks such as scheduling, user and agency/clinic setup, time studies, and data maintenance. The clinic module is used to perform tasks such as precertifying participants; scheduling appointments; assessing nutritional risks; documenting intake, laboratory, and medical and nutrition history data; assigning a food prescription; and issuing benefits. The nutrition module is used to perform tasks such as maintaining universal product code information, creating and editing food packages, and maintaining infant formula information. The vendor module is used to perform tasks such as maintaining vendor information and determining

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

vendor eligibility and compliance. Participant data stored in MI-WIC includes name, address, age, date of birth, health data, family data, food authorization, and case notes. All data that individually identifies an applicant, a participant, or family members is considered confidential according to federal regulations.

Department of Technology, Management, and Budget (DTMB)

DTMB provides information technology support services to DCH for MI-WIC, including operating system* configuration and database administration. Also, according to the service level agreement between DCH and DTMB, DTMB is responsible for information technology general controls for MI-WIC.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Michigan Women, Infants, and Children Information System (MI-WIC), Department of Community Health (DCH) and Department of Technology, Management, and Budget (DTMB), had the following objectives:

1. To assess the effectiveness* of DCH and DTMB's security* and access controls* over the MI-WIC database.

2. To assess the effectiveness of DCH's efforts to control high-risk access to MI-WIC.

3. To assess the effectiveness of DCH's efforts to establish application controls* over the processing of client data within MI-WIC.

Audit Scope

Our audit scope was to examine the information processing and other records related to the Michigan Women, Infants, and Children Information System. 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 June through September 2011, generally covered the period October 1, 2009 through September 30, 2011.

Audit Methodology

We conducted a preliminary review of security and access controls over MI-WIC. We obtained an understanding of MI-WIC controls, including an understanding of the Women, Infants, and Children (WIC) Program business processes. We also attended a MI-WIC application demonstration by DCH to obtain an understanding of the application and the eligibility determination process for a WIC participant. 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, DCH's WIC Program, and third party vendor staff and reviewed DTMB policies and procedures to obtain an understanding of security and access controls. We also reviewed controls over the production database and operating system. In addition, we reviewed the service level agreement between DCH and DTMB and the third party vendor's contract with the State to obtain an understanding of each party's roles and responsibilities for security controls. Also, we judgmentally selected and evaluated configuration settings of the database and operating system on which MI-WIC resides for appropriateness with industry standards and best practices. Further, we judgmentally selected and evaluated the access rights of user accounts that had access to the database and operating system for appropriateness with job roles and responsibilities.

To accomplish our second objective, we interviewed DCH's WIC Program staff and reviewed the WIC Program policies and procedures to obtain an understanding of user access rights, monitoring of user access, and high-risk user permissions of the MI-WIC application. Also, we judgmentally selected and tested high-risk user access rights. Further, we judgmentally selected and tested the WIC Program's monitoring processes.

To accomplish our third objective, we interviewed DCH's WIC Program staff to gain an understanding of critical information processing controls within MI-WIC. We reviewed application controls over the clinic module in the MI-WIC. We also reviewed MI-WIC documentation. In addition, we judgmentally selected and tested data fields within MI-WIC to determine the completeness of data processing controls. We developed tests of critical information maintained in MI-WIC used for determining participant eligibility, such as age, date of birth, income, family size, and other participant data. We also developed tests of critical functionality based on federal system requirements, such as calculation of income levels exceeding program standards, calculation of certification expiration date, and edits to prevent overissuance during food package creation.

This report summarizes security and access control weaknesses in MI-WIC. 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 DCH and DTMB management with detailed examples of the security and access control weaknesses identified during our 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. To the extent practical, we add balance to our audit reports by presenting noteworthy accomplishments for exemplary achievements identified during our audits.

Agency Responses

Our audit report contains 4 findings and 4 corresponding recommendations. DCH and DTMB's preliminary response indicates that they agree with all of the recommendations and have complied or will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' 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 DCH and 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 agencies to take additional steps to finalize the plan.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF SECURITY AND ACCESS CONTROLS OVER THE MICHIGAN WOMEN, INFANTS, AND CHILDREN INFORMATION SYSTEM (MI-WIC) DATABASE

COMMENT

Audit Objective: To assess the effectiveness of the Department of Community Health (DCH) and the Department of Technology, Management, and Budget's (DTMB's) security and access controls over the MI-WIC database.

Audit Conclusion: We concluded that DCH and DTMB's security and access controls over the MI-WIC database were moderately effective. Our assessment disclosed one material condition*. DCH, in conjunction with DTMB, did not effectively monitor the third party vendor's security configuration of the MI-WIC database (Finding 1). Our assessment also disclosed two reportable conditions* related to database security and access controls and operating system security and access controls (Findings 2 and 3).

FINDING

1. Database Security Management

   DCH, in conjunction with DTMB, did not effectively monitor the third party vendor's security configuration of the MI-WIC database. As a result of not effectively monitoring the third party vendor's security configuration of the MI-WIC database, we identified numerous database security weaknesses as reported in Finding 2. Securing the MI-WIC database from potential vulnerabilities* is essential for ensuring the confidentiality of participant data.

   Control Objectives for Information and Related Technology* (COBIT) best practices state that there should be a general monitoring framework and approach. Monitoring should include periodically reviewing performance against targets, analyzing the cause of any deviations, and initiating remedial action to address the underlying causes.

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

Title 7, Part 246, section 26(d) of the *Code of Federal Regulations* states that participant data is confidential and state agencies must restrict use and disclosure of participant data. The MI-WIC database contains participant data such as name, address, age, date of birth, health data, family data, food authorization, and case notes.

RECOMMENDATION

We recommend that DCH, in conjunction with DTMB, effectively monitor the third party vendor's security configuration of the MI-WIC database.

AGENCY PRELIMINARY RESPONSE

DCH, in conjunction with DTMB, agrees with the recommendation and will effectively monitor the security configuration of the MI-WIC database. DTMB informed us that DTMB Agency Services will evaluate the MI-WIC database software installation, configuration, and patching levels and recommend the appropriate remediation actions. In addition, DTMB informed us that it will work with the vendor to prepare a plan for the routine monitoring of software versions and for applying any necessary upgrades to the database's security configuration. As part of this process, DTMB, in conjunction with DCH, will ensure that the appropriate security patches are installed.

FINDING

2. Database Security and Access Controls

DTMB, in conjunction with DCH, had not fully established security controls over the MI-WIC database. Fully established database security controls would help prevent or detect inappropriate access to the MI-WIC data.

According to ISO/IEC 27002:2005*, *Information technology - Security techniques - Code of practice for information security management,* a well-secured database provides a protected environment to maintain the integrity and confidentiality of data. Appropriate security controls include using individual user accounts and passwords, monitoring to ensure that users are performing only the activities which they are explicitly authorized to perform, and using audit logs to record and monitor significant events.

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

Our review of the MI-WIC database disclosed:

a. DTMB had not fully developed and implemented policies and procedures for managing database security and access. For example, DTMB had not established policies and procedures for granting privileged access* or other direct database access, hardening the database management system, maintaining a secure database configuration, and monitoring privileged activities. Without complete policies and procedures, security controls may be inadequate and may not be consistently applied.

b. DTMB, in conjunction with DCH, did not document and maintain the authorization and approval of database access. Documenting authorization and approval of database access helps to ensure that only appropriate individuals have access to the database and that access is appropriate.

c. DTMB did not ensure effective configuration of the database security settings, such as profile settings and configuration parameters. Proper configuration of database security settings helps to prevent unauthorized access and ensure the integrity of data within the database.

d. DTMB did not sufficiently restrict access granted to all database users. As a result, user accounts had privileges beyond their business need, which could allow individuals to exploit database weaknesses and to view, copy, or modify confidential or sensitive data.

e. DCH, in conjunction with DTMB, did not evaluate the sensitivity of the data to determine the need to encrypt data stored within the MI-WIC database. Encryption is a method used to change data into an unreadable format. DTMB technical standard 1340.00.03 encourages State agencies to encrypt sensitive data. Encryption would help ensure that confidential data in MI-WIC, such as participant name and health data, is protected from unauthorized disclosure.

f. DTMB did not use database audit logs to monitor the activity of database administrators* and other privileged accounts*. In addition, DTMB did not

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

implement a process to routinely monitor database activity. Audit logs can be configured to record privileged access to identify unusual or unauthorized activity. The recording and monitoring of selected high-risk events would help to enhance database security.

RECOMMENDATION

We recommend that DTMB, in conjunction with DCH, fully establish security controls over the MI-WIC database.

AGENCY PRELIMINARY RESPONSE

DTMB, in conjunction with DCH, agrees with the recommendation and will fully establish security controls over the MI-WIC database.

With regard to part a., DTMB indicated that it will fully develop and implement policies and procedures for managing database security and access. Upon DCH's approval, DTMB indicated that it will assume control of production database user access procedures.

With regard to part b., DTMB indicated that it will document and maintain the authorization and approval of database access. In addition, DTMB and DCH will determine if existing Oracle user access request procedures and forms for granting and modifying database accounts are appropriate for MI-WIC.

With regard to part c., DTMB indicated that it will review the database security settings, such as user profile settings and database configuration parameters, and direct the application vendor to implement the recommended settings.

With regard to part d., DTMB indicated that it will review database access and determine what, if any, additional restrictions are necessary. DTMB will direct the vendor to implement modifications to access settings as appropriate.

With regard to part e., DTMB and DCH indicated that they will evaluate the sensitivity of the data and determine if encryption of the MI-WIC database is necessary. If it is determined that encryption is necessary, DTMB informed us that it will review available options with DCH and assist DCH in determining which solution best fits MI-WIC business needs.

With regard to part f., DTMB indicated that it will periodically monitor database activity and implement the use of database audit logs to monitor the activity of database administrators and other privileged accounts. DTMB will implement enterprise solutions addressing account monitoring.

FINDING

3. Operating System Security and Access Controls

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

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

Our review of two servers that contained the MI-WIC database identified potentially vulnerable operating system configurations on both servers. Because of the confidentiality of operating system configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to DTMB.

After we provided the detailed results to DTMB, DTMB informed us that it had started taking steps to correct the weaknesses. DTMB also informed us that it had enterprise-wide projects in progress that would address some of the weaknesses.

RECOMMENDATION

We recommend that DTMB fully establish effective security and access controls over the MI-WIC operating system.

AGENCY PRELIMINARY RESPONSE

DTMB agrees with the recommendation and will fully establish effective security and access controls over the MI-WIC operating system. As noted in the finding, during the audit, DTMB already began to implement the necessary corrective actions and will continue to work to fully implement the recommendation.

EFFECTIVENESS OF EFFORTS TO CONTROL HIGH-RISK ACCESS TO MI-WIC

COMMENT

Audit Objective: To assess the effectiveness of DCH's efforts to control high-risk access to MI-WIC.

Audit Conclusion: We concluded that DCH's efforts to control high-risk access to MI-WIC were effective. However, our assessment disclosed one reportable condition related to application access controls (Finding 4).

FINDING

4. Application Access Controls

DCH did not document authorization for user access to MI-WIC for selected high-risk State level MI-WIC users. Documenting the authorization of user access helps to ensure that only appropriate individuals have access to MI-WIC and that access is appropriate.

DTMB Administrative Guide policy 1335.00 states that DCH should provide a mechanism for controlling and documenting the authorization of user access rights.

We reviewed 18 high-risk MI-WIC users to determine if their access rights were appropriate and approved. DCH was unable to support that the 18 users were authorized to have access or that the roles assigned were appropriate. WIC Program management informed us that these 18 users assisted with the development of the system before the authorization process was in place and that the level of access of each of the 18 users was appropriate. However, for the

18 high-risk MI-WIC users, management did not have documentation of its formal approval.

RECOMMENDATION

We recommend that DCH document authorization for user access to MI-WIC for selected high-risk State level MI-WIC users.

AGENCY PRELIMINARY RESPONSE

DCH agrees that it did not appropriately document access authorization for the 18 MI-WIC users cited in the finding. These users assisted with initial system development of MI-WIC and were granted these roles before the authorization process was established.

As part of the system development process, DCH established procedures to authorize and document role assignments at the State level. DCH indicated that it will reevaluate the access of the 18 users identified and assign more restrictive roles if necessary.

EFFECTIVENESS OF EFFORTS TO ESTABLISH APPLICATION CONTROLS OVER THE PROCESSING OF CLIENT DATA WITHIN MI-WIC

COMMENT

Audit Objective: To assess the effectiveness of DCH's efforts to establish application controls over the processing of client data within MI-WIC.

Audit Conclusion: We concluded that DCH's efforts to establish application controls over the processing of client data within MI-WIC were effective. Our audit report does not include any reportable conditions related to this audit objective.

Noteworthy Accomplishments: DCH and the third party vendor completed the development and implementation of MI-WIC within the projected time frame. In 2009, the U.S. Department of Agriculture (USDA) approved MI-WIC for administering the WIC Program in Michigan. The USDA has recognized MI-WIC as a model system that can be used by other states for administering their WIC Program. Since 2010, 18 agencies from other states and 5 USDA regional offices have visited Michigan to review MI-WIC for implementation in their home state or region.

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.
application controls	Controls that are directly related to individual computer applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
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 administrator	The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.
DCH	Department of Community Health.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
ISO/IEC 27002:2005	A security standard published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an

organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management.

material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
mission	The main purpose of a program or an agency or the reason that the program or the agency was established.
MI-WIC	Michigan Women, Infants, and Children Information System.
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 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.
privileged access	Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
privileged account	An account that has access to all commands and files on an operating system or database management system.
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 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.
security controls	Controls that safeguard an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
USDA	U.S. Department of Agriculture.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.
WIC	Women, Infants, and Children.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL