MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

OPERATING SYSTEM CONTROLS
FOR THE UNEMPLOYMENT INSURANCE AGENCY'S MAINFRAME
INFORMATION SYSTEMS

DEPARTMENT OF INFORMATION TECHNOLOGY AND
DEPARTMENT OF LABOR AND ECONOMIC GROWTH

July 2007

E PLURIBUS UNUM
TUEBOR
SI QUÆRIS PENINSULAM AMŒNAM
CIRCUMSPICE

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

641-0591-06

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

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

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Operating System Controls for the Unemployment Insurance Agency's Mainframe Information Systems

Department of Information Technology and Department of Labor and Economic Growth

Report Number:
641-0591-06

Released:
July 2007

The mainframe information systems that support the Unemployment Insurance Agency's (UIA's) core business operations consist of the Employer Tax, Employee Benefit, and the Trust Fund Accounting Systems. These information systems operate on a third party service provider's mainframe computer. The Department of Information Technology (DIT) is responsible for security administration (including operating system configuration), system development, maintenance, and support of UIA's mainframe information systems.

Audit Objective:

To assess the effectiveness of DIT's efforts to configure the operating system software to ensure the confidentiality, integrity, and availability of UIA's mainframe information systems.

Audit Conclusion:

DIT's efforts to configure the operating system software to ensure the confidentiality, integrity, and availability of UIA's mainframe information systems were not effective. We noted four material conditions (Findings 1 through 4).

Material Conditions:

DIT did not fully restrict the use of privileged access rights to individuals based on their job function. Unauthorized use of privileged access rights could compromise the integrity of unemployment data and deny its availability to UIA. (Finding 1)

DIT did not properly secure unemployment data and operating system files. As a result, DIT could not ensure that confidential unemployment data and critical operating system files were protected from unauthorized access and use. (Finding 2)

DIT had not established effective security administration and monitoring over the third party service provider's mainframe computer system. As a result, DIT could not ensure that it would detect the unauthorized use of privileged access circumventing security and controls. (Finding 3)

DIT did not fully develop and maintain complete security requirements for the mainframe security system. Consequently, DIT did not properly configure the mainframe security system and effectively protect critical system resources. (Finding 4)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 4 findings and 4 corresponding recommendations. DIT and the Department of Labor and Economic Growth'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

July 24, 2007

Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan
and
Mr. Keith W. Cooley, Director
Department of Labor and Economic Growth
Ottawa Building
Lansing, Michigan

Dear Ms. Takai and Mr. Cooley:

This is our report on the performance audit of the Operating System Controls for the Unemployment Insurance Agency's Mainframe Information Systems, Department of Information Technology and Department of Labor and Economic Growth.

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

Our comment, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agencies 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

OPERATING SYSTEM CONTROLS FOR THE UNEMPLOYMENT INSURANCE AGENCY'S MAINFRAME INFORMATION SYSTEMS DEPARTMENT OF INFORMATION TECHNOLOGY AND DEPARTMENT OF LABOR AND ECONOMIC GROWTH

Page

INTRODUCTION

COMMENT, FINDINGS, RECOMMENDATIONS,
AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of Agencies

Department of Labor and Economic Growth (DLEG)

DLEG's Unemployment Insurance Agency (UIA) was created as the Michigan Employment Security Commission (MESC). MESC was created by the Michigan Employment Security Act of 1936 (Sections 421.1 - 421.75 of the *Michigan Compiled Laws*).

The primary responsibility of UIA is to collect unemployment taxes from employers and to pay unemployment benefits to eligible unemployed persons (claimants*). UIA administers the collection of tax payments from its central office in Detroit. In October 2004, UIA completed the closure of its Statewide network of 41 branch offices. Since closing the branch offices, UIA receives unemployment claims by telephone, via the Internet, and electronically from large employers on behalf of employees.

The mainframe information systems that support UIA's core business operations consist of the Employer Tax, Employee Benefit, and Trust Fund Accounting Systems. These information systems operate on a third party service provider's mainframe computer. UIA has outsourced the operational support for these systems to this third party service provider since 1995.

In fiscal year 2005-06, UIA expended $25.15 million on information technology, including $8.15 million to the third party service provider to operate the UIA systems.

In fiscal year 2005-06, UIA received approximately $1.6 billion in employer tax contributions for the Michigan Unemployment Compensation Fund and expended approximately $1.9 billion for unemployment benefits.

Department of Information Technology (DIT)

DIT was created in October 2001 by Executive Order No. 2001-3 to achieve a unified and more cost-effective approach for managing information technology among all executive branch agencies.

As part of DIT's creation, UIA's information technology personnel transferred to DIT's Bureau of Agency Services, which is now known as the DLEG/MDCR-Detroit Division*.

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

The DLEG/MDCR-Detroit Division has primary responsibility for security administration (including operating system* configuration), system development, maintenance, and support of UIA's mainframe information systems.

DIT's Office of Enterprise Security (OES) is responsible for identifying, managing, and mitigating security risks* and vulnerabilities* within State government's computing, communication, and technology resources. OES is also responsible for disaster recovery planning, risk management, security awareness and training, assistance to State agencies with their security issues, and enforcement oversight of State security policies and procedures intended to maintain suitable enterprise-wide security.

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

Audit Objective, Scope, and Methodology
and Agency Responses

Audit Objective

The audit objective for our performance audit* of the Operating System Controls for the Unemployment Insurance Agency's (UIA's) Mainframe Information Systems, Department of Information Technology (DIT) and Department of Labor and Economic Growth (DLEG), was to assess the effectiveness* of DIT's efforts to configure the operating system software to ensure the confidentiality*, integrity*, and availability* of UIA's mainframe information systems.

Audit Scope

Our audit scope was to examine the information processing and other records related to the third party service provider's operating system controls for the Unemployment Insurance Agency's mainframe information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances. Our audit procedures, performed from June 2006 through January 2007, included examination of DIT's mainframe security practices and records primarily for the period September 2005 through December 2006 and the mainframe operating system software's configuration as of June 8, 2006.

Audit Methodology

The criteria used in the audit included control objectives and audit guidelines outlined in the Control Objectives for Information and Related Technology* (CobiT), issued by the Information Systems Audit and Control Foundation (ISACF) in July 2000, as well as other information security best practices.

To accomplish our audit objective, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We reviewed the security practices defined for the third party service provider's mainframe computer system. We reviewed related audits of the third party service provider's mainframe processing operations. We researched and obtained an

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

understanding of the third party service provider's mainframe security system and the techniques and strategies to establish a secured processing environment. We used the results of our review to determine the extent of our detailed analysis and testing. We reviewed relevant DIT policies and procedures.

2. Detailed Analysis and Testing Phase

   We performed an assessment of DIT's efforts to ensure that the third party service provider's mainframe computer system is configured in accordance with agreed upon security requirements and best practices:

   a. We reviewed the security agreement between DIT and the third party service provider for completeness.

   b. We reviewed DIT's security administration and monitoring function over the third party service provider mainframe computer system.

   c. We compared DIT's security requirements and settings with the settings in the third party service provider's mainframe security system database.

   d. We evaluated access granted to UIA application and mainframe computer system resources.

3. Evaluation and Reporting Phase

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

We use a risk and opportunity based approach when selecting activities or programs to be audited. Accordingly, our audit efforts are focused on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. By design, our limited audit resources are used to identify where and how improvements can be made. Consequently, our performance audit reports are prepared on an exception basis.

Agency Responses

Our audit report contains 4 findings and 4 corresponding recommendations. DIT and DLEG'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 Department of Management and Budget Administrative Guide procedure 1280.02 require DIT and DLEG to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF EFFORTS TO CONFIGURE OPERATING SYSTEM SOFTWARE

Background: The mainframe security system, which is part of the operating system software, is designed to ensure the confidentiality, integrity, and availability of data on the third party service provider's mainframe computer system. This mainframe computer system supports the Unemployment Insurance Agency's (UIA's) information systems.

The mainframe security system provides a means of controlling who has access to the mainframe and to specific resources as well as what capabilities authorized users are granted. In addition, the security system provides a means of logging and reporting access activity. The security system should be configured to restrict authorized users to the specific resources, programs, and files needed to perform their jobs and to prevent others, such as hackers, from accessing the mainframe computer system.

COMMENT

Audit Objective: To assess the effectiveness of the Department of Information Technology's (DIT's) efforts to configure the operating system software to ensure the confidentiality, integrity, and availability of UIA's mainframe information systems.

Conclusion: DIT's efforts to configure the operating system software to ensure the confidentiality, integrity, and availability of the UIA's mainframe information systems were not effective. Our assessment disclosed four material conditions*. DIT did not fully restrict the use of privileged access* rights to individuals based on their job function (Finding 1). Also, DIT did not properly secure unemployment data and operating system files (Finding 2). In addition, DIT had not established effective security administration and monitoring over the third party service provider's mainframe computer system (Finding 3). Further, DIT did not fully develop and maintain complete security requirements for the mainframe security system (Finding 4).

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

FINDING

1. Privileged Access Rights

DIT did not fully restrict the use of privileged access rights to individuals based on their job function. Unauthorized use of privileged access rights could compromise the integrity of unemployment data and deny its availability to UIA.

Privileged access rights enable a user to configure the security system and to bypass application controls. ISO/IEC 17799:2005(E)*, *Code of Practice for Information Security Management*, states that the assignment and use of privileged access rights should be restricted to the minimum number of users necessary to perform privileged tasks. The assignment of privileged access should be controlled through a formal authorization process.

Our review of privileged access rights disclosed:

a. DIT did not restrict the security administration privilege to only security administrators. This privilege allows a user to manage user accounts and assign access to system resources. We determined that 15 of the 23 users with the security administration privilege did not require that level of access to perform their job responsibilities.

b. DIT did not restrict the operations support privilege to only those individuals responsible for system maintenance and operations. This privilege allows individuals to manage all mainframe disk and tape files. The operations support privilege also provides full access, such as read, copy, add, delete, and modify, to these same files. We determined that 17 of the 28 users with the operations support privilege did not require that level of access to perform their job responsibilities.

c. DIT did not prohibit all users from having multiple incompatible privileged access rights. We identified 20 users who were assigned multiple incompatible privileges, such as security administration and operations support. Users with multiple incompatible privileges could inadvertently or intentionally grant themselves or others the ability to copy, add, delete, and modify production programs or data without authorization.

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

Excessive assignment of privileged access was caused in part by DIT's insufficient understanding of the third party service provider's security system. The security system can be configured to restrict privileged access to specific resources. If used properly, DIT could tailor users' privileged access based on their job roles and responsibilities instead of granting privileged access rights to all resources on the mainframe computer system.

RECOMMENDATION

We recommend that DIT fully restrict the use of privileged access rights to individuals based on their job function.

AGENCY PRELIMINARY RESPONSE

DIT and the Department of Labor and Economic Growth (DLEG) agree and informed us that they have complied or will comply with the recommendation. DIT stated that it has restricted the use of privileged access rights to individuals based on their job function. In addition, DIT informed us that it has removed user accounts that do not require administrative access and removed user accounts that do not require operations access. Further, DIT informed us that DIT and its third party service provider established a project to review all aspects of mainframe system security. The project began in March 2007 with a scheduled completion date of December 31, 2009.

FINDING

2. Access to Unemployment Data and Operating System Files

DIT did not properly secure unemployment data and operating system files. As a result, DIT could not ensure that confidential unemployment data and critical operating system files were protected from unauthorized access and use.

Department of Management and Budget (DMB) Administrative Guide procedure 1350.40 requires the protection of data and operating system files from misuse by establishing controls that limit access to only authorized users who have a justified business need to access the files.

Our review of access to the third party service provider's mainframe computer system disclosed:

a. DIT did not restrict access to UIA unemployment system data files. The default system access allows all users to read and copy confidential employer and employee data, such as employee name, date of birth, social security number, and wage earnings without DIT or UIA's knowledge. Section 421.11(b)(1) of the *Michigan Compiled Laws* prohibits the distribution of this data to nongovernmental third parties. However, we noted no compensating controls that would prevent or detect a user from copying and selling this confidential data to an unauthorized third party.

b. DIT granted its development staff, operations support staff, and the third party service provider's staff unnecessary modify access to application data files. Modify access allows users to bypass established controls and make unauthorized changes to data. During our audit, DIT initiated action to address the security weaknesses identified in this finding.

c. DIT did not restrict access to operating system files. DIT granted its development staff, operations support staff, and the third party service provider's staff modify access to the operating system files. These files contain codes that define system operation and system security. Inappropriate access to operating system files could adversely affect the availability of UIA's mainframe information systems to users.

DMB Administrative Guide procedure 1350.40 provides high level guidance for granting access; however, there was no specific guidance for administering access to the third party service provider's mainframe computer system. Specific guidance is needed to address the unique requirements of the mainframe security system.

RECOMMENDATION

We recommend that DIT properly secure unemployment data and operating system files.

AGENCY PRELIMINARY RESPONSE

DIT and DLEG agree and informed us that they have complied or will comply with the recommendation. DIT stated that it will ensure that unemployment data and operating system files are properly secured. In addition, DIT informed us that, currently, only UIA, DIT, and the third party service provider staff have access to unemployment data and operating system files and that all staff have signed confidentiality statements. Further, DIT informed us that UIA, DIT, and the third party service provider adhere to the regulations in Section 11(b) of the Michigan Employment Security Act of 1936 and Title 20, Part 603 of the *Code of Federal Regulations* as they pertain to confidentiality. Further, DIT informed us that it has established a project that will review all aspects of mainframe system security with a scheduled completion date of December 31, 2009.

FINDING

3. Security Administration and Monitoring

DIT had not established effective security administration and monitoring over the third party service provider's mainframe computer system. As a result, DIT could not ensure that it would detect the unauthorized use of privileged access circumventing security and controls.

Our review of security administration and monitoring disclosed:

a. DIT did not ensure proper segregation of duties*. We noted:

(1) DIT assigned individuals primarily responsible for system development the incompatible duties of security administration. The security administration privilege allows administrators to manage user accounts and assign access to system resources. Without proper segregation of duties, there is a risk that these individuals could grant themselves or others inappropriate access.

(2) DIT did not assign the responsibility for security monitoring to an individual independent of the security administrator function. Consequently, DIT cannot ensure that the system administrator is performing only appropriate and authorized activities. The security monitoring and security administrator functions are incompatible and should be performed by independent individuals.

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

COBIT states that management should implement a division of roles and responsibilities to prevent a single individual from circumventing a critical control process. Also, management should ensure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained for the systems development, security administration, and security monitoring functions.

b. DIT did not define the security administrator duties and authority in the security administrators' position descriptions. Without defined duties and authority, DIT cannot evaluate security administrators or establish accountability for the security of the third party service provider's mainframe computer system.

COBIT states that management should ensure that position descriptions define both duties and authority.

c. DIT did not ensure that security administrators were adequately trained to effectively perform their job responsibilities. The security administrators' position descriptions did not identify the necessary knowledge, skills, and abilities needed to effectively perform security administrator duties. Without identifying the necessary knowledge, skills, and abilities, DIT management cannot ensure that security administrators receive appropriate training.

COBIT states that management should regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training, and/or experience.

d. DIT did not have a strategy to monitor the privileged access of system administrators. As a result, DIT cannot be assured that its monitoring practices will deter or detect misuse of privileged access.

ISO/IEC 17799:2005(E), *Code of Practice for Information Security Management*, states that system administrator activities should be logged and that those logs should be reviewed on a regular basis.

e. DIT had not developed and implemented complete security reports to monitor the privileged access of all user accounts. In addition, DIT had not developed and implemented policies and procedures for monitoring security on the mainframe computer system. Security reports should identify the critical security activities to be monitored, which user accounts will be monitored, and the process for using and maintaining security reports.

The federal Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual (FISCAM) states that security reporting should be implemented to selectively identify unauthorized, unusual, and sensitive access activity.

RECOMMENDATION

We recommend that DIT establish effective security administration and monitoring over the third party service provider's mainframe computer system.

AGENCY PRELIMINARY RESPONSE

DIT and DLEG agree and informed us that they have complied or will comply with the recommendation. DIT stated that it will establish effective security administration and monitoring over the third party service provider's mainframe computer system. In addition, DIT informed us that it has implemented procedures to review all security logs on a weekly basis. Further, DIT informed us that its Bureau of Agency Services security staff is working with human resources to ensure that user accounts are removed when employees leave UIA or DIT employment. DIT also informed us that its staff have been sent to security training to address the identified training concerns. In addition, DIT informed us that it has established a project that will review all aspects of mainframe system security with a scheduled completion date of December 31, 2009.

FINDING

4. Security Requirements

DIT did not fully develop and maintain complete security requirements for the mainframe security system. Consequently, DIT did not properly configure the mainframe security system and effectively protect critical system resources.

The State's contractual agreement with the third party service provider specifies that the State is responsible for security administration, such as establishing security policies, procedures, and practices. Although DIT and the third party service provider have made recent efforts to document the security requirements and settings of the mainframe security system, our review of DIT's efforts disclosed:

a. DIT did not clearly define its security administration role and responsibility in the security requirements. The agreement with the third party service provider stipulated that the State was responsible for security administration. However, our review of the security requirements and DIT's practices indicated that DIT had not assumed responsibility for security administration.

b. DIT had not established policy and procedures to administer the third party service provider's security system. As a result, significant aspects of the security requirements, such as user account and password management, assignment of privileged access, resource access management, and segregation of duties, were not well defined or were missing. Policy and procedures would provide direction to the security administrator and facilitate development of complete security requirements.

c. DIT did not sufficiently understand the functions of the mainframe security system or the strategy used to configure it. According to DIT, documentation that explained the State's initial strategy to configure the mainframe security system had been missing for several years. Maintaining complete and accurate documentation will help ensure that DIT security administrators understand the strategy used to configure the system.

d. DIT did not ensure the appropriateness of detailed security requirements and settings used to configure the third party service provider's security system. DIT had not explicitly agreed to most of the third party provider's recommended security settings that were placed into operation. Although DIT recently documented these security settings, DIT should evaluate the appropriateness of the settings, revise where necessary, and document its agreement with the third party service provider.

It is in DIT's best interest to ensure that security requirements are effective and documented. However, DIT will find it difficult to establish effective information security for its customers because, as we reported in our performance audit of the Enterprise Information Security Program, Department of Information Technology (084-0581-06), DIT has not yet fully implemented an enterprise-wide information security program. We reported that an information security program was needed to ensure that security roles and responsibilities are defined, security risks are identified, cost-effective policies and controls are developed, and methods to monitor and measure progress are established.

RECOMMENDATION

We recommend that DIT fully develop and maintain complete security requirements for the mainframe security system.

AGENCY PRELIMINARY RESPONSE

DIT and DLEG agree and informed us that they have complied or will comply with the recommendation. DIT stated that the design of the security in the mainframe systems was established over 13 years ago. In addition, DIT informed us that, while the mainframe's system software had been kept current, at the time of the audit, the State had not redefined/redeveloped the internal security structure. Further, DIT informed us that, proactively, UIA and DIT began planning a system rewrite project in 2005, during which new security policies and procedures were to be implemented as a part of the rewrite project. According to DIT, a delay in the start-up of the rewrite project had delayed implementation of the security changes. DIT also informed us that it will develop and maintain complete security requirements for the mainframe security system. In addition, DIT informed us that it has established a project that will review all aspects of mainframe system security with a scheduled completion date of December 31, 2009.

GLOSSARY

Glossary of Acronyms and Terms

availability

Timely and reliable access to data and information systems.

claimant

A jobless worker who files a claim for unemployment benefits.

confidentiality

Protection of data from unauthorized viewing.

Control Objectives for Information and Related Technology (COBIT)

A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.

DIT

Department of Information Technology.

DLEG

Department of Labor and Economic Growth.

DLEG/MDCR-Detroit Division

The organizational group within DIT's Bureau of Agency Services that is located in Detroit and is responsible for information technology support of DLEG and the Michigan Department of Civil Rights.

DMB

Department of Management and Budget.

effectiveness

Program success in achieving mission and goals.

integrity

Protection of data from unauthorized modification.

ISO/IEC 17799:2005 (E)

A detailed security standard published by the International Standards Organization (ISO). The standard is organized into 10 major sections.

material condition

A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.

MESC
Michigan Employment Security Commission.

OES
Office of Enterprise Security.

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

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

privileged 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.

reportable condition
A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.

security risk
The probability that a particular security threat will exploit a system vulnerability.

segregation of duties
Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.

UIA Unemployment Insurance Agency.

vulnerabilities Weaknesses in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL