

Office of the Auditor General
Performance Audit Report

Office of Collections
Department of Treasury

July 2015

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

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



OAG

Office of the Auditor General

Report Summary

Performance Audit

Office of Collections

Department of Treasury

Report Number:
271-0153-14

Released:
July 2015

The Office of Collections is the centralized collection agency for delinquent taxes administered by the Department of Treasury and delinquent non-tax debts owed to various State agencies. The Office performed collection activities on 1.4 million delinquent accounts in fiscal year 2014 and collected an average of \$431 million each year during fiscal years 2012 through 2014. The Office contracts with a collection agency for collection services for which it pays a commission based on the amount of delinquent debt received by the State as a result of the collection efforts. The Office and contractor utilize the Michigan Accounts Receivable Collection System (MARCS) to assist in the collection process.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness and efficiency of the Office's efforts to collect referred delinquent debt.			Moderately effective and efficient
Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
The Department of Treasury did not ensure that the automated system for managing sales, use, and withholding (SUW) tax returns and payment information was programmed to accurately identify delinquent assessment balances. Inaccurate programming caused the Office to issue 76,000 SUW tax assessments with an incorrect balance and incur at least \$142,000 in avoidable processing costs (Finding #1).	X		Agrees
The Office did not timely pursue delinquent debts, which could result in State revenue being delayed or uncollected (Finding #2).	X		Agrees
The Office did not consistently monitor the contractor to ensure that it performed the services specified in the contract. Monitoring would help ensure the completion of required activities to maximize the collection of delinquent debts and the accuracy of billings for services provided (Finding #3).		X	Agrees
The Office did not comply with legislative reporting requirements related to collection activities performed by the contractor. Failure to report collections data could prevent the Legislature from having the information it needs to make decisions about the value and effectiveness of the Office (Finding #4).		X	Agrees

Findings Related to This Audit Objective (Continued)	Material Condition	Reportable Condition	Agency Preliminary Response
The Office did not consistently follow Department procedures for supervisory review of delinquent tax accounts. As a result, the Office could not ensure that delinquent tax accounts were processed timely and appropriately to maximize revenue for the State (<u>Finding #5</u>).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness and efficiency of the Office's efforts to identify businesses operating in the State of Michigan without a current SUW tax license.			Moderately effective and efficient
Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
The Office did not provide sufficient program management and oversight of the Unregistered Business Program (UBP) to ensure the identification and registration of businesses owing delinquent taxes (<u>Finding #6</u>).	X		Partially Agrees
The Office did not fully implement effective security and access controls over the UBP database to help prevent or detect inappropriate access to and modification of taxpayer and business data (<u>Finding #7</u>).		X	Agrees

Audit Objective			Conclusion
Objective #3: To assess the effectiveness of the Office's efforts to ensure appropriate security and access controls over MARCS.			Moderately effective
Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
The Office did not fully establish and implement effective security configurations for the MARCS application and database to help prevent or detect inappropriate modification of MARCS data (<u>Finding #8</u>).	X		Agrees
The Office did not fully implement effective user access controls over the MARCS application and database to help prevent or detect inappropriate access to delinquent account data (<u>Finding #9</u>).		X	Agrees

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>

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

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General



OAG

Office of the Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • <http://audgen.michigan.gov>

Doug A. Ringler, CPA, CIA
Auditor General

July 20, 2015

Mr. Nick Khouri
State Treasurer
Richard H. Austin Building
Lansing, Michigan

Dear Mr. Khouri:

I am pleased to provide this performance audit report on the Office of Collections, Department of Treasury.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above 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,

Doug Ringler
Auditor General

TABLE OF CONTENTS

OFFICE OF COLLECTIONS

	<u>Page</u>
Report Summary	1
Report Letter	3
Audit Objectives, Conclusions, Findings, and Observations	
Collecting Referred Delinquent Debt	8
1. System programming should be improved to accurately identify delinquent SUW assessment balances.	10
2. More timely pursuit of delinquent debts is necessary.	11
3. Consistent contractor monitoring could help maximize the collection of delinquent debts.	12
4. Accurate reporting would improve the quality of information provided to the Legislature.	14
5. Department procedures for supervisory review of accounts should be followed.	15
Identifying Unregistered Businesses	17
6. Improved UBP management and oversight is needed to identify businesses owing taxes.	18
7. Improvements are needed to UBP database security and access controls.	21
Ensuring Appropriate MARCS Security and Access Controls	23
8. More comprehensive security configurations are vital to protecting the MARCS application and database.	24
9. Improvements are needed to MARCS user access controls.	26
Agency Description	29
Audit Scope, Methodology, and Other Information	30
Glossary of Abbreviations and Terms	33

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

COLLECTING REFERRED DELINQUENT DEBT

BACKGROUND

The Office of Collections is the centralized collection agency for delinquent taxes administered by the Department of Treasury and delinquent non-tax debts owed to State agencies. The Office uses various techniques to collect debts owed to the State. These techniques include letters, phone calls, installment agreements, State income tax refund offsets, wage and bank levies, tax warrants (property seizure and sale), and tax liens.

The following table presents the number of delinquent accounts, the associated amount of unpaid debt, and the amount collected on the debt during fiscal years 2012 through 2014:

Fiscal Year	Number of Delinquent Accounts (in millions)	Estimated Amount of Debt (in billions)	Total Collected (in millions)
2012	1.3	\$3.8	\$449.7
2013	1.3	\$3.5	\$452.3
2014	1.4	\$3.7	\$391.4

The Office contracts with a collection agency to provide collection services and administer the Michigan Accounts Receivable Collection System (MARCS). The following table identifies the amount paid to the contractor for collection services and the amount collected by the contractor during fiscal years 2012 through 2014:

Fiscal Year	Paid to Contractor (in millions)	Collected by Contractor (in millions)
2012	\$28.8	\$197.8
2013	\$30.1	\$206.4
2014	\$28.9	\$189.5

AUDIT OBJECTIVE

To assess the effectiveness* and efficiency* of the Office's efforts to collect referred delinquent debt.

CONCLUSION

Moderately effective and efficient.

FACTORS IMPACTING CONCLUSION

- The Office collected over \$1 billion of delinquent debt during fiscal years 2012 through 2014.
- The Office established and implemented some procedures for the collection of referred delinquent debt.

* See glossary at end of report for definition.

- Two material conditions* (Findings #1 and #2) related to inaccurate identification of delinquent assessment balances and the timely pursuit of delinquent debts.
- Three reportable conditions* (Findings #3 through #5) related to contractor monitoring, inaccurate reporting to the Legislature, and enforcement of supervisory review procedures.

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

FINDING #1

System programming should be improved to accurately identify delinquent SUW assessment balances.

Inaccurate programming resulted in at least \$142,000 in avoidable processing costs.

The Department of Treasury did not ensure that the automated system for managing SUW tax returns and payment information was programmed to accurately identify delinquent assessment balances. Inaccurate programming caused the Office to issue 76,000 SUW tax assessments with an incorrect balance and incur at least \$142,000 in avoidable processing costs. Also, as a result, some businesses and individuals unnecessarily paid a tax assessment because of the erroneous notification that they owed delinquent taxes.

In March 2014, the Department implemented an automated system for managing SUW tax returns and payment information. The system was not accurately programmed to reduce an assessment balance when an electronic payment was received from a taxpayer. In addition, the system could not accept paper registration forms, causing several months' delay in processing taxpayer registration information. These issues resulted in assessments being inappropriately referred to the Office for collection processing. Processing costs included postage for mailing delinquent notification letters, employee costs for processing the accounts, and contractor commissions for following up on the accounts.

If the programming errors are not corrected by October 2015, the Office estimated that an additional 79,000 assessments will be inappropriately referred for collection processing. These assessments would result in an additional \$112,000 in mailing costs plus additional employee costs to follow up the assessments. The Office informed us that, as of April 2015, it had placed the assessments in question on hold and would resolve the errors by July 2015.

RECOMMENDATION

We recommend that the Department ensure that the automated system for managing SUW tax returns and payment information is programmed to accurately identify delinquent assessment balances.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department agrees with the recommendation. Assessments with potentially incorrect balances were placed on hold in April 2015. Subsequent actions have been taken to address the issue with significant progress made. The Department expects to have all affected assessments corrected to the proper balance by the end of July 2015. Monies applied as a result of this issue will be refunded to the taxpayer as appropriate.

FINDING #2

More timely pursuit of delinquent debts is necessary.

The Office did not timely pursue delinquent debts, which could result in State revenue being delayed or not collected.

The Office refers delinquent business tax accounts to its Field Operations section. The Field Operations section consists of revenue officers and enforcement officers who collect delinquent business tax debt.

From a population of 903 accounts assigned to enforcement officers, we sampled 30 accounts to review for revenue officer activity and 30 accounts to review for enforcement officer activity. Our review disclosed:

- a. Revenue officers did not meet required deadlines for performing their job responsibilities. We noted that 21 (70%) of 30 accounts reviewed by the revenue officers were not processed in accordance with Department policy.
- b. Policies and procedures were not developed and implemented for enforcement officers, resulting in inconsistent practices being followed. Without defined policies and procedures, enforcement officers may not process accounts as effectively and efficiently as possible.

Section 205.28(1)(f) of the *Michigan Compiled Laws* (Act 122, P.A. 1941, as amended, known as the Revenue Act) provides that any information that would enable a person to ascertain the audit selection or processing criteria of delinquent tax processing will remain confidential. Therefore, we summarized our testing results for presentation in this finding and provided the detailed results to Department management.

RECOMMENDATION

We recommend that the Office timely pursue delinquent debts.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation. The Office has completed the update and formalization of procedures as of June 2015. Current, formal procedures in conjunction with training and management oversight will assist with ensuring timely collection of delinquent debts.

Revenue officers Statewide will be trained on the new procedures in July 2015 with full implementation effective August 1, 2015. Procedures for the enforcement officers are in the final review process, with a target date of September 1, 2015 for full implementation.

FINDING #3

Consistent contractor monitoring could help maximize the collection of delinquent debts.

The Office did not consistently monitor the contractor to ensure that it performed the services specified in the contract. Monitoring would help ensure the completion of required activities to maximize the collection of delinquent debts and the accuracy of billings for services provided.

Our review disclosed that the Office did not:

- a. Ensure that the contractor followed performance metrics related to delinquent account processing.

These metrics included:

- Answering 85% of phone calls within 20 seconds.
- Achieving a call abandonment rate of less than 3% after the introductory recording.
- Limiting account holders' time on hold during phone calls.
- Resolving 30% of the accounts on the first phone call.
- Achieving a 90% accuracy rate for following the proper collections process.

Management indicated that the contractor routinely did not meet these performance metrics and that the Office did not put corrective action in place.

- b. Ensure that the contractor actively processed cases.

We reviewed 10 cases assigned to the contractor and noted that 6 (60%) of the 10 cases had no collection activity for 9 or more months. Untimely collection activity results in delayed revenue for the State.

- c. Reconcile the amount of commissions billed by the contractor with the amount of debts collected by the contractor for driver responsibility fees (DRFs) in fiscal years 2012 through 2014. In addition, the Office did not consistently reconcile the amount billed by the contractor with the amount of other debts collected. The following table summarizes the number of

reconciliations performed by the Office for DRFs and other debts by fiscal year:

Fiscal Year	Reconciliations of Commissions With Collections	
	For DRF	For Other Debts
2012	0 (0%) of 12	4 (33%) of 12
2013	0 (0%) of 12	3 (25%) of 12
2014	0 (0%) of 12	2 (17%) of 12

RECOMMENDATION

We recommend that the Office consistently monitor the contractor to ensure that it performs the services specified in the contract.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation and either has resolved the identified issues or is conducting further research to determine how to resolve the identified issues:

- a. *The Office is evaluating processes to ensure consistent monitoring of the contractor's performance metrics related to delinquent account processing by the end of fiscal year 2015. Further, contract compliance inspectors will be attending training by the end of August 2015 that will include training regarding effectively monitoring contracts.*
- b. *The Office is evaluating procedures to ensure that the contractor actively processes cases by the end of fiscal year 2015.*
- c. *The Office has implemented reconciliation processes for the amount of commissions billed by the contractor with the amount of debts collected by the contractor for debts other than DRFs as of May 2015. In addition, the Office will evaluate and implement a reconciliation process for DRFs by the end of fiscal year 2015.*

FINDING #4

Accurate reporting would improve the quality of information provided to the Legislature.

The Office did not comply with legislative reporting requirements related to collection activities performed by the contractor. Failure to fully report collections data could prevent the Legislature from having the information it needs to make decisions about the value and effectiveness of the Office.

According to Section 903(3), Part 2, Act 59, P.A. 2013, the Department of Treasury shall submit an annual report to the State Budget Director and the Senate and House of Representatives standing committees stating the name of the contractor, the amount collected by the contractor, the cost of collections, and other pertinent information related to determining whether the contract should be continued.

The Office did not include all debts collected by the contractor in its annual legislative reports. When DRFs were added to MARCS, the Office did not modify the reporting query to include these collections in the legislative report. For fiscal years 2012 through 2014, the following collections were not reported to the Legislature:

<u>Fiscal Year</u>	<u>Collections Not Reported (in millions)</u>
2012	\$39.2
2013	22.0
2014	<u>28.0</u>
Total	<u><u>\$89.2</u></u>

RECOMMENDATION

We recommend that the Office comply with legislative reporting requirements related to collection activities performed by the contractor.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation and has modified the reporting query to ensure that all collection activity performed by the contractor is included in the annual legislative report.

FINDING #5

Department procedures for supervisory review of accounts should be followed.

The Office did not consistently follow Department procedures for supervisory review of delinquent tax accounts. As a result, the Office could not ensure that delinquent tax accounts were timely and appropriately processed to maximize revenue for the State. Knowledge of and compliance with Department procedures would provide uniformity and improve the credibility of the collections process.

Department procedure PC-49043 requires that the Field Operations section's entire caseload must be reviewed over the course of one year. It also requires that supervisors must review 10% of each employee's cases monthly, and the next level supervisor must review 15% of the cases reviewed by each supervisor. Further, the procedure requires the assistant administrator to review one or more accounts from each field office. In addition, the Office developed a training presentation in November 2011 that identified weekly goals for case reviews. The Office also developed a job aid in January 2014 that provided additional case review guidance based on the amount of time a case was delinquent.

Our review disclosed:

- a. The Office did not ensure that supervisor, next level supervisor, and assistant administrator reviews were completed as required by Department procedure PC-49043.
- b. The Office did not meet its goal of supervisors completing 175 account reviews weekly as identified in the training presentation. As of July 2014, the Office reviewed 9,045 (51%) of its goal of 17,850 cases.
- c. The Office did not meet its goal of reviewing cases that had been delinquent for over 9 months. As of July 2014, the Office reviewed 371 (22%) of the 1,695 cases that had been assigned for over 9 months.

Management indicated that procedures for supervisory review were unreasonable given the current level of staffing and would be modified to provide a uniform review process.

RECOMMENDATION

We recommend that the Office consistently follow Department procedures for supervisory review of delinquent tax accounts.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the importance of following Department procedures, including supervisory review of delinquent tax accounts.

The Office has evaluated procedure PC-49043 and has updated the procedure to reflect best practices as of June 2015. Supervisors Statewide will be trained on the new procedure in July 2015, with full implementation effective August 1, 2015. Current, formal procedures, along with training and management oversight, will assist in ensuring that the Office consistently follows Department procedures for supervisory review of delinquent tax accounts.

IDENTIFYING UNREGISTERED BUSINESSES

BACKGROUND

Act 122, P.A. 1941, as amended, provides the Department with the authority to collect taxes and obtain information on which to base tax assessments. During 2010, the Office initiated a pilot project to identify active businesses that had not registered for an SUW tax license and had not filed SUW tax returns. Based on the results of the pilot project, the Office determined that 15% of the businesses were either not registered or not in compliance with filing requirements. The Office projected that an additional \$11 million in revenue could be collected by the implementation of the Unregistered Business Program (UBP). In spring 2010, the Office established treasury officer* positions and the UBP to identify businesses operating in the State of Michigan that had not registered for an SUW tax license.

AUDIT OBJECTIVE

To assess the effectiveness and efficiency of the Office's efforts to identify businesses operating in the State of Michigan without a current SUW tax license.

CONCLUSION

Moderately effective and efficient.

FACTORS IMPACTING CONCLUSION

- In 2010, the Office created the UBP to identify businesses operating in the State of Michigan that did not have an SUW tax license.
- Centralized database was maintained to gather program information.
- Material condition (Finding #6) related to UBP management and oversight and reportable condition (Finding #7) related to security* and access controls*.

* See glossary at end of report for definition.

FINDING #6

Improved UBP management and oversight is needed to identify businesses owing taxes.

The Office did not provide sufficient program management and oversight of the UBP to ensure the identification and registration of businesses owing delinquent taxes.

The UBP is administered by treasury officers who are assigned a specific geographical location in the State. Treasury officers are responsible for determining whether businesses are in compliance with Michigan tax laws.

Our review disclosed:

- a. The Office did not establish goals* and objectives* for the UBP. The mission* of the UBP is to identify businesses that incur tax liabilities but are not filing tax returns or are not registered for an SUW tax license with the Department. Measurable goals and objectives would provide the Office with a means for measuring its progress toward the attainment of the overall mission.
- b. The Office did not fully develop and implement policies and procedures for the UBP. Policies and procedures will assist the Office in consistently identifying unregistered businesses, tracking field visit data, and effectively monitoring and managing field activity.
- c. The Office did not have a process to monitor and manage field activity.

Treasury officers were allowed to plan their own field visits. As of July 2014, cities and towns representing 457 (39%) of the 1,169 Michigan zip codes had not been visited by a treasury officer. Therefore, the UBP did not identify delinquent businesses in these 457 zip code areas.

- d. The Office did not ensure that the information gathered during field visits was accurate and complete.

Our review of the UBP database disclosed missing or inaccurate data in the following fields: field officer name, business status, and zip code. Without complete and accurate data, the Office is unable to accurately evaluate staff performance, determine whether follow-up is needed on a business, and identify which areas of the State have been visited.

- e. The Office did not track UBP expenditures. Tracking expenditures such as management and staff wages as well as associated travel costs will allow management to effectively assess the value of the program.

* See glossary at end of report for definition.

RECOMMENDATION

We recommend that the Office provide sufficient program management and oversight of the UBP to ensure the identification and registration of businesses owing delinquent taxes.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department partially agrees with the recommendation:

- a. *The Office disagrees with part a. of the finding. The mission of the UBP is to identify businesses operating in the State that did not have an SUW tax license. The goals and objectives of the UBP are to generate revenue and improve compliance with tax laws. The Office has established measurable goals and objectives, including tracking revenues collected, since UBP inception.*
- b. *The Office agrees that policies and procedures for the UBP were not fully developed and implemented. The Office is in the process of updating and formalizing policies and procedures and will be completed by the end of fiscal year 2015. Current, formal procedures, along with training and management oversight, will assist the Office in consistently identifying unregistered businesses, tracking field visit data, and effectively monitoring and managing field activity.*
- c. *The Office partially agrees that it did not have a process to monitor and manage field activity. Treasury officers work independently, with appropriate management oversight, to plan field visits. Cities and towns representing 61% of the 1,169 Michigan zip codes had been visited by a treasury officer, concentrating on the most populated areas and areas where unregistered business activity was suspected. The treasury officers are not wholly dedicated to the UBP; treasury officers are also involved in the collection of complex tax cases that may require a significant amount of time, thus reducing hours spent on the UBP. The Office is reviewing current processes to monitor and manage UBP field activity and will be completed by the end of fiscal year 2015. Current, formal processes, along with training and management oversight, will assist in monitoring and managing UBP field activity and ensuring consistency across the State.*
- d. *The Office agrees that information in the UBP database was not always accurate or complete. The Office is in the process of updating and formalizing policies and procedures and will be completed by the end of fiscal year 2015. Current, formal procedures, along with training and management oversight, will assist in ensuring that accurate and complete information is gathered during field visits and appropriately documented. Further, by the end of fiscal year 2015, the Office will research and explore the potential*

for a cost-effective, more efficient replacement to the UBP database currently being used.

- e. The Office disagrees with part e. of the finding. The Office does track expenditures, such as management and staff wages as well as associated travel costs. The treasury officers and management staff are not wholly dedicated to the UBP; treasury officers are also involved in the collection of complex tax cases. The Office will review methodologies for determining UBP program-related expenditures.*

FINDING #7

Improvements are needed to UBP database security and access controls.

The Office did not fully implement effective security and access controls over the UBP database to help prevent or detect inappropriate access to and modification of taxpayer and business 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.

Our review of selected security and access controls disclosed:

- a. Vulnerable security configurations on the UBP database.

Because of the confidentiality of database configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to Department management.

- b. Ineffective processes for granting database access rights based on a user's job responsibilities.

Specifically:

- (1) The Office did not grant user access based on the principle of least privilege*. As a result, all users who had access to the database had the ability to read, insert, and update all of the data within the database.
- (2) The Office did not have effective processes for documenting the authorization of user access rights. As a result, the Office could not ensure that only appropriate individuals had access to the database and that their level of access was appropriate.

User access was not limited to the principle of least privilege.

RECOMMENDATION

We recommend that the Office fully implement effective security and access controls over the UBP database.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation. The Office of the Auditor General (OAG) did not perform tests for inappropriate activity and, therefore, did not identify any specific

* See glossary at end of report for definition.

inappropriate activity as a result of the security and access control weaknesses. Additionally, the Office has not identified any inappropriate activity.

Presently, the ability to change information in the Access database is limited to users who can sign into the State of Michigan network and restricted to only users who have access to the network folder containing the Access database. In addition, this database is not used to post financial transactions and is only used as a reporting mechanism.

By the end of fiscal year 2015:

- a. The Office will add additional user controls to the Access database to further prevent unauthorized access or changes.*
- b. The Office will research the capability of the Access database and implement the maximum encryption and security controls available.*
- c. The Office will research and explore the potential for a cost-effective, more efficient replacement for the Access database currently being used.*

ENSURING APPROPRIATE MARCS SECURITY AND ACCESS CONTROLS

BACKGROUND

Security and access controls limit or detect inappropriate access, which is important to ensure the availability*, confidentiality, and integrity of data. Poor application and database management system* security not only compromises the system but may also compromise the operating system* and other trusted network systems.

MARCS consists of an application and a database that are used to support the Office's collection of delinquent debts. The Office is responsible for security and access controls over MARCS because it is the owner of all data held within MARCS.

AUDIT OBJECTIVE

To assess the effectiveness of the Office's efforts to ensure appropriate security and access controls over MARCS.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Establishment and implementation of some security configurations and access controls in accordance with State policy and best practices.
- Material condition (Finding #8) related to application and database security configurations and reportable condition (Finding #9) related to user access controls.

* See glossary at end of report for definition.

FINDING #8

More comprehensive security configurations are vital to protecting the MARCS application and database.

The Office did not fully establish and implement effective security configurations for the MARCS application and database to help prevent or detect inappropriate modification of MARCS 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.

Our review of selected security configurations disclosed:

- a. Vulnerable security configurations on the MARCS application and database.

Because of the confidentiality of database configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to Department management.

- b. Lack of monitoring of security settings on the databases managed by the contractor.

As a result, the contractor did not implement Department and Department of Technology, Management, and Budget (DTMB) policies regarding database security. Securing databases is essential for ensuring the integrity and confidentiality of the Office's data.

RECOMMENDATION

We recommend that the Office fully establish and implement effective security configurations for the MARCS application and database.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation and either has resolved the identified issues or is conducting further research to determine how to resolve the identified issues. The OAG did not perform tests for inappropriate activity and, therefore, did not identify any inappropriate activity as a result of security and

access control weaknesses within MARCS. Additionally, the Office has not identified any inappropriate activity.

- a. The Office has resolved certain vulnerable security configurations as of April 2015 and, by the end of fiscal year 2015, will conduct further research to determine how to resolve the remaining issues in the MARCS application and database without impacting system availability and efficiency.*
- b. By the end of fiscal year 2015, the Office will evaluate its processes to determine how to effectively implement procedures to monitor security settings on the databases managed by the contractor.*

FINDING #9

Improvements are needed to MARCS user access controls.

The Office did not fully implement effective user access controls over the MARCS application and database to help prevent or detect inappropriate access to delinquent account data.

DTMB Administrative Guide policy 1335, Information Technology Access Control, requires the establishment of a process to control and document the allocation of user access rights based on current job responsibilities and to allow access to be managed, controlled, and periodically reviewed to ensure that user access is based on the principle of least privilege. In addition, DTMB Technical Standard 1335.00.03 requires system owners to identify authorized users and specify access privileges, deactivate accounts of terminated or transferred users, and review accounts every 120 days.

Our review of selected MARCS user access controls disclosed:

- a. Ineffective processes for promptly disabling user accounts that no longer required access to MARCS.

We identified 163 active MARCS user accounts that had not logged in to the application in over 120 days. Of these 163 accounts, 128 had not been used in over one year. As a result, accounts that no longer require access could be used to gain inappropriate access to confidential information.

- b. Ineffective processes for granting access to the MARCS application and database based on a user's job responsibilities.

We noted:

- (1) The Office did not grant user access to the database based on the principle of least privilege. As a result, all accounts with access to the database had the ability to inappropriately perform high-risk activities, such as modifying tables, creating tables, or viewing sensitive data within the database.
- (2) Compensating controls did not exist to effectively identify the actions taken by users with access to shared privileged accounts* in the database.
- (3) Documentation of the authorization of user access rights did not ensure that only appropriate individuals had access to the database and that their level of access was appropriate.

128 active MARCS accounts had not been used in over one year.

User access was not limited to the principle of least privilege.

* See glossary at end of report for definition.

Developers of the MARCS database were responsible for designing, testing, and implementing program changes.

We judgmentally selected 25 users with access to MARCS data and noted that 10 (40%) of the 25 users did not have access forms.

- c. Inappropriate segregation of duties* over change control processes.

Developers of the MARCS database were responsible for designing, testing, and implementing program changes. Department policy ET-03173 states that separation of duties is a key internal control* that prevents a single individual from controlling two or more phases of a specific operational or technical process to reduce the risk of erroneous or fraudulent transaction processing, implementation of improper program changes, and/or destruction of computer resources.

- d. A lack of user access reviews for the application and database.

Periodic reviews ensure that privileges granted to each user are appropriate for the user's job responsibilities.

- e. MARCS database vulnerabilities existed because of ineffective or incomplete user access controls.

Because of the confidentiality of database controls, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to Department management.

RECOMMENDATION

We recommend that the Office fully implement effective user access controls over the MARCS application and database.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Office agrees with the recommendation and either has resolved or is working on resolving all identified issues, as well as implementing additional compensating and system controls over MARCS access. The OAG did not perform tests for inappropriate activity and, therefore, did not identify any inappropriate activity as a result of security and access control weaknesses within MARCS. Additionally, the Office has not identified any inappropriate activity.

- a. *The Office will evaluate and modify MARCS programming to ensure that inactive users are disabled promptly by the end of fiscal year 2015.*

* See glossary at end of report for definition.

- b. (1) *The Office has reduced developer access to the database as of April 2015. The Office will continue to research how to further reduce access while not degrading support for business processes by the end of fiscal year 2015.*
- (2) *The Office has implemented compensating controls for shared accounts as of April 2015.*
- (3) *The Office has modified processes to ensure that users are granted the proper level of access as of April 2015. The Office will implement a security framework and an annual review of user access by the end of fiscal year 2015.*
- c. *As of April 2015, the Office has limited MARCS access to one developer. The Office will continue to review current processes to determine how to best implement a further segregation of duties relating to the MARCS change control process by the end of fiscal year 2015.*
- d. *The Office is implementing an annual review of user access by the end of fiscal year 2015. This includes implementing a security framework and an annual review of user access by fiscal year end.*
- e. *The Office has resolved certain identified issues as of April 2015, and by the end of fiscal year 2015, will conduct further research to determine how to resolve the remaining issues without impacting system availability and efficiency.*

AGENCY DESCRIPTION

Under the authority of Act 122, P.A. 1941, as amended, the Office of Collections, Department of Treasury, is responsible for pursuing the collection of delinquent tax liabilities identified by the other divisions within the Department.

The Office is the centralized collection agency for delinquent assessed taxes administered by the Department and delinquent non-tax debts owed to State agencies. The Department tax divisions refer delinquent tax debts to the Office for billing and collection. In addition, other State agencies refer non-tax accounts for collection. The Office consists of five major functions:

- Maintenance of an accounts receivable database.
- Bankruptcy claims.
- Centralized collection and tax clearance.
- Field operations.
- Oversight of a private collection agency contract.

The Office uses various techniques to collect amounts due the State. These techniques include letters, phone calls, installment agreements, State income tax refund offsets, wage and bank levies, tax warrants (property seizure and sale), and tax liens.

The Office also contracts with a private collection agency to provide collection services and to administer MARCS. The collection agency receives a commission based on the amount of delinquent debt received by the State as a result of the collection efforts.

Act 122, P.A. 1941, as amended, provides the Department with the authority to collect taxes and obtain information on which to base tax assessments. During 2010, the Office initiated a pilot project to identify active businesses that had not registered for an SUW tax license and were not in compliance with the filing of tax returns. The Office determined that approximately 15% of businesses were either not registered or not in compliance with filing requirements. As a result, the UBP was established within the Office to identify unregistered businesses operating in the State of Michigan.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records of the Office of Collections. 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 of the Office of Collections did not include a review of controls within the State Treasury Accounts Receivable System (STAR), which supports the Office's delinquent tax processing. We issued a performance audit report of STAR in March 2014.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2011 through September 30, 2014.

METHODOLOGY

We conducted a preliminary survey of the Office to formulate a basis for defining our audit objectives and scope. During our preliminary survey, we:

- Conducted interviews to obtain an understanding of the Office's operations, activities, and internal control.
- Reviewed applicable sections of the *Michigan Compiled Laws*.
- Obtained an understanding of collection policies, standards, and procedures.
- Analyzed available collection data and statistics.

OBJECTIVE #1

To assess the effectiveness and efficiency of the Office's efforts to collect referred delinquent debt.

To accomplish our first objective, we:

- Sampled and reviewed disclosure of interest forms for Office staff involved in delinquent account processing.

* See glossary at end of report for definition.

- Randomly selected delinquent tax and non-tax accounts to determine if the Office:
 - Processed accounts according to Department and Office policies.
 - Processed accounts in a timely manner.
 - Had appropriate supervisory review throughout processing.
 - Reviewed the Office's monitoring of the contractor that provides collection services and administers MARCS.
 - Verified the accuracy of annual legislative reports prepared by the Office.
 - Verified that Office staff were processing only delinquent SUW tax accounts.

OBJECTIVE #2

To assess the effectiveness and efficiency of the Office's efforts to identify businesses operating in the State of Michigan without a current SUW tax license.

To accomplish our second objective, we:

- Interviewed the Field Operations section administrator to obtain an understanding of the UBP and its internal control.
- Reviewed disclosure of interest forms for Office staff involved in identifying unregistered businesses.
- Reviewed the Office's methodology for identifying unregistered business.
- Obtained and analyzed the UBP database.
- Observed Office staff performing field visits to identify unregistered businesses.
- Interviewed the database administrator* to obtain an understanding of security and access controls implemented over the UBP database.

OBJECTIVE #3

To assess the effectiveness of the Office's efforts to ensure appropriate security and access controls over MARCS.

* See glossary at end of report for definition.

To accomplish our third objective, we:

- Interviewed the MARCS support team to obtain an understanding of security and access controls.
- Tested the configuration of the MARCS application and database against Department policy, DTMB policy, and industry best practices.
- Tested the appropriateness of user access to the application and database.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions and reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

AGENCY RESPONSES

Our audit report contains 9 findings and 9 corresponding recommendations. The Department of Treasury's preliminary response indicates that it agrees with 8 recommendations and partially agrees with 1 recommendation.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of 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 an audited agency to develop a plan to comply with the 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.

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
assessment	An amount determined as payable to the Department of Treasury when a taxpayer fails or refuses to make a return or payment or when the Department of Treasury believes that a taxpayer has not provided sufficient information to determine the amount of tax due.
availability	Timely and reliable access to data and information systems.
confidentiality	Protection of data from unauthorized disclosure.
database administrator	The person 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.
database management system	Software that uses a standard method of cataloging, retrieving, and running queries on data. The database management system manages incoming data, organizes the data, and provides ways for the data to be modified or extracted by users or other programs.
DRF	driver responsibility fee.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
efficiency	Achieving the most outputs and the most outcomes practical with the minimum amount of resources.
goal	An intended outcome of a program or an entity to accomplish its mission.
integrity	Accuracy, completeness, and timeliness of data in an information system.

internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.
ISO/IEC 27002:2005	A security standard published by the International Organization for Standardization (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.
MARCS	Michigan Accounts Receivable Collection System.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and 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 entity or the reason that the program or the entity was established.
OAG	Office of the Auditor General.
objective	Specific outcome(s) that a program or an entity seeks to achieve its goals.
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.

principle of least privilege	The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
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 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.
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.
STAR	State Treasury Accounts Receivable System.
SUW	sales, use, and withholding.
treasury officer	An Office of Collections employee responsible for determining whether businesses are in compliance with Michigan tax laws.
UBP	Unregistered Business Program.

