Office of the Auditor General
Performance Audit Report

Office of Privacy and Security

Department of Treasury

September 2017

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

271-0160-16

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 Privacy and Security (OPS)

Department of Treasury (Treasury)

Report Number:
271-0160-16

Released:
September 2017

OPS's mission is to protect the privacy, confidentiality, and integrity of information collected, used, and retained by Treasury. OPS is responsible for administering the disclosure provisions of Section 205.28(1)(f) of the *Michigan Compiled Laws* and privacy and security requirements for applicable State and federal statutes, regulations, and security standards. OPS is also responsible for establishing and enforcing privacy principles, security guidelines, and policies and procedures for Treasury. OPS provides oversight and monitoring for 125 Treasury systems and data applications.

Audit Objective	**Conclusion**
Objective #1: To assess the effectiveness of OPS's efforts to administer access to select information systems and applications.	Moderately effective

Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
OPS did not obtain and review all security access rights frameworks from its business owners. OPS did not obtain 27% of the frameworks in fiscal years 2014 and 2015 and granted access to 50% of sampled users without a current framework, which impacted its ability to ensure that confidential information is available to only authorized individuals (Finding #1).		X	Agrees
OPS did not ensure that its security monitoring policy was updated in accordance with the State standard, which requires access rights to be reviewed every 120 days (Finding #2).		X	Disagrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of OPS's efforts to monitor business owners' compliance with select security guidelines.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
OPS did not implement and maintain an accurate inventory or document key information related to Treasury's information systems and applications (Finding #3).		X	Agrees
For 30% of 125 systems we reviewed, OPS did not ensure that business owners properly classified their data as public, sensitive, or confidential and assigned a level of low or high based on the data's sensitivity, criticality, and risk. Also, OPS did not timely validate that classifications were still appropriate for 16% of the systems reviewed (Finding #4).		X	Agrees

Obtain Audit Reports

Online: audgen.michigan.gov
Phone: (517) 334-8050

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

Doug A. Ringler, CPA, CIA
Auditor General

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

September 1, 2017

Mr. Nick A. 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 Privacy and Security, 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

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

OFFICE OF PRIVACY AND SECURITY

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

EFFORTS TO ADMINISTER ACCESS TO SELECT INFORMATION SYSTEMS AND APPLICATIONS

BACKGROUND

The Office of Privacy and Security (OPS) is responsible for securing and monitoring access to the Department of Treasury's (Treasury's) systems and applications. Additional key functional responsibilities of OPS include:

- Ensuring compliance and continuity of access controls across systems that utilize tax information.
- Maintaining and tracking agreements and compliance surrounding data use and disclosure with federal, State, and local government agencies.

Prior to granting access to Treasury's systems and applications, OPS obtains the user's request form, which is approved by the business owner*, and a completed Treasury confidentiality agreement. OPS reviews the request by comparing the user's job classification or purpose for access with the security access framework currently on file. A framework typically specifies the level of access (view, edit, create, or delete) and role based upon the job title or classification. The business owners and OPS are required to complete an annual review of the framework to ensure that access privileges are limited and restricted to the minimum required for performance of the job duties.

Prior to approving and granting access to tax data, OPS obtains a completed questionnaire to determine if the requesting entity is a local unit of government, a contractor, or another State agency and what specific tax information the entity is requesting. OPS then enters into a disclosure agreement with the requesting agency and ensures that the requestor has successfully completed online security awareness training and signed a confidentiality agreement. OPS contacts the agencies annually to confirm the individuals who have access to the tax data and to confirm that these individuals have passed the online training program and signed a confidentiality agreement within the past year.

AUDIT OBJECTIVE

To assess the effectiveness* of OPS's efforts to administer access to select information systems and applications.

CONCLUSION

Moderately effective.

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

FACTORS IMPACTING CONCLUSION

- Testing of 61 users with access to 9 systems administered by OPS disclosed that all users signed a confidentiality agreement, passed the online security awareness training program, and submitted a request form with the appropriate approval for access to the applicable system.

- Testing of 14 disclosure agreements disclosed that all agreements included specific language for safeguarding tax data and included specific individuals who have access to the tax data. Also, our testing of the 14 disclosure agreements disclosed that all individuals with access to the tax data had signed confidentiality agreements and completed the online training program.

- Reportable conditions* exist related to obtaining and reviewing security access rights frameworks and updating OPS's security monitoring policy.

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

FINDING #1

OPS needs to obtain and review all security access rights frameworks.

OPS did not obtain and review all security access rights frameworks from its business owners. This affects OPS's ability to ensure that confidential information is available to only employees whose job duties require such access. Also, OPS may not be able to assess whether new access or change in access requests are appropriate and consistent with internal control* without the current framework.

We used OPS's fiscal year 2014 and 2015 lists of frameworks and requested documentation to substantiate that the frameworks were obtained. We also reviewed a sample of 70 users to determine if their access rights were appropriate. We noted:

a. OPS did not obtain 18 (27%) of the 67 frameworks in fiscal year 2014.

b. OPS did not obtain 18 (27%) of the 66 frameworks in fiscal year 2015.

OPS granted access to 50% of sampled users without obtaining a current framework.

c. OPS granted access for 35 (50%) of the 70 sampled users without documentation of a current framework to validate that user access was appropriate.

Treasury policy ET-03179 requires OPS to annually request and review security access rights frameworks for information systems and applications for which it serves as the security administrator. The policy also requires OPS to evaluate and grant or deny user access rights and create accounts and unique user identification codes.

OPS informed us that business owners did not always provide OPS with the frameworks as requested. OPS also informed us that it used a prior framework to help ensure that access was appropriate when business owners did not provide the current framework.

RECOMMENDATION

We recommend that OPS obtain and review security access rights frameworks from its business owners.

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

OPS agrees with the recommendation. Process improvements have been implemented in FY 2016 and 2017 including enhanced training for Security Liaisons, monitoring, and an established escalation process to ensure compliance.

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

FINDING #2

OPS should ensure that its security monitoring policy is updated.

OPS did not ensure that its security monitoring policy was updated to be in compliance with the State standard requiring access rights to be reviewed every 120 days. Less frequent reviews may not timely detect and prevent unauthorized users and inappropriate user access.

Treasury's security monitoring policy (ET-03168) requires each business owner to evaluate annually whether employees' and vendors' access privileges are in accordance with their job responsibilities and to modify accordingly. Department of Technology, Management, and Budget (DTMB) Technical Standard 1340.00.020.01 (formerly 1335.00.03) requires a review of user accounts for compliance with account management requirements every 120 days. Account management requirements include controls such as authorizing access to information systems based on valid access authorization and intended system usage.

After we notified OPS of the discrepancy, OPS informed business owners to immediately begin reviewing access controls every 120 days. Also, OPS informed us that it created an action plan to update applicable policies and procedures to require the review of access controls at 120-day intervals as required by the DTMB Technical Standard.

RECOMMENDATION

We recommend that OPS ensure that its security monitoring policy is updated to be in compliance with the State standard requiring access rights to be reviewed every 120 days.

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

OPS does not agree that the security monitoring policy requiring access rights be reviewed every 120 days be updated at this time for all systems. Treasury is in compliance with nationally recognized standards, including the IRS Tax Information Security Guidelines that require agencies review accounts for compliance with account management requirements at a minimum of annually for user accounts. Additionally, the National Institute of Standards and Technology (NIST) does not define a review period. DTMB Agency Services, in collaboration with Treasury, has submitted an exception request to the DTMB Technical Review Board as the frequency of monitoring user access should be based on the data's sensitivity, criticality and risk before establishing a statewide standard.

EFFORTS TO MONITOR BUSINESS OWNERS' COMPLIANCE WITH SELECT SECURITY GUIDELINES

BACKGROUND

Treasury policy designates business owners as the division administrator, office director, or bureau director. Each business owner is responsible for determining the appropriate and compatible user access rights for each system or application, evaluating and limiting these rights, performing risk assessments, conducting periodic audit log reviews of user activities, and monitoring production data and database updates to ensure that only authorized changes were made. Treasury policy requires OPS to monitor activities of business owners and employees and vendors who have administrative or special access privileges assigned by business owners. OPS also monitors business owners' compliance with compensating control reports (CCRs) and prepares review reports upon completion of its monitoring activities.

OPS receives and compiles information from incident reports in which some aspect of physical or financial security is threatened; confidentiality or privacy of data is violated; data is manipulated, lost, or stolen; or financial resources or items of value are lost, stolen, or misused. Incidents may range from an unattended computer screen displaying sensitive information to a data breech. Also, OPS is responsible for reporting incidents regarding taxpayer information to the Internal Revenue Service, reviewing plans of action, and assessing corrective actions regarding the incidents.

AUDIT OBJECTIVE

To assess the effectiveness of OPS's efforts to monitor business owners' compliance with select security guidelines.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- OPS appropriately sampled and reviewed CCRs, provided written reports to the business owner regarding the CCR reviews, provided suggestions for corrective action, and conducted follow-up CCR reviews as required.

- For 52 privileged users* reviewed, OPS had ensured that its business owners reviewed and approved each privileged user for proper access and approvals.

- For 201 and 204 sampled access rights certifications completed in 2014 and 2015, respectively, OPS monitored business owners to ensure that the business owners reviewed the system access of their employees.

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

- A reportable condition exists related to the annual review of system access rather than the DTMB-required 120-day review (Finding #2).

- Reportable conditions exist related to implementing and maintaining a current inventory of Treasury information systems and applications and obtaining data classifications.

FINDING #3

OPS needs to improve its inventory of information systems and applications.

OPS did not implement and maintain an accurate inventory or document required information related to Treasury's information systems and applications.

This impacted OPS's ability to monitor business owners' reviews of their systems and applications at required intervals (see Findings #1 and #4) and prevented OPS from evaluating overall compliance of the business owners. In addition, OPS could not evaluate the overall effectiveness of its monitoring activities.

Control Objectives for Information and Related Technology* (COBIT) requires entities to maintain a current and accurate record of all information systems and applications and to identify those systems and applications that are critical in providing services. COBIT also requires an inventory to include information such as the business owner, custodian, data classifications, and criticality levels.

Our review of OPS's inventory disclosed that OPS did not:

a. Document the information systems and applications that capture, store, transfer, or maintain sensitive or confidential information.

   During our preliminary survey, OPS initially provided a list of 24 systems and applications and later provided another list containing 136. Finally, OPS determined that 125 systems and applications were applicable to Treasury operations. OPS did not document on any of the lists which information systems and applications maintain or contain sensitive or confidential information.

b. Identify, on its inventory lists, which systems and applications were considered critical to Treasury operations.

   However, Treasury identified 21 of the systems and applications as critical on its 2014 internal control evaluation.

c. Document the dependencies between information systems and applications.

   Identification of related processes and controls helps ensure that monitoring and assessment of all related access controls are not overlooked.

d. Document the security requirements for each information system and application.

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

RECOMMENDATION

We recommend that OPS implement and maintain an accurate inventory and document required information related to Treasury's information systems and applications.

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

OPS agrees with the recommendation. On June 20, 2017, OPS received the inventory of Treasury's information systems and applications, which includes required information applicable to each information system and application. OPS will establish a monitoring process by October 31, 2017 to ensure the inventory is updated regularly and the inventory is accurate and complete.

FINDING #4

OPS should ensure that business owners appropriately classify data.

OPS did not ensure that business owners classified their data as public, sensitive, or confidential and assigned a level of low or high based on the data's sensitivity, criticality, and risk. Classifying data into risk levels is intended to help protect data from security compromises that involve misuse and unauthorized access, disclosure, modification, or deletion.

Treasury's data classification policy requires OPS to ensure that all data is classified by the business owners and to confirm the business owners' review and reclassify data and risk levels every three years.

OPS's practice is to review the data classification that is included in the business owners' security plans*. Treasury business owners are required to ensure that all applications are covered by a security plan and that the security plans are reviewed at least every three years or when significant changes to the applications are planned. Treasury requires the security plans to include the data classification and associated risk level.

Our review of the 125 systems and applications monitored by OPS disclosed that it did not ensure that:

a. Business owners appropriately classified data for 38 (30%) systems and applications.

b. Data classification was still appropriate for 14 (16%) of the remaining 87 systems and applications.

The security plans for these exceptions were not completed or updated, and OPS did not have a process in place to review the data classification outside of the security plans.

RECOMMENDATION

We recommend that OPS ensure that business owners classify their data as public, sensitive, or confidential and assign a level of low or high based on the data's sensitivity, criticality, and risk.

AGENCY PRELIMINARY RESPONSE

Treasury provided us with the following response:

OPS agrees with the recommendation and is taking the necessary steps to establish a process to ensure business owners classify their data as public, sensitive or confidential and assign a level of low or high based on the data's sensitivity, criticality, and risk. The completion date is scheduled for January 31, 2018 and will be reviewed according to DTMB standards.

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

AGENCY DESCRIPTION

OPS's mission is to protect the privacy, confidentiality, and integrity of information collected, used, and retained by Treasury through progressive prevention, detection, and enforcement practices. OPS is responsible for administering the disclosure provisions of Section 205.28(1)(f) of the *Michigan Compiled Laws* as they relate to the safeguarding, use, storage, and disclosure of confidential tax return information, as well as privacy and security requirements for applicable State and federal statutes, regulations, and security standards. OPS is also responsible for establishing and enforcing privacy principles, security guidelines, and policies and procedures for Treasury. OPS provides oversight and monitoring for 125 Treasury systems and data applications in the areas of tax, investments, and accounting.

OPS's responsibilities include:

- Securing and monitoring access to Treasury's critical systems and applications.

- Fostering a privacy and security-oriented culture through participating in system development, security awareness education, and enforcement activities.

- Monitoring compliance with privacy, security, and nondisclosure requirements through periodic reviews.

- Participating in security incident investigations and resolutions within Treasury.

- Reviewing system security plans to ensure that security controls are acceptable and risks have been identified and accepted by appropriate Treasury management and executive personnel.

- Developing and negotiating data exchange agreements with federal, State, and local agencies to ensure the protection and integrity of State tax information.

OPS had expenditures of $1.1 million and $1.3 million for fiscal years 2014 and 2015, respectively. As of May 2016, OPS had 10 full-time equated employees.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine OPS's activities and other records regarding granting access to select information systems and applications and monitoring business owners' compliance with security guidelines. 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2013 through February 29, 2016.

METHODOLOGY

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

- Interviewed OPS management and staff to obtain an understanding of OPS's organizational structure, operations, responsibilities, and activities.

- Reviewed applicable laws, regulations, policies and procedures, and other relevant information provided by OPS.

- Analyzed the inventory of Treasury systems and applications provided by OPS management.

- Reviewed a list of active users and security access rights frameworks for 4 of Treasury's critical systems.

- Reviewed disclosure letters.

- Reviewed monitoring schedules for annual access rights certifications and CCRs.

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

OBJECTIVE #1

To assess the effectiveness of OPS's efforts to administer access to select information systems and applications.

To accomplish this objective, we:

- Reconciled lists of frameworks for critical systems and applications that OPS administers with the inventory list of Treasury systems and applications to ensure that OPS included all necessary frameworks in its population for monitoring.
- Reviewed 67 frameworks for 9 critical systems and related applications that OPS administers to ensure that OPS obtained the frameworks from Treasury's business owners for use in administering access.
- Selected a sample of 70 of the 6,806 users in 9 critical systems administered by OPS to determine that system access was consistent with established frameworks, properly authorized, and granted to eligible users who had signed a confidentiality agreement and successfully completed online security awareness training. We randomly selected the users and judgmentally selected the systems to ensure that we obtained sufficient audit coverage. Therefore, we could not project our results to the entire population.
- Reviewed records for a random sample of 14 of 37 disclosure agreements in effect during October 1, 2013 through February 29, 2016. Our sample was randomly selected to eliminate any bias and to enable us to project the results to the entire population.

OBJECTIVE #2

To assess the effectiveness of OPS's efforts to monitor business owners' compliance with select security guidelines.

To accomplish this objective, we:

- Analyzed 136 Treasury systems and applications to determine the population of systems and applications for which OPS is responsible for ensuring that a data classification was completed.
- Reviewed records for each of the 125 Treasury systems and applications to determine if OPS ensured that business owners completed required data classifications.
- Selected a sample of 201 and 204 individual certifications for 2014 and 2015, respectively, to determine if OPS ensured that business owners had completed user access reviews. Our

sample was judgmentally selected to ensure that we obtained sufficient audit coverage. We could not efficiently determine the number of individual certifications in the population. Therefore, we could not project our results to the entire population.

- Reviewed 11 CCR compliance reviews prepared by OPS to determine if OPS reviewed the required number of CCRs and prepared a compliance review for all applicable business owners.

- Reviewed 52 privileged users identified by OPS as of February 11, 2016 to determine if OPS ensured that all business owners submitted approvals for the applicable privileged users and roles.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions* or 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 4 findings and 4 corresponding recommendations. Treasury's preliminary response indicates that OPS agrees with 3 recommendations and disagrees 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.

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

GLOSSARY OF ABBREVIATIONS AND TERMS

business owner

The division administrator, office director, or bureau director responsible for the primary business functions served by the system or application.

CCR

compensating control report.

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 IT.

DTMB

Department of Technology, Management, and Budget.

effectiveness

Success in achieving mission and goals.

internal control

The plan, policies, methods, and procedures adopted by management to meet its mission, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.

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.

OPS

Office of Privacy and Security.

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.

privileged user

A user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform. Privileged users manage access rights of individual users and monitor user activities.

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 plan

Documents the security requirements to protect the availability, confidentiality, and integrity of information assets (information and information resources). The plan describes the security controls that are necessary for preventing or minimizing unauthorized disclosure, fraud, waste, and abuse.

Treasury

Department of Treasury.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650