Office of the Auditor General
Performance Audit Report

Offender Management System

Department of Corrections and
Department of Technology, Management, and Budget

July 2018

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

471-0593-17

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

Offender Management System (OMS)

Department of Corrections (DOC) and Department of Technology, Management, and Budget (DTMB)

Report Number:
471-0593-17

Released:
July 2018

DOC uses OMS to maintain and process offender-related information, including release date computations, daily counts of offenders housed at DOC correctional facilities, and misconduct tracking. OMS data is also used to generate notifications to crime victims as required by Michigan law. DOC implemented OMS in August 2014 at a cost of $13.8 million. As of April 2017, OMS had 2,881 active users.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of DOC's and DTMB's security and access controls over OMS.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DOC did not fully establish and implement access controls over OMS. Forms to approve user access were not maintained for 89% of our sample items, 35% of users did not use their accounts for over 60 days, and 2 (17%) of 12 user roles tested allowed greater capabilities than what was intended (Finding #1).	X		Agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DOC's OMS.	Effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
None reported.	Not applicable.		

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

This Page Left Intentionally Blank

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

July 31, 2018

Ms. Heidi E. Washington, Director
Department of Corrections
Grandview Plaza Building
Lansing, Michigan
and
Mr. David L. DeVries
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Ms. Washington and Mr. DeVries:

This is our performance audit report on the Offender Management System, Department of Corrections and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. The Department of Corrections provided a preliminary response to the recommendation 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

OFFENDER MANAGEMENT SYSTEM

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

OMS 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.

AUDIT OBJECTIVE

To assess the effectiveness* of the Department of Corrections' (DOC's) and the Department of Technology, Management, and Budget's (DTMB's) security and access controls over the Offender Management System (OMS).

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DOC defined and implemented OMS user roles and the level of access for each role.

- DOC implemented group access to improve its management of access for users performing similar OMS activities.

- No reportable issues were identified related to read-only access roles in OMS.

- One material condition* related to establishing and implementing access controls over OMS (Finding #1).

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

FINDING #1

Improved OMS access controls are needed.

DOC did not fully establish and implement access controls over OMS, thereby increasing the risk of unauthorized access, use, and modification of offender data.

State of Michigan Technical Standard 1340.00.020.01 requires that State agencies establish a process to control and document the assignment of access rights based on current job responsibilities and the principle of least privilege*. This Standard also requires the review of access rights every 120 days for appropriateness, disabling of accounts inactive for more than 60 days, monitoring of privileged users' activity, and implementation of a session time-out after 15 minutes of inactivity.

DOC did not:

a. Fully establish a formal process to grant and remove access to OMS, including the consistent use of a standard access authorization form to document business owner approval of the access rights granted to OMS users.

We noted:

Access authorization forms not always maintained.

(1) DOC did not maintain an authorization form for 75 (89%) of 84 randomly and judgmentally selected OMS accounts.

DOC informed us that it did not implement the use of an access authorization form until 2017. However, as indicated in the following chart, DOC did not maintain a form for 3 (60%) of the 5 accounts created in 2017:

	Number of Active User Accounts Created	Number of User Accounts Reviewed	Number of User Accounts Without an Authorization Form
Before 2017	2,840	79	72 (91%)
In 2017	41	5	3 (60%)
Total	2,881	84	75 (89%)

DOC also indicated that it did not require users from other State agencies to complete the authorization form because these accounts were grandfathered in from the prior offender management system.

(2) The authorization form does not require or capture an approval signature. For the 9 instances in which DOC maintained the form, 8 (89%) lacked the name of the authorized requestor and all 9 lacked an approval signature.

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

b. Always perform effective user account management.

We noted:

(1) DOC did not have formalized procedures for periodically reviewing and recertifying user rights to ensure that access remained appropriate based on the user's job responsibilities. DOC indicated that, although it did not require management to periodically recertify users' access rights, it did conduct monthly reviews of OMS user access rights. However, DOC did not document the results of its reviews and, therefore, we were unable to verify that they occurred.

Inactive user accounts should be reviewed and disabled.

(2) DOC did not review and disable user accounts that were inactive for more than 60 days.

We reviewed all 2,881 active OMS accounts and determined that:

(a) 48 (2%) were associated with an individual who left DOC employment and, therefore, no longer required access.

(b) 637 (22%) had never logged in to OMS.

(c) 1,000 (35%) had not been accessed in the last 60 days.

(3) DOC, in conjunction with DTMB, did not ensure that OMS database access was removed timely when individuals left employment or changed job responsibilities. Three (7%) of 45 database accounts should have been disabled. One of the 3 accounts had administrator access rights which allowed elevated privileges.

Periodic reviews of user accounts help ensure that privileges granted to each user remain appropriate for his/her job responsibilities. On February 2, 2017, DOC began a process to identify and remove unnecessary user accounts. At the end of our fieldwork, DOC informed us that it had created reports to identify when users last accessed their accounts.

c. Always grant access to OMS based on the principle of least privilege.

We noted:

(1) 3 (33%) of the 9 accounts had been assigned access rights greater than those requested on the authorization form.

DOC informed us that when its Data Security and Privacy section reviewed these access forms, it recognized that the users did not request all roles necessary to perform their job responsibilities. Therefore, Data Security and Privacy staff granted the additional roles.

Although additional rights beyond those documented in the request were necessary, the Data Security and Privacy staff should require the authorized requestor to resubmit an amended form. This would ensure that all access has been requested by an individual knowledgeable of the user's job responsibilities, ensuring proper segregation of duties* between the authorized requestor and Data Security and Privacy staff.

(2) 13 DTMB employees, including database administrators, were granted access rights in excess of those necessary to perform their job responsibilities.

(3) 7 generic test accounts not associated with a specific user inappropriately had access to the production environment.

DTMB indicated that these accounts should be used to test OMS functionality in the development and test environments and should be disabled in the production environment. Eliminating generic production accounts will increase accountability for actions performed in OMS.

d. Routinely monitor audit logs for inappropriate user activity.

Monitoring audit logs can assist in identifying inappropriate or unusual user activity.

e. Fully ensure that OMS user roles functioned as described.

We judgmentally selected and tested 12 roles that were read-only or allowed a user to update offender data for a specific facility. Two (17%) of the 12 roles allowed a user to update offender data at all facility locations rather than at only the facility to which the user was authorized to access.

f. Employ a session time-out after 15 minutes of inactivity.

DTMB informed us that it had a plan to implement this feature.

We consider this finding to be a material condition because the number of weaknesses we reported, when taken as a whole, represent a lack of basic access controls and business processes. Also, OMS contains sensitive and confidential information, such as personally identifiable information and health records.

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

RECOMMENDATION

We recommend that DOC fully establish and implement access controls over OMS to help mitigate the risk of unauthorized access, use, and modification of offender data.

AGENCY PRELIMINARY RESPONSE

DOC provided us with the following response:

DOC agrees with the recommendation.

DOC initially bulk loaded user accounts which had prior approved security access from the prior data system (CMIS). The three specific user accounts identified in the audit belonged to DTMB Agency Services staff who were assisting in testing and verifying the OMS security system. This testing was completely under the control of DOC's Data Security and Privacy team. Access requests are processed from the authorized requestor's email accounts, which are effectively signed by virtue of the email account. DOC did not always retain the associated emails that accompanied the access requests, therefore, DOC agrees to take steps to comply by retaining the email authorizations.

Also, DOC has a process to review OMS user access rights monthly but did not effectively document these reviews. DOC will begin documenting these reviews. Also, prior to the onset of the audit, DOC had already initiated internal reviews to correct the issues noted.

In addition, DOC will ensure that the Data Security and Privacy team verify, in writing, the needed level of access prior to authorizing more than requested. Also, security reviews have been performed and user account reports have been developed.

EFFECTIVENESS OF OMS

BACKGROUND

DOC uses OMS to maintain and process offender-related information. The primary OMS functionality includes calculating offender release dates, processing offender misconducts*, tracking offender headcount, and maintaining crime victim notification information.

AUDIT OBJECTIVE

To assess the effectiveness DOC's OMS.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

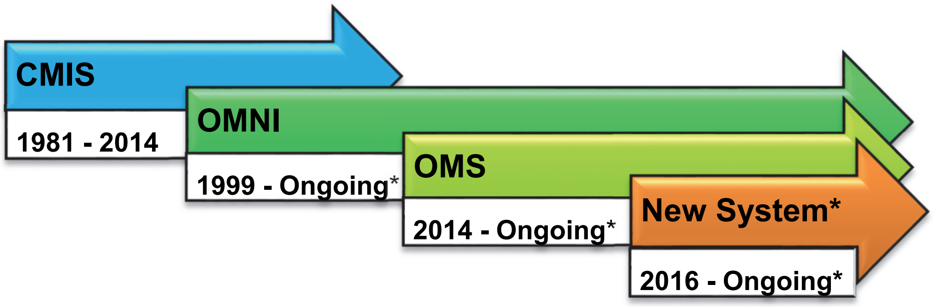
- DOC's Central Time Computation Unit performs audits of offender records, including recalculating release dates before an offender is released on parole or discharged.
- DOC's Automated Data Systems Section routinely updates OMS to address issues related to time computation and other OMS functionality.
- No significant data integrity weaknesses were identified related to critical OMS data fields such as offense date, corrected date*, sentence minimum and maximum term, and sentence begin date.
- No significant data integrity weaknesses were identified related to selected OMS data fields compared with source documents in the case files.
- No significant weaknesses were identified related to our testing of the accuracy of offender release dates for selected offenders and sentence types.

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

SYSTEM DESCRIPTION

In 1981, DOC implemented the Corrections Management Information System (CMIS). The main functionality of CMIS was the computation of offender release dates. DOC implemented the Offender Management Network Information System (OMNI) in 1999 to replace CMIS; however, OMNI only replaced some functionality and the time computation functions remained in CMIS. In August 2014, DOC replaced CMIS by implementing OMS at a cost of $13.8 million. OMS functions alongside OMNI to manage offender information.

As of March 2017, DOC was in the process of selecting a vendor to implement a new offender management system that will incorporate OMS and other computer systems such as OMNI, Crime Victim Information System, and NextGen (health care) into a single system. The following time line shows DOC's offender management systems:



**As of March 2017, DOC utilized OMS alongside OMNI and was in the process of selecting a vendor to implement a new offender management system.*

OMS interfaces with OMNI and eight other DOC computer systems to maintain and process offender-related information. As of April 2017, OMS had 2,881 active users, including DOC's central office, correctional facilities, and Reception and Guidance Center employees.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records related to OMS. 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 August 2014 through September 2017.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of OMS. During our preliminary survey, we:

- Interviewed DOC management and staff to gain an understanding of how DOC utilizes OMS.

- Reviewed DOC policies and procedures to gain an understanding of the offender management process.

- Obtained an understanding of the time computation rules in OMS.

OBJECTIVE #1

To assess the effectiveness of DOC's and DTMB's security and access controls over OMS.

To accomplish this objective, we:

- Interviewed DOC management and staff to gain an understanding of the process for granting and revoking access to OMS users.

- Randomly and judgmentally selected 84 of 2,881 OMS user accounts created prior to May 2017 to determine whether DOC maintained access request forms.

- Judgmentally selected 12 of 44 user roles as of April 2017 to determine whether OMS access rights were appropriate as described by system documentation.

- Reviewed 45 accounts with access to the OMS database as of July 2017 to determine whether their access was appropriate.

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

We made our selections using a risk-based approach on the user activation date and the security role type. Because our selections were judgmental, we could not project our results to the respective populations.

OBJECTIVE #2

To assess the effectiveness of DOC's OMS.

To accomplish this objective, we:

- Obtained and analyzed an extract of selected offender data from the OMS database.

- Judgmentally selected 44 of 8,057 offenders who served in prison between August 2014 and June 2017 and recalculated their release dates. We also reviewed hard-copy records to assess whether OMS accurately reflected the records.

- Judgmentally selected 94,030 of 736,420 offenders in OMS as of June 2017 who served a prison sentence between August 2014 and June 2017 to test the accuracy and completeness of selected offender data fields in OMS.

- Interviewed Crime Victim Unit staff to gain an understanding of the process for notifying crime victims of changes to an offender's status, location, and release dates as required by law.

- Judgmentally selected 93 of 22,966 notification letters, such as discharge and parole decision letters, sent to crime victims between August 2014 and July 2017 to determine whether DOC notified victims as required by law.

- Conducted a survey of OMS users to gain an understanding of their satisfaction with OMS.

We made our selections using a risk-based approach. Because our selections were judgmental, we could not project our results to the respective populations.

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.

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

AGENCY RESPONSES

Our audit report contains 1 finding and 1 corresponding recommendation. DOC's preliminary response indicated that it agreed with the recommendation.

The agency preliminary response that follows the recommendation in our report was taken from the agency's written comments and oral discussion at the end of our 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 to 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.

CMIS
Corrections Management Information System.

corrected date
The sentence begin date minus the jail credits.

DOC
Department of Corrections.

DTMB
Department of Technology, Management, and Budget.

effectiveness
Success in achieving mission and goals.

IT
information technology.

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. Our assessment of materiality is in relation to the respective audit objective.

misconduct
A violation by a prisoner of DOC prison rules.

OMNI
Offender Management Network Information System.

OMS
Offender Management System.

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.

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.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

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