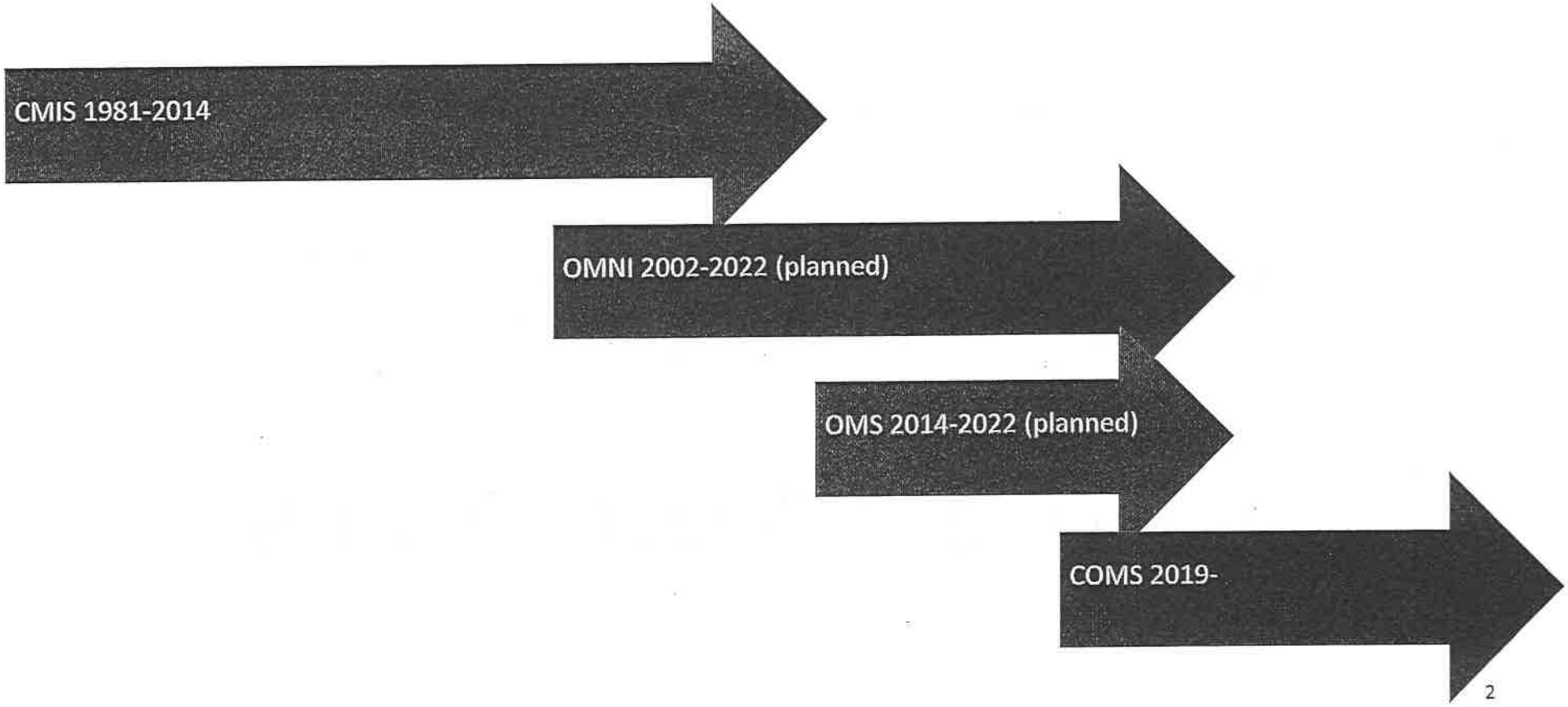
Senate Oversight Committee

Review of OAG Performance Audit of MDOC Offender Management System (OMS)

(471-0593-17 July 2018)

February 19, 2019

MDOC Offender Data Systems Roadmap



OMS Functions

- Parole Board Actions
- Crime Victims Registrations
- Facility Head Counts
- Offender Misconduct Processing
- Time Computations (Release Dates)
- Reports including Physical and Mental Health

- 2,734 OMS Users

OAG Performance Audit Timing

- August 2014 – OMS goes live with role-based security initially bulk loaded with active CMIS user accounts and security roles

- January 2017 – MDOC engages DTMB Agency Services to assist with formal review of OMS user accounts and security roles
  - MDOC and DTMB review, test, revise, and document the OMS security roles and develop user account and user access reports

- March 2017 – OAG initiates OMS performance audit kickoff

Audit Findings

- Objective 1 – Effectiveness of access controls over OMS
  - Moderately Effective, though Material Finding due to weak documentation of user access forms and weak enforcement of account inactivity

- Objective 2 – Effectiveness of OMS
  - Effective – Reviewed Time Computations controlling release dates for prisoners

Objective 1 Documentation Weaknesses

- 1.a – Due to the volume of MDOC data system users, MDOC uses an Authorized Requestor (AR) process to request user access. The AR process provides the Data Security and Privacy Team (DSP) with a formal predefined list of requestors.
- Form CFJ-558 is used to request OMS access
- 1.a.1 – Missing authorization forms
  - Pre-2017 OMS user access was bulk loaded from CMIS
  - In 2017, the 3 new OMS users reviewed were DTMB staff helping DSP test each OMS security role – their roles were rapidly changing under direct supervision of DSP

Objective 1 Documentation Weaknesses (cont'd)

- 1.a.2 – Authorization forms missing signatures
  - DSP accepted CFJ-558 without AR signatures. Forms were received from AR's email account, effectively providing a signature. However, AR emails were not archived and available for audit.
- 1.b.1 – Monthly OMS user access rights reviews were not archived
  - Reviews of access rights vs. job duties were not saved for audit
- 1.b.2 – OMS user accounts inactive for more than 60 days
  - When audit began, user account activity reports hadn't been created
- 1.b.3 – DTMB OMS user accounts not reviewed for changes
  - When audit began, user account activity reports hadn't been created

Objective 1 Documentation Weaknesses (cont'd)

- 1.c.1 – OMS access rights granted greater than requested by DSP
  - Review of initial access request by DSP determined missing security roles based on job function – these were granted by DSP without return to the AR for correction
- 1.c.2 – DTMB staff had access rights greater than job duties
  - Higher access rights are temporarily needed for OMS system maintenance duties but were not removed when work was completed
- 1.c.3 – Generic test accounts exist
  - Generic test accounts were initially created for user acceptance testing, but later determined unusable with individual SOM Active Directory based user network accounts. These generic accounts were rediscovered when user account activity reports were created.

Objective 1 Documentation Weaknesses (cont'd)

- 1.d – Use audit logs to identify unusual user activity
- 1.e – Ensure user security roles function as described
- 1.f – Employ session timeout after 15 minutes of inactivity

Lessons Learned and Next Steps

- DSP user account processes are being formalized
- DSP has enhanced their documentation retention processes to ensure review artifacts are maintained for future audits
- Monthly user account activity reports are being reviewed for appropriate follow up action and the results retained for future audits
- DTMB has implemented 60 day SOM network account inactivity disabling and 90 day inactivity account deletion
- DTMB has implemented 15 minute idle time-out for SOM network accounts, preempting the need for a 15 minute OMS idle time-out

Offender Management System (OMS) User Request Form

CFJ-558 8/14

Section I

Instructions: Submit one completed form per user to OMNI_User_Accounts@michigan.gov. Complete Section I& II on all applications, complete Section III based on the type of request. A State of Michigan (SOM) account must be created before an OMS account can be created.

Create Account ☐	Modify Account ☐	Deactivate Account ☐	Date Click here to enter a date.

Section II

Last Name: Click here to enter text.	First Name Click here to enter text.	Middle Name Click here to enter text.
SOM Username Click here to enter text.	HRMN Choose an item.	Work Location Click here to enter text.

Section III

Security Roles = Each security role is associated with a set of privileges that determines the user's access to information within OMS. **Business Unit** = Each user must be assigned a business unit, usually their work location. Business Units limit what data a user can update. **Team** = Teams are an additional layer of security that provide additional update access. **See OMS Security Document in DAS**

Security Role	Business Unit (a Location)	Team (not being used at this time)
1. Click here to enter text. 2. Click here to enter text. 3. Click here to enter text. 4. Click here to enter text. 5. Click here to enter text.	1. (Only one Business Unit) _____ Print Yes ☐ No ☐	1. Click here to enter text. 2. Click here to enter text. 3. Click here to enter text. 4. Click here to enter text. 5. Click here to enter text.

Authorized Requestor: Click here to enter text.	Date: Click here to enter a date.

Section IV – For ADSS use only

Application Status Approved ☐ Denied ☐ Reason Click here to enter text.	Date Processed Click here to enter a date.	Processed By Click here to enter text.	Secondary Approval Approved ☐ Denied ☐

Offender Management System (OMS) User Request Form

CFJ-558 8/14

Section I

Instructions: Submit one completed form per user to OMNI_User_Accounts@michigan.gov. Complete Section I& II on all applications, complete Section III based on the type of request. A State of Michigan (SOM) account must be created before an OMS account can be created.

Create Account ☐	Modify Account ☐	Deactivate Account ☐	Date Click here to enter a date.

Section II

Last Name:	First Name	Middle Name
Click here to enter text.	Click here to enter text.	Click here to enter text.
SOM Username	**HRMN**	**Work Location**
Click here to enter text.	Choose an item.	Click here to enter text.

Section III

Security Roles = Each security role is associated with a set of privileges that determines the user's access to information within OMS. **Business Unit** = Each user must be assigned a business unit, usually their work location. Business Units limit what data a user can update. **Team** = Teams are an additional layer of security that provide additional update access. **See OMS Security Document in DAS**

Security Role	Business Unit (a Location)	Team (not being used at this time)
1. Click here to enter text. 2. Click here to enter text. 3. Click here to enter text. 4. Click here to enter text. 5. Click here to enter text.	1. (Only one Business Unit) Print Yes ☐ No ☐	1. Click here to enter text. 2. Click here to enter text. 3. Click here to enter text. 4. Click here to enter text. 5. Click here to enter text.

Authorized Requestor: Click here to enter text.	Date: Click here to enter a date.

Section IV – For ADSS use only

Application Status	Date Processed	Processed By	Secondary Approval
Approved ☐ Denied ☐ Reason Click here to enter text.	Click here to enter a date.	Click here to enter text.	Approved ☐ Denied ☐