GRETCHEN WHITMER
GOVERNOR

STATE OF MICHIGAN
STATE BUDGET OFFICE
LANSING

CHRIS KOLB
DIRECTOR

June 13, 2019

Rick Lowe, Director
Office of Internal Audit Services
State Budget Office
George W. Romney Building
111 South Capitol, 8th Floor
Lansing, MI 48913

Dear Rick:

In accordance with the State of Michigan Financial Management Guide, Part VII, I have attached a summary table identifying our responses and corrective action plans to address recommendations contained within the Office of the Auditor General's performance audit report of SIGMA Selected Application Controls and Service Level Requirements.

Questions regarding the summary table or corrective action plans should be directed to Ruth Schwartz, Director, SIGMA Operations and Support.

Sincerely,

Signature Redacted

Chris Kolb
State Budget Director

cc: Executive Office
Office of the Auditor General
House Fiscal Agency
Senate Fiscal Agency
General Government Subcommittee

GRETCHEN WHITMER
GOVERNOR

STATE OF MICHIGAN
STATE BUDGET OFFICE
LANSING

CHRIS KOLB
DIRECTOR

June 13, 2019

SIGMA Operations and Support
State Budget Office

Summary of Agency Responses to Recommendations
Audit Period: October 1, 2016 through September 30, 2018

1. Audit recommendations the agency complied with:
   - SBO agrees with and has complied with the recommendations associated with findings 1, 2, and 4 (see table, below).

2. Audit recommendations the agency agrees with and will comply:
   - SBO agrees with or partially agrees with the recommendations associated with findings 3, 5, and 6. Portions of the actions are complete and portions for the recommendations we agree with are in progress (see table, below).

Finding #	Recommendation	SIGMA Operations & Support Response	Status
1	We recommend that SBO, in conjunction with State agencies, improve its user account management controls to help ensure that SIGMA access is secure and that controls are properly designed and implemented in accordance with SOM technical standards.	SBO agrees that continual improvement of user account management controls help ensure that SIGMA access is secure and controls are properly designed and implemented in accordance with SOM technical standards. Regarding the specific parts of the finding: • The users noted in part a. were in a pending status for final timesheet and payroll processing. Access was timely and systematically removed once the final termination status was complete. SIGMA will review the systematic	COMPLETE The systematic user disabling is functioning properly at this time. ASAs can process UDOCS to remove access other than ESS if appropriate. Users access is completely removed once an employee is in terminated status. SIGMA Operations and Support has established and implemented proper monitoring through TOPP-0006. Central and agency level

Finding #	Recommendation	SIGMA Operations & Support Response	Status
		removal of access to determine if changes are needed. • The guidance noted in part b. was issued in August 2018. SIGMA completes monitoring centrally and in coordination with State agencies to ensure bypassed approvals are monitored weekly. • The monitoring noted in part c. will continue to evolve as needed to meet State standards and needs.	review of high access activity (bypass and overrides) is performed weekly. SIGMA completes compliance reviews to ensure agencies are following TOPP guidance. DTMB agency services completes reviews of ADMN level access weekly. This includes ADMN, ADMINLITE, CTRLFINADMNSU, CTRLHRMSU, and other high access roles.
2	We recommend that SBO implement workflow controls for all document codes that should require approval.	SBO provided us with the following response: SBO agrees with this recommendation. Workflow was tested and then added to the EAMD document in production in February 2019. The remaining document codes are not believed to require workflow for one of the following reasons: • The document code is not being used in SIGMA and has been inactivated to prevent its use. • The document code is systematically generated after a different document code received all required approvals and became final. • The document code is created from an interface where the approvals are documented in the initiating system. SBO is reanalyzing all 175 document codes without workflow based on 1-year plus of operations to confirm that EAMD was the only document code requiring the addition of workflow.	COMPLETE SIGMA Operations and Support has reviewed all documents and established workflow or documented the justification where workflow is not necessary. SIGMA has a review process to ensure workflow is evaluated and established, if appropriate, for all new documents. Removal of workflow requires justification prior to implementation. A log of documents without workflow is maintained.
3	We recommend that SBO, in conjunction with State	SBO agrees with the recommendation that State	

Finding #	Recommendation	SIGMA Operations & Support Response	Status
	agencies, fully establish and implement interface controls over the SIGMA application.	agencies, in conjunction with SIGMA, fully establish and implement interface controls over the SIGMA application. SIGMA developed the Interface Feedback Report to provide detailed record status, record counts, and control totals to assist agencies with interface reconciliation. In addition, SIGMA Vendor / Customer Update data, EFT and Warrant Payment Status, EFT Payment Return and Notice of Change (NOCs), and Converted Warrant Status Update data is available to agencies on a daily basis through the Extract Management Layer (EML) for reconciliation purposes. Agencies are responsible for leveraging this data and similar data from interfacing systems in order to complete reconciliation activities and are responsible for documenting their reconciliation procedures as these procedures may differ by agency and by interfacing system. SIGMA issued Temporary Operating Policy & Procedure 0007 on November 9, 2018, providing guidance to the agencies regarding interface reconciliation. As noted in part c., there is a potential software defect related to the display of payroll reconciliation data online. This has been logged with the software vendor and is being researched. SIGMA is printing the balanced screens and attaching the information to the reconciliation documentation to ensure that the reconciliations can be recreated and relied upon after subsequent cycles are processed.	COMPLETE COMPLETE IN PROGRESS SIGMA continues to maintain the paper documentation for payroll reconciliation as a back-up and also has verified that this issue does not appear to be occurring any longer. We will continue to monitor.
4	We recommend that SBO improve the completeness	SBO agrees with the recommendation to improve the	COMPLETE

Finding #	Recommendation	SIGMA Operations & Support Response	Status
	and accuracy of its vendor master data to help ensure that all SOM payments are made to legitimate entities.	completeness and accuracy of vendor master data and the related processes, and has taken corrective action regarding the issue that caused missing TINs. SIGMA is in the process of updating and creating procedures to improve the use of the TIN matching process to help ensure accurate and complete vendor data. SBO (SIGMA and OFM) complies with IRS requirements for obtaining TIN information, issuing B-notices as directed by the IRS, and applying backup withholding when appropriate. In addition, SBO requires W8 or W9 information from registered vendors and this serves as a safe harbor with the IRS regarding the accuracy of vendor information. With the implementation of SIGMA, SBO elected to use a nightly IRS TIN match process to further ensure the accuracy of TIN information as reported by vendors. Although these processes were used to help ensure accurate and complete vendor data, a formal process for steps to take regarding mismatches identified in the process had not been established.	SIGMA has implemented data fixes for all vendors without TINs to either inactivate the vendor or add a TIN following vendor submission of appropriate documentation. SIGMA has established and implemented a process for IRS TIN matching (TIPP-0018). The process extracts new registrations nightly and sends a file weekly to the IRS and results are returned. Vendors are contacted if the process returns an invalid TIN entry. Corrections are made to the vendor file with the submission of appropriate documentation from the vendor.
5	We recommend that SBO improve management of the service level requirements within the SIGMA contract to help ensure that services provided by the vendor meet the level of performance agreed to with the State.	SBO partially agrees with the recommendation. SBO agrees that additional details in the reporting against the standards and associated formal processes for monitoring were necessary. A change notice to the contract was executed in December 2018 to address this. This change notice resulted in further detailing the service level requirements from 15 to 26 and included clarifications to calculations and reporting requirements.	COMPLETE

Finding #	Recommendation	SIGMA Operations & Support Response	Status
		SBO disagrees that improved management of the service level requirements is necessary to ensure the vendor meets the level of performance agreed to with the State. In addition, SBO disagrees with some of the details contained in the finding. SIGMA extensively and thoroughly monitors and enforces service level requirements. The failure to meet the requirements was not the result of the level of management and monitoring performed by SBO. Except for Standard 14, the OAG-Determined Status of the Service Level Standards (as presented in the supplemental information) matches the status that was determined by SBO. All contractual provisions were properly enforced. It is SBO's position that Standard 14 was met based on the contractual requirements, however, increased detail in the report was needed. As noted above, a change notice to the contract was executed in December 2018 and additional details are now included in the monthly reports. As with any new system, particularly one of this size and complexity, numerous adjustments and tuning efforts have been done and continue to be done to improve the level of service received by the vendor. SBO is conducting a cost benefit analysis regarding additional monitoring processes and third-party monitoring options.	IN PROGRESS As a result of the contract change notice executed in December 2018, SOSTIPP 0010 is being reviewed and updated to ensure monitoring of the SLAs are in alignment with the modified standards. SBO continues to work with CGI to increase the detail provided in the SLA report related to the server capacity and security standards. These activities are anticipated to be complete by 7/31/2019. IN PROGRESS SBO has engaged with DTMB to explore independent monitoring of response time associated with several SLA standards. The assessment is anticipated to be complete by 8/31/2019 including a recommendation for implementation options.
6	We recommend that SBO sufficiently assess the level of coverage obtained in the Annual Security Review service level requirement.	SBO partially agrees with the recommendation. SIGMA agrees with the need to continually assess the level of coverage obtained in the annual security review service level requirement. In addition, the	IN PROGRESS SIGMA Operations and Support is working with DTMB Agency Services to develop a schedule to review 1/3 or the NIST control families on an annual basis. In addition, the

Finding #	Recommendation	SIGMA Operations & Support Response	Status
		formal assessment of complementary user-entity controls began with the preliminary Top Down Risk Assessment effort that is a precursor to the biennial internal control evaluation which will be completed by May 2019. SBO disagrees with the assertion that the level of coverage obtained was not sufficiently assessed. Extensive analysis was conducted jointly by SIGMA, the Office of Internal Audit Services, and DTMB Agency Services with advisement from the Office of the Auditor General to identify and define the scope (level of coverage) of the annual security review (SOC report). We agree that a more formal assessment of complementary user-entity controls needs to be completed and that additional formalized processes to review the results of the examinations are needed. The scope of coverage from the SOC engagements and additional required penetration and vulnerability testing will be continually evaluated. SIGMA has multiple informal processes in place including processes published in Temporary Internal Policies and Procedures (TIPPs), Temporary Operational Policies and Procedures (TOPPs), and the Operational Framework. In addition, SIGMA leverages multiple weekly and twice daily meetings to review issues, discuss upcoming activities, coordinate support needs, and review Plan of Action & Milestone (POAM) security vulnerabilities.	penetration and vulnerability test includes an independent assessment of 1/3 of the NIST control families annually. Both of these efforts will provide information used to assess the level of covered required by the vendor's annual security review. COMPLETE IN PROGRESS SIGMA Operations and Support is leveraging the work done on the Biennial Internal Control Assessment, the Penetration and Vulnerability Test, and the results of the most recent third party SOC Engagements contracted by CGI to determine if changes to the scope of the SOC engagements are needed. This evaluation will be documented and completed by the end of July 2019.