LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Kenneth E. Varns, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
William Soller
Miki Cestnik

# MEMORANDUM

**TO:** Legislative Audit Committee Members

**FROM:** Shaina Geubtner, Associate Information Technology Auditor

**CC:** Department of Administration
Misty Ann Giles, Director
Cheryl Grey, Administrator, State Financial Services Division
Karol Anne Davis, Administrator, State Human Resources Division
Martha Watson, Human Resources Information Systems Manager
State Information Technology Services Division
Kevin Gilbertson, Chief Information Security Officer
Michele Snowberger, Deputy Chief Information Security Officer
Diane Stuart, IT Security Specialist Supervisor
Penne Cross, IT Security Specialist

**DATE:** August 2024

**RE:** Information Technology Audit Follow-up (24SP-21): *SABHRS Security Assessment* (orig. 22DP-01)

## Introduction

The *SABHRS Security Assessment (22DP-01)* report was issued to the Legislative Audit Committee in June 2023. The audit included two recommendations for the Department of Administration (department). From March to August 2024, we conducted follow-up work to assess the implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

**Overview**

The Department of Administration oversees the Statewide Accounting, Budgeting, and Human Resources System (SABHRS), used by all state agencies to maintain human resource and financial information for state employees and programs. Our audit examined SABHRS system security and IT management. We found that the department had not designated a dedicated role for SABHRS security responsibilities. The management of the SABHRS audit logs also needed improvement, and the department did not have a continuous monitoring program in line with state requirements. In response, the department has assigned a SABHRS security officer and is working to capture additional audit log information. The audit contained two recommendations, one implemented and the other is being implemented.

## Background

The department's mission is to provide effective, efficient, and customer-driven solutions to benefit the citizens of Montana through the transformation of delivery and access to services. The department serves the state government by providing other agencies with business services, like accounting and human resources. These business services are delivered through SABHRS, which contains all state financial transactions and data for over 15,000 state employees. SABHRS is managed by two separate divisions

within the department — the State Financial Services Division (FS) and the State Human Resources Division (HR).

During our audit, we found that security documentation managed the SABHRS HR and FS system functions as separate systems, despite their nearly identical security processes. This duplication led to redundant maintenance and management efforts. Additionally, filling a dedicated position for SABHRS security proved difficult. Consequently, various other staff members maintained different parts of the security program, such as updating the security plan and ensuring compliance with the continuous monitoring program requirements.

Our original audit of SABHRS resulted in two recommendations to the department, both of which were met with concurrence. These recommendations were derived from concerns regarding the undefined security responsibilities associated with the SABHRS system, lack of management over SABHRS audit logs and the absence of a continuous monitoring strategy in alignment with the State's Continuous Monitoring Plan.

**Audit Follow-up Results**

During the follow-up, we worked to find out more information on the department's efforts to fill the SABHRS Information Systems Security Officer (ISSO) role. We interviewed SABHRS HR and FS staff, as well as SITSD Risk Management Bureau (RMB) personnel responsible for aspects of SABHRS security. At the end of the follow-up, SITSD informed us that they had assigned an internal ISSO to SABHRS security. In addition to identifying key personnel, we were provided a document that fully documents SABHRS responsibilities between the department's SABHRS and SITSD staff.

We also followed up on the expanded capture of SABHRS audit log information and the configuration of notifications in alignment with a continuous monitoring process. We found that the department captures audit log information sufficient to enforce administrative accountability for SABHRS FS, but lacks this capture for SABHRS HR. Additionally, notifications for audit log manipulation events did not exist. The department noted these opportunities and informed us that additional work was still required to satisfy this recommendation.

The following sections discuss our recommendations and the department's progress in designating a dedicated SABHRS ISSO, formally documenting SABHRS security responsibilities for both divisions, improving audit log management, and implementing a continuous monitoring plan.

**Recommendation #1**

***We recommend the Department of Administration formally document and fulfill SABHRS information security responsibilities for both divisions.***

***Implementation Status – Implemented***

As part of the audit work, we focused on the IT management of SABHRS and its IT personnel within the HR and FS divisions that support the system. We found that the department did not have an individual responsible for day-to-day SABHRS information security operations:

- The maintenance and assessment of general IT controls for the system
- Maintenance of system security documents
- Development of a SABHRS security program that aligns with State requirements for a system to operate on the State network

Based on this finding, we recommended that the department designate a full-time employee to fulfill the responsibilities of SABHRS security and formally document them to support both the HR and FS divisions.

Prior to follow-up, the department had assigned three SITSD RMB Information Security Specialists to handle SABHRS security. RMB staff discussed spending time on SABHRS weekly for these responsibilities. During the follow-up, the department attempted to hire a dedicated SABHRS ISSO for day-to-day security management. However, due to slow progress in filling this role, the department eventually assigned an internal ISSO to SABHRS security by the end of the follow-up. After this assignment, the department provided a document delineating security responsibilities between RMB staff

and SABHRS HR and FS personnel, which was updated to include the new ISSO role.

Given these actions taken by the department, we have determined that this recommendation has been implemented.

**Recommendation #2**

***We recommend the Department of Administration improve management of the SABHRS audit logs and implement the State's Continuous Monitoring Plan as part of SABHRS system security planning and security program.***

***Implementation Status - Being Implemented***

Original audit work identified that SABHRS database administrators had unrestricted access to the SABHRS audit logs and monitoring of these logs was not in place. Therefore, the department did not have a continuous monitoring strategy in place that was in alignment with state requirements.

These findings introduced concern for administrative accountability as the database administrators would have the opportunity to conceal their actions within the system. Due to this, the expansion of captured audit log information and the active monitoring of these logs were cited as areas of opportunity for improvement in the original audit report.

We followed up on the expanded capture of log information to enforce administrative accountability. During interviews with SABHRS HR, FS, and SITSD RMB staff, we could not identify any additional audit log information being captured. We then contacted SABHRS FS database administrators, who indicated that a change in SABHRS audit log information capture occurred at the end of 2023, and SITSD staff provided evidence of this change. Initially, the evidence only applied to FS and did not include HR. Towards the end of the follow-up, the agency confirmed that these logs were now being captured for HR as well.

To verify the monitoring implementation for captured audit information, we followed up with SABHRS and SITSD staff. SITSD personnel indicated that they are working on rolling out dashboards to FS and HR management to improve visibility and monitoring by providing access to all events within the ingested logs. Although these dashboards were still in development at the follow-up's conclusion, SITSD staff indicated that current reports are reviewed weekly. Throughout the follow-up, the department and SITSD staff indicated that there is only one notification configured, alerting the system administrator of errors in data capture but not for events indicative of audit log manipulation. The department is aware of this limited configuration and indicated they are working to identify and configure additional notifications.

The department has made some progress toward capturing and monitoring expanded audit log information. However, a complete process has not been implemented. Given these circumstances and the progress currently being made by the department, we have determined that this recommendation is currently being implemented.