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: Deborah Stratman, Associate Information Technology Auditor

CC: Department of Administration
Misty Ann Giles, Director
Kevin Gilbertson, Chief Information Officer
Michele Snowberger, Deputy Chief Information Officer
Chris Santucci, Chief Information Security Officer

DATE: March 2024

RE: Information Systems Audit Follow-Up (23SP-17): *eGovernment Series: Security Consolidation* (orig. 20DP-04)

Introduction

The *eGovernment Series: Security Consolidation* (20DP-04) report was issued to the Legislative Audit Committee in June 2022. The audit included one recommendation to the Department of Administration (DOA). In January and February 2024, we conducted follow up work to assess implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

The Department of Administration oversees IT planning and management within state government through its State Information Technology Services Division (SITSD). In January 2021, SITSD revised its statewide IT strategy, emphasizing the consolidation of State IT security operations under the state chief information security officer (CISO).

In January 2022, an audit examined SITSD's consolidation efforts thus far and the plan for completing this task. We found that SITSD lacked a comprehensive statewide strategy for security consolidation, leading to confusion among agencies regarding the consolidation process.

Following up on these findings, we observed that SITSD had integrated lessons learned from the initial consolidation efforts and developed a framework for future consolidation projects, implementing the recommendation outlined in the original audit.

Background

Montana has adopted electronic government service (eGovernment) to offer comprehensive solutions to its constituents, employing Internet applications to deliver specific services to citizens, businesses, and governmental entities. This approach enhances user convenience and yields efficiencies for the state and its customers.

Within DOA, SITSD is vital in delivering eGovernment services, acting as a facilitator and provider rather than merely a manager. Serving as a conduit for various stakeholders, including citizens, state agencies, and the Legislature, SITSD's goal is to offer standardized, strategic, secure, and state-of-the-art information technology to enhance government service delivery. To this end, SITSD seeks to centralize State security operations under the CISO.

Concerns regarding shared security responsibilities, security review of newly acquired eGovernment applications, and security consolidation's impact on eGovernment services prompted an audit of SITSD's security consolidation efforts. In the audit, we found that SITSD lacked a statewide strategy for security consolidation, resulting in confusion among agencies regarding the scope and requirements of the consolidation process.

Audit Follow-up Results

Follow-up work included multiple discussions about SITSD's efforts to consolidate security over the past 20 months. In October 2022, SITSD provided a Corrective Action Plan (CAP) that described how the CISO planned to implement the recommendation from the audit. The recommendation was not to complete security consolidation; rather, it required a comprehensive plan to complete this significant change. The CAP indicated that this plan would be complete by July 2023, and the original estimate was that security consolidation would be completed before July 2024.

Recently, there has been a change in the CISO, leading to the replacement of the CAP with a more comprehensive strategy. Implementing this strategy required additional staff, prompting SITSD to request additional full-time equivalent (FTE) positions from the Legislature during the 2023 Legislative Session, which was approved. Subsequently, a kick-off meeting between SITSD and state agencies took place in October 2023, marking the initiation of the project. The target milestone set for security consolidation at that time was June 30, 2024.

In January 2024, the IT Consolidation Advisory Committee convened its initial meeting with the objectives of:

- Defining its purpose and scope
- Examining the approach, milestones, and deliverables of the consolidation project
- Addressing any identified gaps or areas requiring additional staff support
- Outlining immediate next steps and action items

During this session, SITSD projected that the initial set of six agencies slated for consolidation would transition into the stabilization phase of the project by May 2024. However, SITSD is currently reassessing this timeline. Subsequent consolidation efforts for the remaining agencies will be planned and executed following the completion of the initial set.

The following section discusses our recommendation and the agency's progress toward implementing a comprehensive plan to increase the consolidation project's success.

Recommendation #1

We recommend that the State Information Technology Services Division (SITSD) reference appropriate frameworks and create a statewide security consolidation strategy prior to consolidating other agencies that includes:

A. Communication and change management plan,

B. Key performance indicators and measurable goals for success, and

C. Newly identified roles and responsibilities between agencies and SITSD via standard Memorandum of Understanding.

Implementation Status – Implemented

At the time of the audit, SITSD had taken over IT security and service desk operations for the Department of Labor & Industry (DLI) in an improvised manner. SITSD had not intended for this consolidation process to model the consolidation strategy that would be used for all other agencies; however, this raised doubt about the effectiveness of the process. SITSD did not effectively communicate the work's intent with DLI to the other agencies, who assumed that the consolidation with DLI was to be a roadmap of how future consolidation would progress. To ensure successful consolidation, SITSD needs to formulate a statewide strategy that clearly communicates changes, establishes and monitors consolidation objectives, and secures buy-in from involved agencies.

Since the audit, SITSD has analyzed the insights gained from its collaboration with DLI and crafted a framework for integrating IT security, service desk operations, and project management across various agencies. This framework encompasses:

- A communication plan
- A change management strategy
- A mechanism for establishing key performance indicators (KPIs) and tangible objectives for success between SITSD and the agencies undergoing consolidation.

Formal agreements such as Memoranda of Understanding (MOUs), Service Level Agreements, and Statements of Work are utilized to define and document the roles and responsibilities of both the agencies and SITSD.

SITSD also drafted a project charter to create a shared understanding of IT security consolidation's goals, objectives, and resource requirements. Within the project charter, SITSD defines the roles and responsibilities and provides success measures to achieve IT security consolidation objectives. While SITSD has set KPIs and measurable success criteria, the specifics are contingent upon conducting a security needs assessment for each agency throughout the consolidation process. Although its original target was to complete IT Security integration for its first agency by May 2024, SITSD knows adjustments to this timeline are necessary based on the initial evaluation of the current security landscape. Nonetheless, SITSD indicated a commitment to the endeavor even though it believes the project will take several years to complete.