LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

MEMORANDUM

TO:	Legislative Audit Committee Members
FROM:	Hunter McClure, Information Systems Auditor
CC:	Galen Hollenbaugh, Deputy Commissioner, Department of Labor and Industry George Parisot, Chief Information Officer, Technology Bureau Brenda Nordlund, Administrator, Unemployment Insurance Division
DATE:	April 2018
RE:	Information Systems Audit Follow-Up 18SP-04: Data Integrity of the Status, Tax Accounting, Audit, and Rating System (STAARS) - original 16DP-01
ATTACHMENTS:	Original Information Systems Audit Summary

Introduction

The *Data Integrity of the Status, Tax Accounting, Audit, and Rating System (STAARS) (16DP-01)* report was issued to the Legislative Audit Committee in September 2016. The audit included 11 recommendations to the Department of Labor and Industry (DLI). In January 2018, audit staff conducted follow-up work to assess implementation of the report recommendations. While progress has been made, there are some areas still in need of improvement. This memorandum summarizes the results of our follow-up work.

Overview

DLI uses STAARS to manage unemployment insurance tax collections from employers, and maintains data used to calculate unemployment insurance employers must pay, such as employee social security numbers and quarterly wages. An information systems audit, with the focus of data integrity, was conducted due to the sensitive information managed by STAARS and the need for complete data to ensure the accuracy of unemployment taxes and other programs that use this information. Audit work identified the need for improvements in user access management, data validations, and change control procedures. Our audit work contained 11 recommendations to DLI. Based on follow-up work, DLI has implemented 5 recommendations, partially implemented 3 recommendations, and is still working on implementing the other 3 recommendations. Overall, progress has been made to implement all 11 recommendations.

Background

DLI implemented STAARS in 2014 to replace an outdated mainframe system. It relies on STAARS to manage employer contributions of unemployment tax information, including employer registration, status, determination and rating, quarterly reporting and tax payments, collections and refunds, and employer auditing. The information is used by various divisions for labor statistics, wage verifications, and other metrics involved in determining UI tax rating. Information System audit work was completed in order to review data within the system, verify that current data validations used by the department are appropriate, review user access procedures, and review the change control process.

Audit Follow-Up Results

Follow-up work to determine the status of recommendations included system documentation, policy and procedure reviews, interviews with DLI staff, observations of system changes, and review of user access changes since the audit.

Progress is still being made in order to implement several of the audit recommendations, including DLI staff working to finish documentation and processes related to some of the recommendations. The following sections summarize the progress toward implementation of the report recommendations.

RECOMMENDATION #1

We recommend the Department of Labor and Industry:

A. Establish and document procedures for granting, reviewing, changing and terminating access, and

B. Define roles and responsibilities of staff involved in access management and document them within procedures.

Implementation Status – *Implemented*

Access management is the process of granting authorized users the right to specific system functionality, while preventing access to non-authorized users. Audit staff reviewed STAARS policy and procedure defining access management and found that it outlines requesting, adding, terminating, changing STAARS access, and defines the roles and responsibilities of staff involved in access management. A list of terminated users was obtained and all proper forms were present for each termination. A list of new users was also reviewed. Audit staff identified six individuals who did not have access forms. Three were added per a memorandum of understanding with Business Standards Division. The other three individuals were brought to the attention of DLI staff. DLI staff added the missing documentation; however, one of the access forms added did not have the user signature present. While this recommendation has been implemented through defining the proper procedures for access management, the department needs to continue efforts to ensure compliance with these procedures.

RECOMMENDATION #2

We recommend the Department of Labor and Industry:

A. Clearly define and document activities the user is allowed to carry out based on the function and which function or role each position should have.

B. Review the functions assigned to each group on a periodic basis to ensure appropriateness as business process and system changes occur.

Implementation Status – *Being Implemented*

Ensuring each function within the system is clearly defined allows DLI staff to enforce least privilege and other important access security standards. Due to access being assigned at the role level, or group of functions, it is important to know what functions are assigned to each role and review these to ensure accuracy. Since the audit, new policy for reviewing STAARS access has been created. This policy dictates that each group's functions be reviewed on a periodic basis. The original audit found some functions assigned to certain groups were excessive and unnecessary. These issues have been resolved within STAARS. DLI staff have also made progress by going through each function and role within the test environment and determining what each function allows a user to do and this is an ongoing process. DLI staff anticipate completion in summer 2018.

RECOMMENDATION #3

We recommend the Department of Labor and Industry:

A. Create documentation of and enforce segregated processes within the system, and

B. Implement a process to monitor privileged functions including areas where segregation cannot be maintained and users have access beyond their business need.

Implementation Status – *Being Implemented*

Having clear segregation of duties ensures that no single user can circumvent a critical process in the system, like submitting and approving refunds or audits. A review of Audit and Refund functions identified that DLI has reduced the number of users in the audit and refund areas. They are currently working on a notification system. The system would notify both Helena based supervisors and the DLI Bureau Chief if a refund was added and approved by the same individual. DLI is currently working to strengthen internal procedures for manually monitoring the checks and warrants that go out by having a 3rd party review and complete the mailing. DLI is also considering systematic monitoring of refunds and approvals. DLI is still working on the documentation of processes requiring segregation. They are considering using a report to monitor functions that cannot be segregated. DLI is also looking into creating work items in STAARS or having policy and procedure outside of STAARS that would review/monitor the actions. The anticipated completion of system enhancements is June 30, 2018.

RECOMMENDATION #4

We recommend the Department of Labor and Industry increase systematic and manual controls related to NAICS code, custom interest rates, payment agreement abatements, and tax rate changes.

Implementation Status – *Partially Implemented*

Ensuring important data is entered correctly and changes are verified and accurate increases accuracy of data and reduces risks of user errors within the system. Audit staff reviewed the system change request to standardize the North American Industry Classification System (NAICS) code input validations throughout STAARS. The change process shows that a control was put in place to ensure only valid NAICS codes are accepted. There was an additional control put in place that would create a notification when NAICS code is changed. DLI is currently reviewing options for enhanced tax rate change controls within STAARS. DLI would like to implement a double check for the enhanced tax rate change controls. When a tax rate change is made, a notification would automatically be sent out that night via email to supervisors within the department. The department only partially concurred with the recommendation, so no changes have been pursued for custom interest rates and payment agreement abatements. Audit staff still believe systematic or manual controls need to be applied to custom interest rates and payment agreement abatements. Abatements and custom interest rates are used to calculate penalty rates during the collection process when an employer fails to pay taxes in a timely manner. Due to the importance of the assessment of interest and penalties, strong control over the process to change them is necessary to ensure they are done accurately.

RECOMMENDATION #5

We recommend the Department of Labor and Industry:

A. Increase validation and processes concerning invalid and incorrect SSNs, blank last names, and NAICS codes used in rating, and

B. Document these validations and the procedures used to remediate any identified errors.

Implementation Status – *Implemented*

Without effective validations, incorrect data would be allowed in the system and could impact data used for work statistics and shared with other state agencies. Procedural documentation was updated for validating

Social Security Numbers (SSNs) and blank last names. DLI staff created additional input edits in STAARS to disallow any known invalid SSN. A report of wage records containing missing last names was developed and a process for reviewing and updating the wage records, where applicable, was implemented. This new process includes a random selection of manually entered wage records that are verified each quarter.

RECOMMENDATION #6

We recommend the Department of Labor and Industry upgrade the encryption software on field representatives' laptops.

Implementation Status – *Implemented*

DLI staff in the field need access to employee data, including SSNs, in order to complete work. When access to the system is unavailable, data is pulled from the system beforehand and used in spreadsheets that are stored in a secure drive on field representatives' laptops. Having an unsupported encryption software is a vulnerability to the security of data, which includes SSNs and employment information. DLI had indicated that the encryption software on all field laptops was upgraded to a solution supported by the State Information Technology Services Division (SITSD). Documentation provided by DLI showed that all field representatives' laptops have been upgraded.

RECOMMENDATION #7

We recommend the Department of Labor and Industry obtain or develop complete, detailed system documentation that defines:

A. Processes managed by the system and how users should interact with the system during these processes, and

B. How the system is expected to function throughout these processes, including any validations or configurations.

Implementation Status – *Being Implemented*

Proper system documentation improves user understanding of how the system should work and reduces associated risks with improper use. The department only partially concurred with this recommendation, disagreeing on the level of detail recommended regarding the vendor proprietary documentation. During review, DLI staff explained that they are not receiving any more system documentation from the original contractor. Due to this, DLI is having each team and supervisor work on developing policy and procedure. These documents will then be put into the help function within STAARS. Examples of completed policies and procedures were given to audit staff. DLI estimates completing this in December 2018.

RECOMMENDATION #8

We recommend the Department of Labor and Industry comply with access management policy by documenting and implementing procedures to grant, review, and terminate access to the change control system.

Implementation Status – *Implemented*

Access to the change control system is just as important as access to STAARS because it manages how STAARS operates through automating the change control process. Audit staff reviewed the access policy for the change request system. This policy gives guidance on access and documents procedures to grant, review, and terminate access to the change control system. Audit staff also reviewed the process implemented to review access. Audit staff found that DLI is following procedure and conducting access review for the change control system annually (per policy).

RECOMMENDATION #9

We recommend the Department of Labor and Industry develop controls to ensure:

A. The person creating the migration is not allowed to also approve the migration, and

B. Department staff review changes being made by contractors.

Implementation Status – *Implemented*

Having segregation of duties in place ensures that proper changes are approved and moved to production and helps prevent unauthorized changes to the system. During the audit, DLI had a policy in place regarding migrations to the STAARS production environment but the audit identified instances when it was not followed. Audit staff reviewed the migration policy and procedure that DLI communicated to all contracted personnel as well as internal developers. The policy states that the person approving the migration should not be the same person who submitted the migration and that the approver should be a member of the state agency, as opposed to contracted personnel. Audit staff sampled migrations since implementation of this policy and identified no instances where the same individual approved and submitted a migration and found that DLI staff approved all of the migrations. The migration policy mentions situations where an individual would need to submit and approve their own migration due to time constraints, emergencies, etc. A migration report is automatically emailed from STAARS to the technical and business teams leads every night. This report would show if an individual approved and submitted the same migration. DLI staff would then be able to follow up if there were any discrepancies in the report.

RECOMMENDATION #10

We recommend the Department of Labor and Industry develop a formal change control document that clearly defines all necessary components of its change control process.

Implementation Status – *Partially Implemented*

Change control helps ensures that no unauthorized changes are made and that services are not unnecessarily disrupted. Clear documentation of the expectations of the process are important to identify risks and ensure consistency. Audit staff reviewed the updated change control policy and procedure for STAARS. DLI did update this policy; however, the policy is missing aspects mentioned in the original audit. Sections needing further definition that were identified in the original audit include: defining the responsibilities of contractor and Technology Services Division managers, a process to update documentation and configuration, classification definitions, the prioritization process, and post implementation review.

RECOMMENDATION #11

We recommend the Department of Labor and Industry establish and monitor expectations for changes and modifications to STAARS.

Implementation Status – *Partially Implemented*

Having proper expectations for change control helps ensure that resources are used efficiently. DLI reviewed the STAARS change requests completed for the past fiscal year. Staff explained that a report was created to analyze completion of closed change requests. While this report is available, there is no process in documentation to use the report. The STAARS change control policy created from the previous recommendation outlines the expectations for changes for STAARS. However, this document does not address post implementation review related to expectation monitoring. This recommendation could be improved by requiring DLI to formally document change request review procedures.