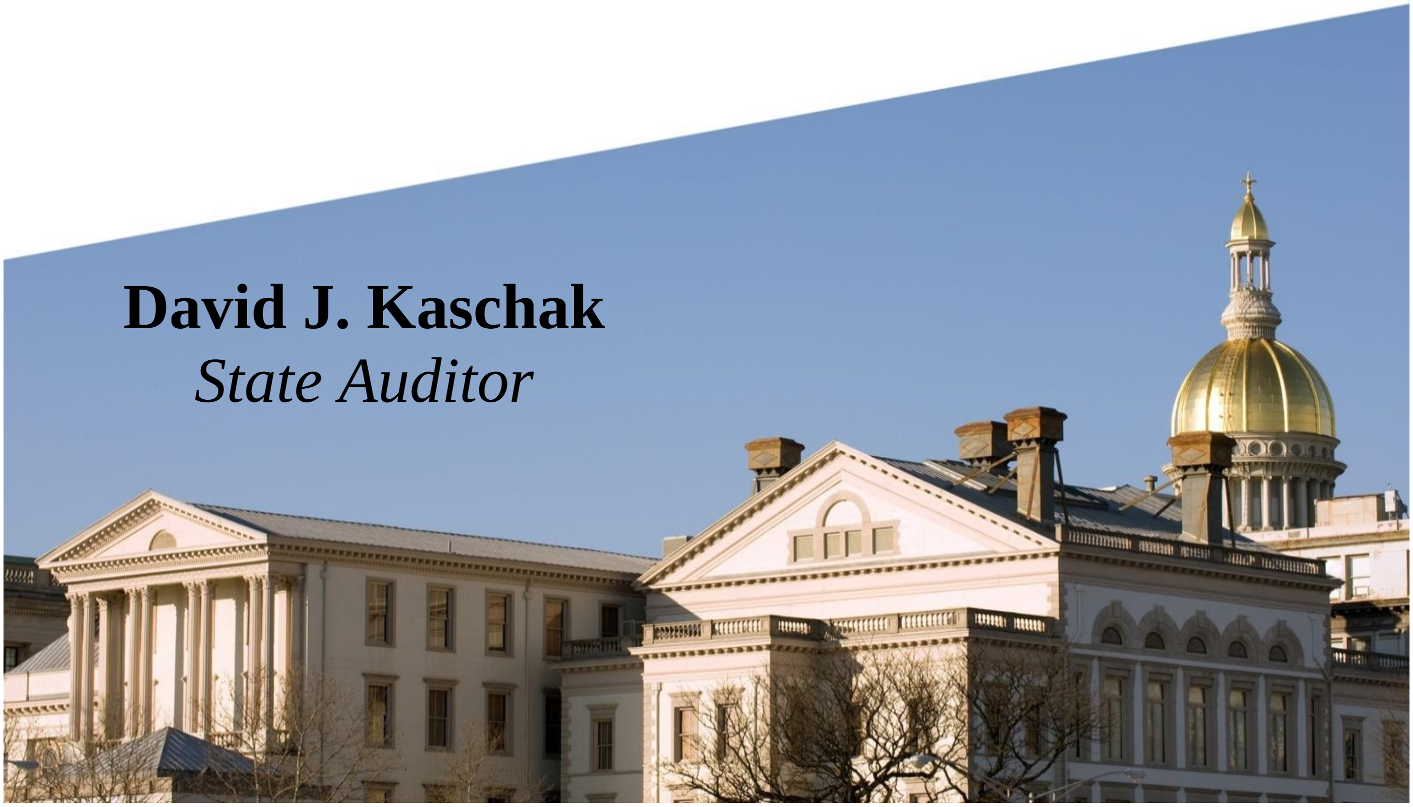
New Jersey Legislature

★ Office of LEGISLATIVE SERVICES ★

OFFICE OF THE STATE AUDITOR

Department of the Treasury
Division of Taxation
Taxpayer Unremitted Liability Inventory Plotting System (TULIPS)
and the Generic Tax System (GENTS)

April 23, 2018 to August 31, 2020



David J. Kaschak
State Auditor

NEW JERSEY STATE LEGISLATURE
★ *Office of* LEGISLATIVE SERVICES ★

OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN ST. • P.O. BOX 067 • TRENTON, NJ 08625-0067
www.njleg.state.nj.us

OFFICE OF THE
STATE AUDITOR
609-847-3470
Fax 609-633-0834

David J. Kaschak
State Auditor

Thomas Troutman
Assistant State Auditor

The Honorable Philip D. Murphy
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Craig J. Coughlin
Speaker of the General Assembly

Ms. Peri A. Horowitz
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of the Treasury, Division of Taxation, Taxpayer Unremitted Liability Inventory Plotting System and the Generic Tax System for the period of April 23, 2018 to August 31, 2020. If you would like a personal briefing, please call me at (609) 847-3470.

David J. Kaschak

David J. Kaschak
State Auditor
March 24, 2021

Table of Contents

Scope 1

Objectives 1

Methodology 1

Conclusions 2

Background 2

Findings and Recommendations

Logical Access – Authentication 3

Change Management 5

Contingency Planning 6

Auditee Response 8

Scope

We have completed an audit of the Department of the Treasury, Division of Taxation, Taxpayer Unremitted Liability Inventory Plotting System (TULIPS) and the Generic Tax System (GENTS), for the period April 23, 2018 to August 31, 2020. Our audit focused on selected general and application controls related to the applications including logical access, change control, disaster recovery and business continuity, and select areas of data integrity.

Objectives

The objective of the audit was to determine if the general and application controls related to the TULIPS and GENTS applications are appropriate and properly functioning to ensure the confidentiality, integrity, and availability of the applications and their data.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional guidance for the conduct of the audit was taken from the *Federal Information Systems Control and Audit Manual* (FISCAM), published by the Government Accountability Office, as well as the *New Jersey Statewide Information Security Manual* (SISM), published by the New Jersey Office of Homeland Security and Preparedness. The SISM was used as the criteria against which controls were measured.

In preparation for our testing, we studied agency and statewide policies and procedures, and industry standards and best practices. Provisions we considered significant were documented, and compliance was verified by interviews of key personnel, review of application-related documentation, and other testing we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions on our audit objectives as well as internal controls and compliance. Sample items were judgmentally selected for testing.

We assessed the reliability of TULIPS and GENTS data by performing electronic testing, reviewing existing information about the data, testing the controls in the applications that produced it, and interviewing agency officials knowledgeable about the applications and the data. We determined that the data were sufficiently reliable for the purposes of this report.

Conclusions

Overall, we found that the Division of Taxation has appropriate general and application controls in place to ensure the confidentiality, integrity, and availability of the TULIPS and GENTS applications and their data. However, we noted areas for improvement in controls and processes that require management's attention regarding logical access, change control, and contingency planning.

Background

The Taxpayer Unremitted Liability Inventory Plotting System (TULIPS) has been the division's case management and tracking system for delinquent and deficient taxpayers and their tax liabilities since 1986. The Generic Tax System (GENTS) is the division's taxpayer account maintenance system and was implemented in 1988. Prior to July 2017, the Office of Information Technology (OIT) administered both applications; however, after the issuance of Executive Order No. 225 in 2017, the OIT programmers and analysts responsible for the TULIPS and GENTS applications were transferred to the Department of the Treasury, Division of Revenue and Enterprise Services (DORES). Since that time, DORES has administered both the TULIPS and GENTS applications. The Department of the Treasury, Division of Taxation (division) is the application and data owner of these applications.

The TULIPS generates approximately 1.7 million notices and completes 1.5 million cases annually with annual compliance collections estimated at $1.0 billion. The GENTS processes more than 10 million transactions totaling $31.2 billion annually. Each of these applications also interfaces with other internal Treasury systems as well as external agency systems.

Logical Access – Authentication

Access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. Logical access authentication controls require users to provide sufficient evidence of their identity before they are granted access to a system. Entities are responsible for managing authentication controls to ensure that only authorized users have the ability to access the system. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can read and copy sensitive data and make changes or deletions which may go undetected. Inadequate access controls can affect the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

The TULIPS and GENTS applications are part of the Division of Taxation's legacy tax system, TAXNET, which also includes two other applications that were not part of the audit scope. As of July 8, 2019, there were 2,023 authorized internal and external users of TAXNET having the ability to access the TULIPS and GENTS applications with varying privileges based upon their job responsibilities.

Separated employees' TAXNET user IDs were still active, and mainframe access was not removed in a timely matter.

We found that 54 user accounts listed as active in TAXNET with access to the TULIPS and/or GENTS applications were associated with individuals who separated from state service. Although active in TAXNET, if a user's mainframe (ACF2) account has been canceled, removed, or suspended, it would prevent the person from accessing the mainframe environment, which would prevent access to TAXNET. We tested these employees' ACF2 accounts to determine if they still had access to the mainframe environment and found that all 54 employees' ACF2 accounts had been canceled, removed, or suspended as of the date of our testing. While all 54 accounts had been successfully canceled, removed, or suspended from ACF2, only 29 had a date attached to their ACF2 account suspension because accounts are removed from ACF2 after being in suspended status for a period of time. We compared these 29 user account suspension dates to the user's separation date and determined that 18 of the user accounts were suspended more than 30 days after their separation date, with an average of 872 days between separation and suspension. Although the risk of not disabling the TAXNET user account could be mitigated by the ACF2 suspension, the ACF2 accounts are not being suspended immediately upon termination, thereby leaving a window where the separated employee could potentially access the TULIPS and GENTS applications.

The division is responsible for maintaining user access to TAXNET, which includes adding new users, modifying privileges for active users, and removing users who no longer require access. The SISM requires agencies to immediately revoke access to systems for any separated users, as well as review users' access rights at least every six months and maintain evidence that the reviews are completed.

Division personnel informed us that they perform a semi-annual review of active TAXNET users; however, our testing indicates that these reviews are not occurring every six months or are not covering all the necessary areas of access controls, and results are not being documented. If the review was being performed and was comprehensive, the accounts for the separated employees we noted would have been disabled or removed on a timelier basis from both TAXNET and ACF2. The division appears to be relying on the compensating control of the disabling of the ACF2 account after 90 days of inactivity.

Recommendation

We recommend the division review all active TAXNET user accounts and disable and/or remove all accounts for users that have separated from state service. The division should also develop and implement a process in accordance with the SISM to ensure that the accounts of future separated employees are disabled or removed immediately upon termination. Finally, the division should perform the required semi-annual review of user accounts in accordance with the SISM, and maintain evidence of the review.

⋙⋘

The division's logical access controls related to granting and modifying access to the TULIPS and GENTS applications need improvement.

When an employee requires new or modified access to TAXNET applications, an employee access form is completed and approved by the appropriate supervisor and sent to the TAXNET help desk. During the audit period, these forms were moved from paper to digital retention by the division's Data Systems area. When we received access to the forms, we observed that the division did not follow a naming convention for these files, which made it difficult to identify an individual's employee access form.

We tested all 14 employees who were added to TAXNET during our audit period and given an approval authority for more than $100,000 in refund or credit areas. We tested these employees for properly completed and approved employee access forms, and to ensure the forms were retained. For 8 of the 14 employees, the access form could not be located. The remaining six forms were properly completed, approved, and retained; however, one of the users was incorrectly assigned an approval level far above what was requested because of a data entry error.

The SISM states that agencies are responsible for proper controls related to the addition, deletion, and any modification of user IDs. This includes retaining the authorization forms as proof of proper modifications. The missing access forms make it difficult to determine if access was appropriately approved and applied.

Recommendation

We recommend that the division create a naming convention for the digital access forms which will make managing user access forms easier and ensure that all forms are retained, as well as allow for easier review to identify and correct errors.

»»➤««

Change Management

The SISM states that asset custodians and data/process owners are required to follow change control processes and procedures for all system changes, including those performed by both internal and external developers. Change control includes a wide range of activities including the establishment of a formal change management process; proper authorization and approval of all changes; development, documentation, and approval of comprehensive test plans and testing; and retention of an audit trail for all changes. The goal of change management is to prevent unnecessary or unauthorized changes, assess the impact of changes on the environment, and maintain necessary documentation of all changes.

The division's change management procedures should be improved and properly documented.

We requested from the division their change management procedures and were informed that there were no formally documented procedures. The division was, however, able to verbally describe the process, as well as provide support of the use of this process through various documents provided during our testing. Based on the information provided to us regarding the change management process, we tested all 22 open GENTS or TULIPS application change requests. We found that 4 of these requests had not been approved by an appropriate officer of the Small Project Prioritization Committee (responsible for approving changes), and of the remaining 18 change requests, 17 were authorized and approved by the same individual.

The SISM reinforces segregation of duties by instructing agencies to ensure that individuals who request authorization to carry out a task are distinct and separate from those who approve the request. Doing so helps mitigate the risk of an unauthorized or improper change being made to the application.

Recommendation

We recommend the division review its current change control process and ensure that proper segregation of duties, proper authorization, and other necessary controls are in place to protect the application from unauthorized, unapproved, or improper changes. Once completed, the division should document a formal procedure and distribute it to all relevant staff.

»»➤««

Contingency Planning

The TULIPS and GENTS applications have aspects of contingency planning that are either outdated or missing.

Contingency planning consists of technical and operational aspects. The technical aspects are the processes connected to backing up and restoring an information technology system to a ready state with minimal loss of time, functionality, and data. The operational aspects are the processes and procedures that are used to put the agencies' employees and customers in a position to resume normal operations. We found that the TULIPS and GENTS applications had deficiencies in both the technical and operational aspects of contingency planning.

The OIT performs quarterly tests of the underlying mainframe infrastructure that supports both the TULIPS and GENTS applications. This test is performed on the backup mainframe and includes activating the application, which requires the hardware and the underlying application to be restarted and brought to a ready state. In addition, agencies can request that their application be exercised (restored to a point in time requested by the agency). At that point, the agency can access the application to perform planned tasks, including running mainframe application jobs and manipulating data, to validate that the recovered application is performing as expected. In order to exercise the application, the agency must coordinate with OIT disaster recovery personnel to build an exercise plan, which would have the requirements needed. The OIT confirmed to us that the TULIPS and GENTS applications have not been exercised by the division.

With regard to the operational aspects, the division's business continuity plan (BCP) was completed in 2009, and upon review we found that the plan had outdated information, including critical personnel contacts and technology requirements in the event of a disruption. In addition, the plan referenced another BCP plan which was incomplete at the time. The OIT also conducts a business impact analysis (BIA) for major IT systems it supports. The BIAs for the TULIPS and GENTS applications were completed in 2009. Since then, the OIT has updated and modified the process to include new information to reflect the changing computing landscape. Based on the completion of the BIA, the OIT performs a risk assessment. During the audit, the division stated that the OIT was in process of obtaining updated BIA information for all systems that had not been reviewed in the previous two years, which includes the TULIPS and GENTS applications.

The SISM states that agencies should review contingency plans at least annually and update the contingency plan to address changes to the agency, system, or environment of operation. In addition, agencies should test the plans to determine their effectiveness and document the test results. Failure to have current contingency plans or to test the recovery and restoration of the TULIPS and GENTS applications and data increases the risk that response to, and recovery from, an incident will not meet objectives. Any resulting service outages due to insufficient and untested plans would impact the ability of the division to perform essential functions for the state.

Recommendation

We recommend that the division work with the OIT to perform an exercise of the TULIPS and GENTS applications which includes recovery of the data and execution of mainframe jobs to validate that the recovered application is functioning as expected, document the results, and provide corrective action as necessary for deficiencies identified. In addition, the division should update its business continuity plan, including and coordinating information from the OIT business impact analysis.

State of New Jersey

DEPARTMENT OF THE TREASURY
DIVISION OF TAXATION
P. O. BOX 240
TRENTON, NEW JERSEY 08695-0240

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

ELIZABETH MAHER MUOIO
State Treasurer

JOHN J. FICARA
Acting Director

March 16, 2021

Thomas Troutman, Assistant State Auditor
Office of the State Auditor
125 South Warren Street, PO Box 067
Trenton, NJ 08625-0067

Dear Mr. Troutman:

We appreciate the opportunity to respond to the recommendations contained in the audit report for the Department of the Treasury, Division of Taxation, Taxpayer Unremitted Liability Inventory Plotting System (TULIPS) and Generic Tax System (GENTS) for the period April 23, 2018 to August 31, 2020.

Working in conjunction with our colleagues at the Division of Revenue and Enterprise Services (DORES), we have already taken significant action on the report's recommendations, including instituting several control measures upon initial notification. The following summary highlights our efforts to date and the actions we plan to undertake this calendar year.

Logical Access, Authentication

Recommendation: We recommend the division review all active TAXNET user accounts and disable and/or remove all accounts for users that have separated from state service. The division should also develop and implement a process in accordance with the SISM to ensure that the accounts of future separated employees are disabled or removed immediately upon termination. Finally, the division should perform the required semi-annual review of user accounts in accordance with the SISM, and maintain evidence of the review.

Response: The Division of Taxation has taken the necessary action to ensure that TAXNET user access is removed for all separated employees immediately upon notification by Treasury – Human Resources. In addition, the Division currently reviews all TAXNET user accounts and will continue to do so on a semi-annual basis as a quality control measure.

Recommendation: We recommend that the division create a naming convention for the digital access forms which will make managing user access forms easier and ensure that all forms are retained, as well as allow for easier review to identify and correct errors.

Response: The Division of Taxation believes that the transition from a paper process to an electronic process may have contributed to the misplaced documents. A new internal naming convention process, including a filing system, has been adopted to manage the electronic user access forms so that requests can be easily tracked.

Change Management

Recommendation: We recommend the division review the current change control process and ensure that proper segregation of duties, proper authorization, and other necessary controls, are in place to protect the application from unauthorized, unapproved, or improper changes. Once completed, the division should document a formal procedure and distribute it to all relevant staff.

Response: As demonstrated by our office during our meeting, DORES has implemented a new Application Development Portal that includes a structured or standardized change control process (which has also been documented). The change control process features an automated change request submission module along with workflow-controlled request approval and staff assignment processes. Collectively, these features help to protect the applications from unauthorized, unapproved, or improper changes. The Portal also provides for request status tracking and dashboard views of work in progress. Authorized end user representatives will be able to view the dashboard. Finally, the Portal is self-documenting.

The programmer analyst team that supports TULIPS and GENTS now uses this Portal to manage its work requests.

Contingency Planning

Recommendation: We recommend that the division work with the OIT to perform an exercise of the TULIPS and GENTS applications which includes recovery of the data and execution of mainframe jobs to validate that the recovered application is functioning as expected, document the results, and provide corrective action as necessary for deficiencies identified.

Response: It appears that the recovery test process was not transitioned to DORES during the transfer of the TAXNET support team to the Department of the Treasury in 2017. Accordingly, DORES has been in contact with OIT. They confirmed that TULIPS and GENTS are part of OIT's quarterly IBM mainframe disaster recovery test. Both systems are tested in a passive/non-production mode. To be in line with the recommendation, we requested to move the test to a production model, which includes testing jobs and data.

Recommendation: In addition, the division should update its business continuity plan, including and coordinating information from the OIT business impact analysis.

Response: The Division of Taxation's Continuity of Operations plan was last updated in March 2020 and is actively being reviewed to include information from the OIT business impact analysis once the information is available.

We thank you for your input and appreciate the professionalism that your staff brought to the engagement.

Very truly yours,

John J. Ficara
Acting Director
Division of Taxation

C: State Treasurer, Elizabeth Maher Muoio