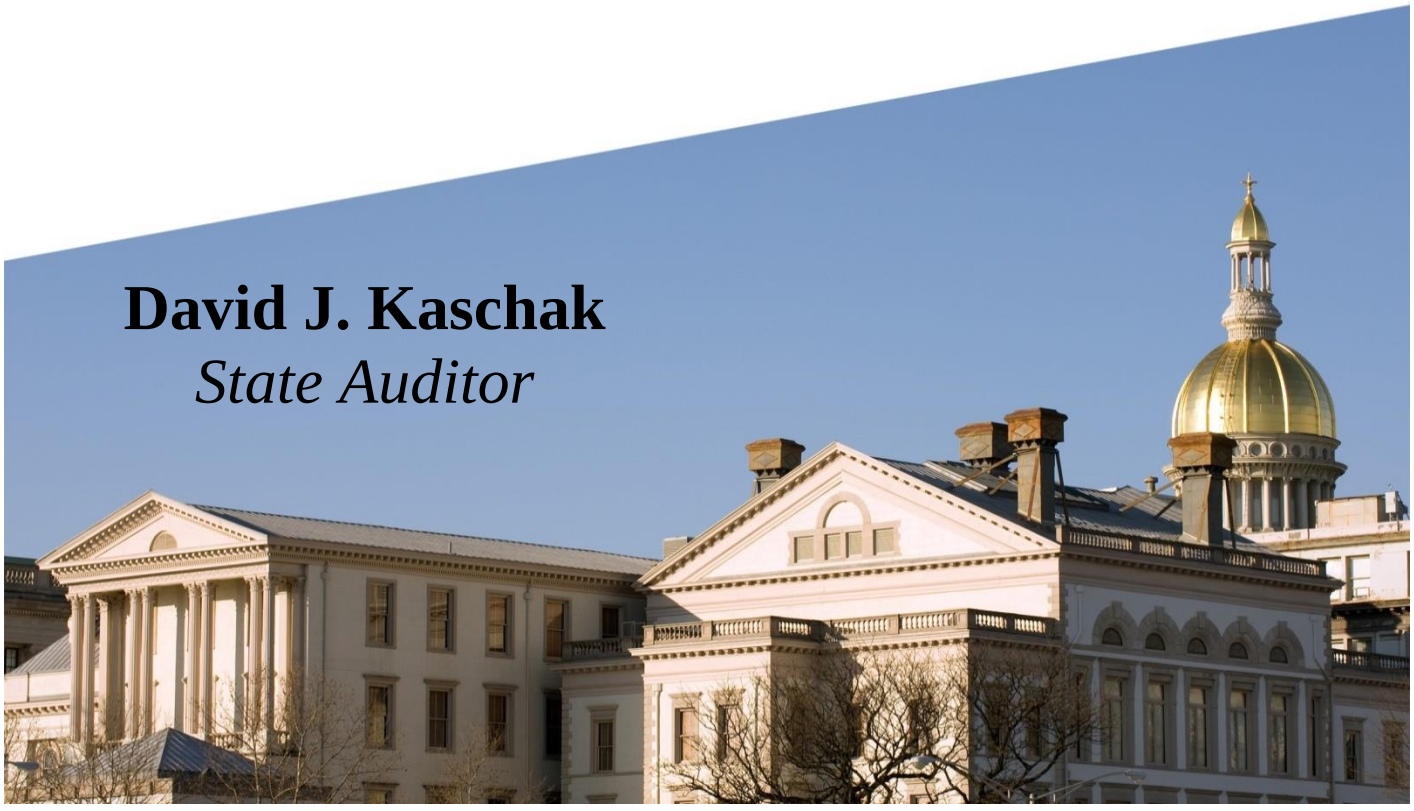
New Jersey Legislature

Office of LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR

Department of the Treasury
Division of Purchase and Property
New Jersey State of The Art Requisition Technology (NJSTART) Information Technology Application

February 4, 2019 to July 31, 2020



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

Brian M. Klingele
Assistant 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 Purchase and Property, New Jersey State of The Art Requisition Technology (NJSTART) information technology application for the period of February 4, 2019 to July 31, 2020. If you would like a personal briefing, please call me at (609) 847-3470.

David J. Kaschak
State Auditor
May 27, 2021

Table of Contents

Scope

We have completed an audit of the Department of the Treasury, Division of Purchase and Property, New Jersey State of The Art Requisition Technology (NJSTART) information technology application for the period February 4, 2019 to July 31, 2020. The scope of our audit included logical access, change control, disaster recovery and business continuity, system interfaces, and system effectiveness.

Objectives

The objective of the audit was to determine if the general and application controls related to the NJSTART application are appropriate and working properly to ensure the confidentiality, integrity, and availability of the application and its data. An additional objective was to determine the effectiveness of the application in meeting the state's purchasing needs.

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 Audit and Control 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 legislation, 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 performance of other tests we considered necessary. A non-statistical sampling approach was used. Our samples were designed to provide conclusions on our audit objectives, as well as internal controls and compliance. Sample populations were judgmentally selected for testing.

Conclusions

Overall, we found that the Division of Purchase and Property has established general and application controls in place to ensure the confidentiality, integrity, and availability of the

application and its data. However, we noted areas where these controls are not functioning effectively, and require management's attention. In addition, our audit identified aspects of the development and implementation of the NJSTART application that have created issues in meeting the purchasing needs of all state agencies. We are presenting these items in an observation at the end of the audit report.

Background

The Division of Purchase and Property (DPP or division) within the Department of the Treasury, was created under N.J.S.A. 52:18A-3 and serves as the state's central procurement agency. The division's mission is to professionally and ethically procure the best valued products and services in a timely and cost effective manner in accordance with state laws and regulations to enable client agencies to meet their objectives.

The NJSTART application is a commercial off-the-shelf Software-as-a-Service (SaaS) application developed by a contracted vendor. SaaS is a software licensing model which allows access to software on a subscription basis using external servers. The DPP does not manage or control the underlying cloud infrastructure or the application code. NJSTART was purchased in 2012 and was first made available to the state's vendor community in 2014. In June 2016, the system was made available to agency procurement specialists for contract administration.

DPP procurement specialists use NJSTART to track the progress of request for proposals (RFPs) to the contract award. Agencies use the system to create purchase orders and approve invoices for payment. Vendors use the system to create their vendor profile, submit bid proposals, and store various state-required compliance documents. Local municipalities use the system to view vendor compliance forms and available contract documents.

The application is accessible to most state purchasing agents and vendors through permissions assigned to their myNJ portal accounts. Agency staff use a pass-through authentication method that allows them to access NJSTART after successful login to the myNJ portal without a secondary log in. In addition, DPP employees can access the application through a web-based program interface. The DPP staff is responsible for managing access to the application, and the using agency's Organization Administrator (OA) determines the roles to be assigned within the respective agency.

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 users who are supposed to access the system have the ability to do so. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can read and copy sensitive data and make changes or deletions that could go undetected. Inadequate access controls also diminish the reliability of computerized data and increase the risk of inappropriate disclosure or destruction of that data.

In each agency that utilizes NJSTART, the OA for the agency is responsible for user account maintenance. Included in this maintenance is the creation, modification, suspension, and removal of user accounts within the guidelines of the SISM, which governs information security practices in the executive branch of government. At the time of our testing, NJSTART had 44,221 vendor accounts, of which 43,918 were active, and 4,909 user accounts, of which 3,815 were active.

Separated employees have active access to the NJSTART application.

Our analysis of the 3,815 active NJSTART user accounts found 476 belonging to employees who have separated from state service. Of those, 286 accounts had no last login date, which indicated they had never been used. We further analyzed the 190 accounts that did have a last login date to determine if the account had been accessed after the individual's separation date and found 67 accounts having a last login date after their separation date. The average number of days after separation that the account was accessed was 311 days, with the longest period between separation and access being 1,681 days. We matched the 67 accounts which had accessed the NJSTART system after their separation date with the purchase order, receipt, and invoice transactions dated during the audit period and found two accounts that were attached to at least one aspect of a transaction where the date of that aspect of the transaction was after the user's separation date. For the remaining 65 users, we were unable to determine what actions these accounts had taken after logging in because the NJSTART application only stores seven weeks of history of complete account activity in its logs, and none of those 65 accounts had a last login that was within seven weeks of the completion of our analysis.

According to the SISM, agencies are responsible for ensuring proper user identification and authentication management for all standard and privileged accounts on systems, which includes immediately revoking access for any terminated users. DPP personnel stated that the OAs of the different agencies that use the NJSTART application are responsible for adding and removing users for their organization; however, the results of our analysis demonstrate that OAs are not removing employee access upon separation from employment.

The use of the pass-through authentication method through the myNJ portal for NJSTART access by a large number of users makes the removal of user accounts in NJSTART even more important

because the myNJ portal does not have password expiration implemented, therefore the myNJ portal account will not be disabled automatically. Active user accounts belonging to separated employees could be used to improperly access and use the system.

Recommendation

We recommend the division perform a review of all users in the NJSTART application, work with the agencies to identify separated employees, and remove their access. In addition, the division should communicate the requirements and procedures for removing access for separated employees to the agency OAs, and monitor the agencies' compliance through periodic reviews.

⋙➤◀⋘

NJSTART users who transferred to other agencies retained access to their previous agency.

We identified 51 active accounts belonging to employees who had transferred to another state agency and whose account access to their previous agency was still assigned. Of those, 14 accounts had no last login date, which indicated that they had never been used. We further analyzed the 37 accounts having a last login date and found that 28 had been logged into after the user's date of transfer. The average number of days after transfer that these accounts were accessed was 364 days, with the longest period between transfer and access being 1,438 days. We matched the 28 accounts which had accessed the NJSTART system after their transfer date with the purchase order, receipt, and invoice transactions dated during the audit period to determine if they were associated with any aspect of a transaction in their old organization after their transfer date. We found four accounts that were attached to at least one aspect of a transaction for their previous organization where the date of that aspect of the transaction was after the user's transfer from that organization. For the remaining 24 users, we were unable to determine what actions these accounts had taken after logging in because the NJSTART application only stores seven weeks of complete account activity in its logs, and none of the 24 accounts had a last login that was within seven weeks of the completion of our analysis.

In addition, we found 11 user accounts where we could not match the user's name with anyone having worked for the agency to which they were assigned in NJSTART. Eight of these accounts had been accessed. We matched the eight accounts which had accessed the NJSTART system with the purchase order, receipt, and invoice transactions dated during the audit period to determine if they were associated with any aspect of a transaction and found one account that was attached to at least one aspect of a transaction. For the remaining seven users, we were unable to determine what actions these accounts had taken after logging in because the NJSTART application only stores seven weeks of complete account activity in its logs, and none of the remaining seven accounts had a last login that was within seven weeks of the completion of our analysis.

Although agency OAs have the ability to disable users within their agency, DPP personnel stated that only the DPP has the ability to change the person's associated approval organization, after a

request from the agency. We found no formal process documented for this. Active accounts with access to transactions in other agencies could allow for unauthorized access by the account owner or by someone else using the account.

Recommendation

We recommend the division perform a review of all users in the NJSTART application, work with the agencies to identify transferred employees, and ensure that access to their previous agency is removed. The division should also communicate the requirements and procedures for handling transferred employees to the agency OAs, and monitor the agencies' compliance through periodic reviews. In addition, the division should work with agency OAs to review the users we identified who were not associated with their agency.

Accounts created and never used are not being disabled after 30 days.

The SISM defines the requirement to disable a user account if the initial password is not used within 30 days. We identified 1,145 active user accounts having no last login date, indicating that they had never accessed the application. The NJSTART application maintains a record of the last date in which the account was altered for any reason (including creation of the account), and based on that date we determined that 1,139 (99 percent) of these active user accounts had been outstanding (not accessed) more than 30 days and should be disabled and/or removed. We aged these accounts by the date last altered and found:

- 144 user accounts had been outstanding one year or less,
- 106 user accounts had been outstanding between one and two years,
- 102 user accounts had been outstanding between two and three years,
- 51 user accounts had been outstanding between three and four years, and
- 736 user accounts (65 percent) had been outstanding more than four years.

The 736 user accounts outstanding more than four years includes the time before the application was rolled out to state agencies for pilot. Prior to commencing operations of the application for the agencies, the DPP requested that agency OAs review, edit, and update their agency users' profiles. However, the number of users outstanding more than four years indicates that many agencies did not perform this review before rollout, and that none has been done since.

The Organization Administrator User Profile Maintenance Guide, created by the DPP, includes account management as a responsibility of each agency's OA(s). Although the guide includes

disabling users as an OA function, a lack of defined steps for disabling user accounts within the guide could have contributed to the difficulty of completing this task.

Recommendation

We recommend the division perform a review of all users in the NJSTART application and work with the agencies to identify and delete accounts that have never been accessed. In addition, the division should communicate the requirements and procedures for removing accounts that are created and not used within 30 days to the agency OAs, and monitor the agencies' compliance through periodic reviews.

Non-utilized User IDs are not being disabled and removed.

The SISM requires that user accounts should be disabled after 60 days of non-use. In addition, once an account has been disabled, it should be removed from the application after 90 days in the disabled status. Our analysis of the 2,670 active NJSTART user accounts having a last login date found that 1,476 (55 percent) should be either disabled (531) or removed (945) from NJSTART based on the time since their last login. These totals included 37 accounts with OA privileges and 13 users whose privileges are assigned to another user via proxy. We aged the 945 accounts that should have been removed based on the last login date, and found:

- 492 user accounts had been outstanding one year or less,
- 251 user accounts had been outstanding between one and two years,
- 149 user accounts had been outstanding between two and three years, and
- 53 user accounts had been outstanding longer than three years.

We found that the NJSTART application has the ability to purge users that are marked as disabled, which would automate the process of removing users (as long as they were disabled in accordance with the SISM); however, the DPP does not utilize this feature. In addition to the active users, we analyzed 401 NJSTART user accounts that are currently disabled, inactive, or locked, and found that 380 (95 percent) should be removed from the application because their last login date was more than 150 days old (60 days to be disabled and an additional 90 days to be removed).

Recommendation

We recommend the division perform a review of all users in the NJSTART application, and work with the agencies to identify and disable user accounts with a last login date older than 60 days, as well as identify and remove accounts that have been (or should have been) disabled for more than 90 days. In addition, the division should communicate the requirements and procedures for

disabling and removing user accounts reaching these thresholds to the agency OAs, and monitor the agencies' compliance through periodic reviews.

Some users in the NJSTART application have duplicate accounts.

The SISM requires agencies to identify and address redundant or duplicate IDs during their required periodic access reviews. Our analysis of the 3,815 active NJSTART accounts identified 39 duplicate accounts belonging to 33 different individuals. Two of these individuals had five active accounts each, though only one of the accounts had been accessed in these cases. Ten individuals had used both of their accounts, three of which were accounts for more than one agency based on a change of employment, and had used the account for the original agency after transfer. In one case, the access levels of the original user account were proxied to the agency OA, thereby giving the OA the authority of the person who is no longer employed there and creating a segregation of duties weakness. Duplicate accounts could allow users to have unnecessary access to application resources that may circumvent application controls.

Recommendation

We recommend the division perform a review of all users in the NJSTART application and work with the agencies to identify and remove unnecessary duplicate users. In addition, because only the DPP has the ability to view across all using organizations, it should include identifying duplicate accounts statewide during its periodic reviews.

Periodic reviews of user access to NJSTART are not being performed by either the DPP or the using agencies.

The SISM requires agencies to document and implement a formal process to periodically review users' access rights in order to maintain effective controls over user access to information assets. To maintain these controls, agencies are required to review user access to resources at least every six months and should retain evidence of the review. The review should specifically identify and revoke access for, or remove, the following:

- Active user IDs that are no longer needed;
- User IDs assigned to terminated users with active access;
- Generic or anonymous user IDs that are no longer needed;
- Redundant or duplicate user IDs; and

- User IDs with excessive privileges, which are no longer necessary and/or are not approved.

The account management issues we found in the preceding findings in the areas of separated and transferred users with active access, as well as active user accounts that should be disabled or removed, question whether periodic reviews of access rights are being conducted. Prior to the commencing operations of the application, the DPP provided instructions to the OAs of the using agencies on the performance of reviews. DPP personnel also stated that they review access for their own employees every six months; however, no documentation or evidence that the reviews had taken place was provided.

Recommendation

We recommend the division perform a review of all users in the NJSTART application, work with the agencies to identify accounts not meeting the requirements of the SISM, and revoke or remove access as appropriate. The division should also communicate the requirements and procedures for performing periodic reviews to the OAs of the agencies, and monitor the agencies' compliance through periodic verification. In addition, the division should document and maintain evidence of the reviews of its own employees.

Logical Access – Authorization

Access controls limit or detect inappropriate access to computer resources, protecting them from unauthorized modification, loss, and disclosure. Logical access authorization controls limit the files and other resources that authenticated users are authorized to access and the actions that they can execute. These restrictions address issues such as proper segregation of duties, as well as preventing authorized users from intentionally (or unintentionally) reading, adding, deleting, modifying, or removing data or executing changes that are outside their span of authority.

The NJSTART application is structured to assign various abilities to user accounts, rather than having specific roles with set permissions. Users can be assigned privileges to perform functions such as creating, approving, processing, as well as creating and altering workflows for, transactions. These can be assigned in various combination as decided by an agency's OA, which is an administrator with limited rights that allow them to maintain the organization's users, approval paths, departments, and settings. Agency OAs handle the provisioning of access rights in their own agency; it is not dictated by the DPP. This was done to allow the flexibility to accommodate different organizational structures at the agencies.

Users with Organization Administrator rights in NJSTART should not have access to purchasing and payment functions in the application.

The SISM requires agencies to adhere to the principle of segregation of duties when assigning functions, tasks, and responsibilities for critical business processes, system maintenance, day-to-day computer operations, and security/system administration. Specifically, it states that "individuals assigned to an information security role are not also assigned to an information systems role". Based on that requirement, users with the OA role should not be assigned functional roles within the application as well. Their ability to create and alter users, workflows, and approval paths is in direct conflict with utilizing those workflows and approval paths. The DPP's agency reference guide reinforces this by stating that users with the OA role should be limited to maintaining user accounts, approval paths, and departments and settings, and should not have access to the other functions in NJSTART.

We identified 147 active users having the OA role, of which 133 have at least one role in addition to OA and inquiry only. Of these, 106 had access to the accounts payable function, with 17 having the ability to generate invoices, and 89 with the ability to approve invoices (it should be noted the application is configured such that a user can be either an invoice creator or approver, but not both).

Discussions with DPP personnel disclosed that, although they agreed that there could be control-related issues related to results of our analysis, they "do not feel that Org Admins (OAs) are abusing their privileges" and actually using the additional roles inappropriately. We attempted to verify this through analysis of the transaction history in NJSTART, which records the user who performs various tasks in the purchasing process. Our analysis found that of the 133 OAs that have at least one role in addition to OA and inquiry only, 103 had at least one transaction where they were the purchase order requestor, purchase order updater, receipt creator, receipt receiver, receipt approver, invoice enterer, or invoice approver. There were a total 161,370 transactions where the OA filled at least one of these roles. We further analyzed purchase order, receipt, and invoice transactions to identify instances where the OA user performed more than one aspect of the transaction. We found 1,491 purchase orders where the OA was both the purchase order requestor and last updater, 401 transactions where the OA was the receipt creator, receiver, and approver, and 1,714 transactions where the OA was the invoice creator and approver.

Recommendation

We recommend the division perform a review of all users with the OA role, and work with the agencies to remove other privileges from these users or assign the OA role to a different person in the agency if the current OA needs to maintain their other functionality. Since the division already expressed to agencies the need to segregate this role in its agency reference guide, we recommend that they perform periodic reviews for the reoccurrence of this issue, address the results with the appropriate agency, and document and maintain evidence of these reviews.

Proxy rights are not being properly controlled.

The NJSTART application has the ability for a user to assign their application authorization rights to another user via proxy. The user being assigned the proxy rights can receive system messages for, and perform any functions of, the person assigning the rights. This includes approvals if the assigning user is on the approval path for a transaction. Proxy rights assignment is a temporary status change and is meant for limited use. Users who assign proxy rights should also be cognizant of allowing privileges that may inadvertently circumvent controls, such as segregation of duties.

Our initial analysis found 42 users who assigned proxy rights to other users. When this same analysis was re-performed thirteen months later, we found that 25 proxy assignments had been removed and 24 new proxies had been established, for a total of 41 active proxies. The remaining 17 proxies had remained in place for the entire thirteen-month period. Although it is possible that the proxy assignment could have been removed and reestablished during the period, there is still a risk of proxy rights being assigned to users to perform actions that supersede their established authority.

Our analysis of the 41 active proxies found two instances where a user had been given OA rights through proxy, eight where an existing OA had been assigned the rights of other users, two where a user had the rights of multiple users assigned to them via proxy, three where a person has a third person's rights assigned because of multiple proxies, and eight where the proxy rights assigned created a segregation of duties weakness. Specifically, a user was able to either create or approve invoices, and was then given the right to perform the other function via proxy, which would allow the person to create and approve invoices, thereby circumventing the system's controls.

Recommendation

We recommend the division perform a review of all users with proxy rights assigned by or to them, and work with the agencies to remove these proxy rights if they are no longer required. We also recommend the division perform periodic reviews for the reoccurrence of this issue, address the results with the appropriate agency, and document and maintain evidence of these reviews.

⋙➤✦⋘

Contingency Planning

The division does not have a documented business continuity plan.

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 will be used to put the agencies' employees and customers in a position to resume normal operations.

The SISM requires agencies to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions of the state. Requirements for business continuity plans should include the following:

- Defined purpose and scope, aligned with relevant dependencies;
- Accessibility to, and understanding by, those who will use them;
- Ownership by the agency CIO or State CTO who is responsible for their review, update, and approval;
- Defined lines of communication, roles, and responsibilities;
- Detailed recovery procedures, manual workaround, and reference information; and
- Method for plan invocation.

For the NJSTART application, the technical aspect is handled by the vendor and its underlying cloud service provider. The technical aspect of contingency planning, also known as disaster recovery, was covered in the provider's Statement on Standards for Attestation Engagements No. 18 (SSAE 18) System and Organization (SOC) report, which is conducted annually. This is a report that focuses on controls at a service provider relevant to security, availability, processing integrity, confidentiality, and privacy of a system. The report found no issues in the disaster recovery process.

The operational aspect of contingency planning for the NJSTART application, also known as business continuity planning, is the responsibility of the DPP. We found that no business continuity plan exists for the DPP's purchasing operation itself. Division management asserted that NJSTART, being a cloud-hosted software-as-a-service product, lessened the impact of a potential issue because of its accessibility from any location; however, simply having the software accessible does not guarantee a continuity of operations for customers. The DPP must also have the necessary business continuity plan related to its business processes. A lack of a documented business continuity plan could result in an unacceptable delay in processing if a business interruption were to occur.

Recommendation

We recommend the division develop, document, and implement a business continuity plan that details the procedures needed to maintain a level of service acceptable to employees and customers if a business interruption occurs.

Observation

Meeting the Purchasing Needs of All Agencies

In the Request for Proposal (RFP) for the system that would eventually become NJSTART, released in May of 2012, the DPP states that its mission is to "professionally and ethically procure the best valued products and services, in a timely and cost effective manner, in accordance with State laws and regulations, to enable government agencies to meet their objectives". The proposal by the winning vendor was accepted in January of 2013 for $5.7 million. During the course of the audit, we became aware of issues with the development and implementation of NJSTART that did not appear to align with the mission of the DPP to procure a system that meets the purchasing needs of all agencies they service.

Contract Deliverables (DPA and Waiver Transactions)

NJSTART is intended to replace the legacy Management Acquisition and Control System enhanced (MACSe) that state agencies use for the procurement of most goods and services. During the audit, more than six years after the contract was signed, we found that NJSTART is still not handling all types of purchasing transactions. Specifically, the MACSe is still handling Delegated Purchase Authority (DPA) and Waiver of Advertising (WOA) transactions for all agencies. At the start of the audit period, the division stated that these transaction types were to be rolled out to agencies in 2019; however, as of the end of our fieldwork they still had not been. The DPP provided us no convincing explanation as to why DPA and WOA transactions were not moved to NJSTART during the projected time period.

Contract Deliverables (MACSe and FMIS Interface)

Part of the functionality of the MACSe system includes job cost allocation for capital projects that is used by at least one state department to track construction projects and to submit appropriate expenses to the federal government for reimbursement through the Financial Management Information System (FMIS). NJSTART does not have this functionality, and any departments utilizing this function of the MACSe must continue to utilize the MACSe for purchasing. Therefore, the MACSe cannot be truly replaced until either a job cost allocation system is a part of NJSTART, or a new cost allocation system is obtained and interfaced with NJSTART, the state's accounting system, and the FMIS.

Our analysis of the RFP and project deliverables for NJSTART, as well as interviews of other state department personnel, identified some issues that may have led to this ongoing situation:

One such issue is that the RFP does not include the job cost allocation function in the system requirements for the FMIS interface, which the RFP only states "must remain intact as currently defined". The FMIS is described as an "internal accounting system for taking time sheet information and determining if Federal funds can be used to pay them and generate an invoice bill to send to the Federal government. The FMIS gets data from MACSe in a nightly batch

process." There is no mention of the job cost allocation aspect of the MACSe, nor its interface with the FMIS.

The assessment of the current program, conducted by the vendor, first identified the interconnection between the FMIS and the MACSe as an entry point for budgetary and accounting transactions that moves transactions between the MACSe, the state's accounting system, and the FMIS for federal funds management. The vendor stated that these transactions are not purchasing related, and that the issue was beyond the scope of their contract with the state. The vendor concluded that the need for NJSTART to provide support for the FMIS budgetary and cost allocation transactions currently supported by the MACSe made an interface between NJSTART and FMIS ineffective for meeting the needs of the departments utilizing it, and when the MACSe is replaced by NJSTART, the current point of entry for budgetary and accounting transactions will be unavailable to support departments' processes. Based on these conclusions, the vendor stated that no interface would be developed and that "the requirements related to this scope element are no longer valid." We were unable to obtain any information from the DPP concerning the process that ended with the vendor's conclusion and the state's acceptance of it because most of the key staff members, including the DPP's project manager from that period, are no longer employed by the state.

The state did create a potential work-around which would allow the addition of the necessary financial information into the state's accounting system before allowing the purchase to process. However, a purchase could still be sent through without this necessary financial information being entered because the work-around does not hold the transaction until the financial information is entered, it only provides the opportunity to enter the information. This work-around therefore could result in missed federal reimbursements. In addition, the work-around only applies to job costing for goods and services, but not to capital projects, which represent a significantly larger percentage of total construction expenditures submitted to the federal government. The work-around would only serve to split commodity and capital projects job costing between NJSTART and the MACSe, a split that would be permanent if the job cost accounting for the capital projects is never developed. There is a current proposal from the vendor for custom configuration which it stated will provide the ability to hold the transaction in NJSTART, as well as address capital purchases, at an additional cost of $1.4 million. By the end of field work, we noted no progress on this issue.

The RFP specifically states that the vendor solution should assist the state in 1) ensuring that all disbursement transactions made in the state's accounting system are reflected in the new system, 2) combining all procurement functions into a single integrated solution, and 3) improving IT economies of scale by eliminating in-house mainframe costs and IT maintenance by consolidating all procurement functions into a single system. Until DPA and WOA transactions utilize NJSTART and a solution to the FMIS interface is developed and implemented, the state must continue to use two purchasing systems for different types of transactions, thereby incurring the additional cost of maintaining the MACSe. In addition, all procurement functions are neither in

a single integrated solution, nor are all disbursement transactions in the state's accounting system reflected in the new system.

State of New Jersey

PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lt. Governor

DEPARTMENT OF THE TREASURY
DIVISION OF PURCHASE AND PROPERTY
OFFICE OF THE DIRECTOR
33 WEST STATE STREET
P. O. BOX 039
TRENTON, NEW JERSEY 08625-0039
https://www.njstart.gov
Telephone (609) 292-4886 / Facsimile (609) 984-2575

ELIZABETH MAHER MUOIO
State Treasurer

MAURICE A. GRIFFIN
Acting Director

May 17, 2021

Mr. David J. Kaschak
State Auditor
Office of Legislative Services
Trenton, New Jersey 08625

Dear Mr. Kaschak:

Thank you for providing me with the opportunity to respond to your recent audit of Department of the Treasury's New Jersey State of The Art Requisition Technology (NJSTART).

As you know, the Department's Division of Purchase and Property (DPP) is the primary custodian of NJSTART. DPP concurs with documentation of the scope and objectives as outlined in your report. Further, we agree with the methodology as outlined and we are pleased your agency has acknowledged the controls established by DPP to "ensure the confidentiality, integrity and availability of the application and its data." For the record, I would further note the background information in your report is accurate.

I would like to take a moment to respond to your findings, recommendations and observations:

"**Separated employees have active access to the NJSTART application.**"

The analysis and conclusions you provide in support of this finding are, of course, materially accurate. DPP would like to add that we do not have control over the procedures deployed by using agencies to monitor and restrict access to NJSTART. While statewide guidelines are in place to eliminate access for separated employees, the management and access of employees occurs at the agency level. Procedures for governing NJSTART access are detailed in the Organization/Department Location Review and User Profile Maintenance user guide. Above and beyond the User Guides, Quick Reference Guides and Frequently Asked Questions (FAQs), the Division has conducted numerous Agency wide training sessions and countless 1x1 Administrator meetings. DPP views this process as a using agency responsibility.

As part of this audit process, the Office of Legislative Services (OLS) recommended a periodic review of active logins with an eye toward eliminating those logins that were unused for a lengthy period of time. DPP agrees that this process will be useful and will establish procedures for a bi-annual review of agency user login to NJSTART. DPP will eliminate those

user credentials that have not been used for the prior 12 months and provide a list of those users to the relevant agency for review. DPP will use the biannual review to remind agencies to review their separated employee lists and ensure NJSTART access has been eliminated.

"**NJSTART users who transferred to other agencies retained access to their previous agency.**"

As a corollary to the issue identified, above, the biannual review will help to offset this concern. There are some nuanced differences in this issue, however. Specifically, agency users that are in an approval path may transfer to another agency and still require NJSTART access for that new agency. It is important for using agencies to notify DPP accordingly so transferred employees may retain NJSTART access under the new agency organization. Again, the biannual review will assist in reminding using agencies how to manage these types of transfers.

"**Accounts created and never used are not being disabled after 30 days.**"

Once again, DPP must rely on using agencies to manage these types of situations. Certainly, the biannual review will eliminate unused accounts. However, it should be noted that a review every six months might allow some accounts to remain dormant for more than 30 days. Again, a reminder to using agencies will be provided during the review process.

"Non-utilized User IDs are not being disabled and removed."

As part of our biannual review, DPP will conduct a purge of these types of user IDs.

"Some users in the NJSTART application have duplicate accounts."

As part of our biannual review, DPP will conduct a purge of these types of accounts.

"**Periodic reviews of user access to NJSTART are not being performed by either the DPP or the using agencies.**"

The recommendation will be addressed by the biannual review of NJSTART account credentials.

"**Users with Organization Administrator rights in NJSTART should not have access to purchasing and payment functions in the application.**"

Generally, DPP agrees with this assessment. It is not considered best practice to allow an Organization Administrator to create, approve, receive and pay for a single procurement. All agencies have been informed that there should be a separation of duties. However, DPP staff has no authority to enforce this requirement. While we do have control over access to the system, precluding a state agency from access, thereby eliminating that agency from procuring goods and services required to support that agency's core mission, is not practical. While DPP is not aware of a specific instance where an agency allows this, we do recognize that several using agencies are quite small. In this case, DPP must rely on individual agencies to function accordingly. In these cases, Organization Administrators may have duplicate roles in terms of either creating or

approving procurements. A separate using agency employee will typically be responsible for receiving the purchase or authorizing payment.

DPP will, however, routinely remind using agencies of the need to separate these responsibilities across agency resources. Further, DPP, going forward will require written justification for allowing this type of access.

"**Proxy rights are not being properly controlled.**"

The audit found a number of individuals who retained proxy rights for an extended period of time. DPP agrees that proxy rights should not be, in essence, permanent. Ideally, those proxies who retain those rights for several months, if not years, at a time should simply be given those responsibilities on a permanent basis within the organization.

Again, however, proxy arrangements are established and maintained at the using agency level. We will address this type of arrangement through our biannual review process, providing agencies with relevant lists of users with extended proxy rights and asking that agency to manage them accordingly.

"**The division does not have a documented business continuity plan.**"

The current global pandemic has put DPP's business continuity planning capabilities into action. As virtually all employees continue to work remotely, we have seen that systems access, communications and production has remained steady while statewide procurement activities have remained robust through NJSTART.

DPP will use this experience to document business continuity plans and produce a written document accordingly, to be incorporated into the departmental plan, which is currently being revised, as well as a state plan.

"**Contract Deliverables (DPA and Waiver Transactions)**"

Your audit observed that Delegated Purchase Authority (DPA) and Waiver transactions are not available in the NJSTART environment. At this time, both functions are now active in NJSTART. The DPA option has been used on a limited basis with select agencies. The intent is to get feedback from those agencies in an effort to ease the transition for all state agencies. The Waiver functionality is active and a similar pilot deployment is expected by the end of the current fiscal year.

It should be noted DPP is waiting on the NJSTART vendor to complete enhancements to the application, allowing for certain transaction exemptions as specified by statute. These enhancements should be completed within the next 30 days.

"**Contract Deliverables (MACSe and FMIS Interface)**"

Once again, your audit's summary and observation on this point are materially accurate. Any agency currently required to submit procurement data to the federal government through the

Financial Management Information System (FMIS) would see a fundamental change in processing through the NJSTART application.

You correctly point out that the new process steps outside of the NJSTART system to complete this task whereas the current process is integrated. The primary difference being that the current process precludes the generation of a purchase order without completion of the FMIS integration while NJSTART generates a purchase order separate from the FMIS submission. DPP views this change as a using agency management issue.

It should be noted that the NJSTART process generates a standing list of pending FMIS submission procurements. This list, updated every 15 minutes, is available for the using agency's inspection and management as necessary. No procurements would simply be forgotten. It would be management's responsibility to ensure staff are completing the FMIS submission on a timely basis.

It was noted in the audit report that the NJSTART derived FMIS integration would not apply to capital projects. While it is true that the NJSTART application is designed to support the procurement of goods and services, it is possible for an agency to manage capital projects in NJSTART, albeit without the FMIS requirement. To date, no agency required to submit data through FMIS has attempted to manage a capital project with NJSTART. Therefore, the level of success of this type of project management in the NJSTART environment is unknown.

Further, your report references a $1.4 million solution to this issue. This dollar figure represents the cost of a scope of work submitted by our NJSTART vendor to build an automated FMIS integration. Typically, an enhancement of this size and scope would be funded by the using agency, as were similar interfaces. We are currently investigating alternative funding options. Please keep in mind that this scope estimate was generated by the vendor more than one year ago and, most likely, has increased in cost.

There are no further observations included in your audit. In conclusion, I would like to thank you and your staff for your diligent efforts to conduct a thorough and complete review of our NJSTART application. The points raised in your report are quite helpful in allowing us to provide better management and support for this critical operational system. Your staff has conducted this review with the utmost in professionalism and courtesy and we remain grateful for understanding the difficulties we all face during these trying times.

Finally, I thank you for the opportunity to respond to your audit report. As always, please feel free to contact me if you have any questions or need any additional information.

Sincerely,

Gregg Olivera
Deputy Director
Division of Purchase and Property