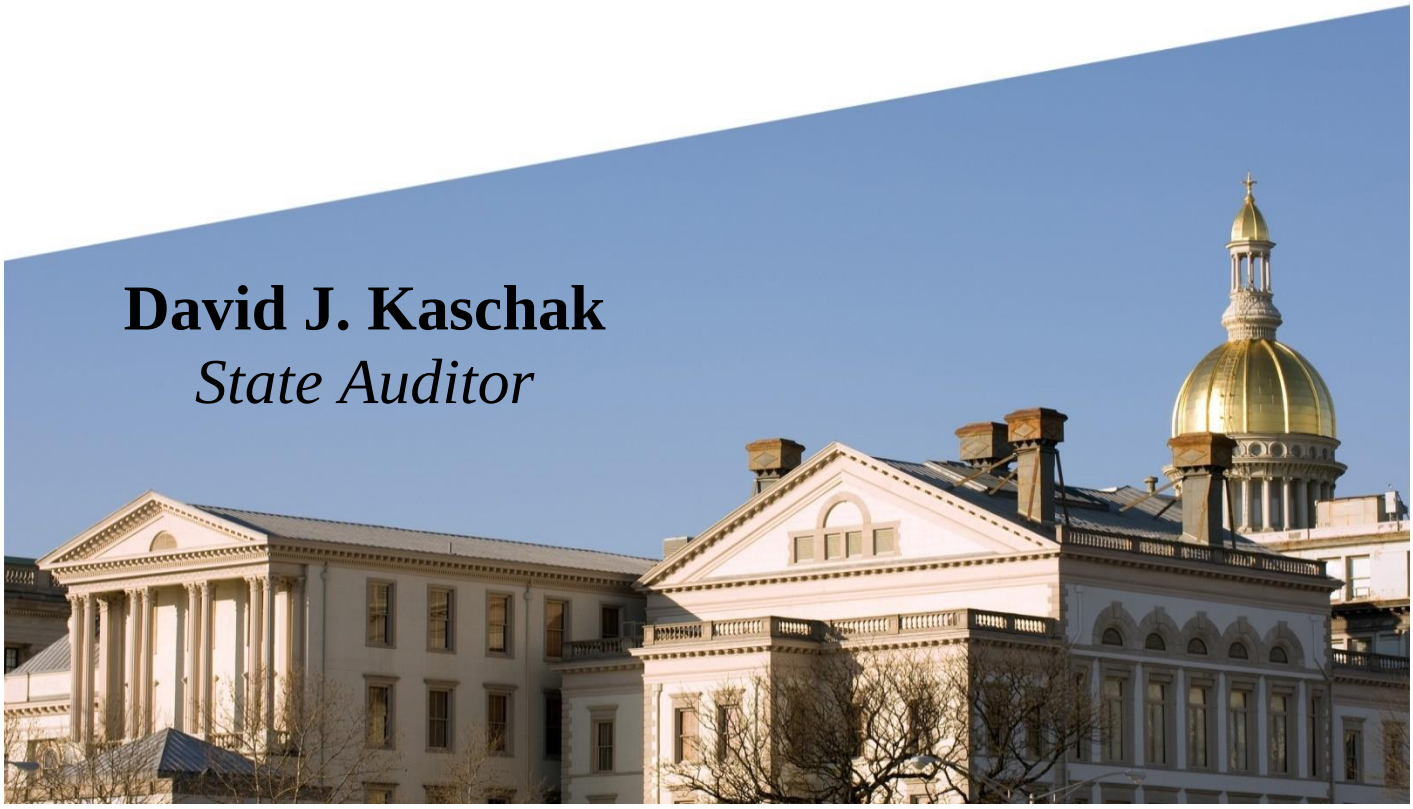
New Jersey Legislature

Office of LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR

Department of the Treasury
Office of Management and Budget
New Jersey Comprehensive Financial System Application

July 1, 2020 to February 28, 2022



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 Nicholas P. Scutari
President of the Senate

The Honorable Craig J. Coughlin
Speaker of the General Assembly

Ms. Maureen McMahon
Acting Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of the Treasury, Office of Management and Budget, New Jersey Comprehensive Financial System application for the period of July 1, 2020 to February 28, 2022. If you would like a personal briefing, please call me at (609) 847-3470.

David J. Kaschak

David J. Kaschak
State Auditor
May 25, 2022

Table of Contents

Scope

We have completed an audit of the Department of the Treasury, Office of Management and Budget, New Jersey Comprehensive Financial System application for the period July 1, 2020 to February 28, 2022. The scope of our audit included logical access, change control, disaster recovery, and data integrity of the application.

Objectives

The objective of the audit was to determine if the general and application controls in the New Jersey Comprehensive Financial System (NJCFS) application are appropriate and working properly to ensure the confidentiality, integrity, and availability of the application and its 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 U.S. Government Accountability Office; the *Statewide Information Security Manual* (SISM), published by the New Jersey Office of Homeland Security and Preparedness; and the *Information Technology Infrastructure Library* (ITIL), published by AXELOS Global Best Practice. These documents were used as the criteria against which internal controls were measured.

In preparation for our testing, we studied agency and statewide policies and procedures as well as 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, observations, and testing of the NJCFS application's controls. To achieve our objectives, we performed various tests and analyses as we determined necessary. Additional detail regarding our methodology and work performed can be found in the Appendix, as well as in the findings section when testing resulted in a reportable condition.

A non-statistical sampling approach was used in situations where the entire population was not tested. Our samples were designed to provide conclusions on our audit objectives as well as on internal controls and compliance. Sample populations were identified, and transactions were judgmentally selected for testing. Because we used a non-statistical sampling approach for our tests, we cannot project the results to the respective populations.

Data Reliability

We assessed the reliability of computer-processed data in the Security (STAB) table and the Approval Log (ALOG) table by reviewing existing information about the data, extracting the data from the Office of Information Technology (OIT) Enterprise Data Warehouse directly using business intelligence software, and tracing selected records back to source documents as part of our testing. We assessed the reliability of the New Jersey Comprehensive Financial System (NJCFS) data by performing a reconciliation between the NJCFS source system data, the Office of the State Auditor Data Warehouse, and the OIT Enterprise Data Warehouse to determine that all agreed on a single version of the NJCFS data. We determined that the data were sufficiently reliable for the purposes of this report.

Conclusions

Overall, we found that the Department of the Treasury, Office of Management and Budget has general and application controls in place in the NJCFS that are appropriate and working properly to ensure the confidentiality, integrity, and availability of the application and its data. However, we noted areas for improvement in controls and processes in the areas of logical access, change control, and disaster recovery that merit management's attention.

Background

The NJCFS is the central accounting system for the state and has been operational since May of 1993. The application is primarily written in COBOL MVS language running under a transaction processing system and contains approximately 2,000 modules.

The NJCFS application's primary function is the recording and processing of financial transactions. It comprises eight functional subsystems: Budgeting, Expenditures/Accounts Payable, Revenue/Accounts Receivable, Grants, Projects, Job Costing, Ledgers, and Travel. A secondary function of the NJCFS is to provide reliable accounting data for use in the preparation of financial statements and analysis of financial information. Data is extracted from the NJCFS to the OIT Enterprise Data Warehouse for use in statement preparation and financial data analysis.

According to information provided by the OIT, as of November of 2020 the NJCFS was accessed real-time by approximately 2,000 users statewide, and batch interfaces to exchange transactions with state agencies were executed on a periodic basis. In addition, there are real-time interfaces with the state's purchasing systems, as well as the Department of Transportation's accounting system, FMIS. Approximately 6,000 transactions are accepted daily into the NJCFS, as well as printing of approximately 3,500 checks per day and sending more than 600 payments through electronic file transfer directly to banks.

The Department of the Treasury, Office of Management and Budget (OMB) is the owner of the NJCFS and the custodian of its data. Application development, maintenance, and production

support is provided by the OIT. As of June 2021, the NJCFS application and data were moved to a vendor-managed infrastructure Mainframe-as-a-Service (MFaaS) offering, with the processing and real-time replication sites being geographically distant.

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 can 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. The NJCFS authentication uses Access Control Facility (ACF2), a mainframe security software that handles access control and permission requirements to resources. The STAB table is used to control access to NJCFS data and, as of February 2021, there were 2,578 authorized users in the STAB table, a total that includes full-time, part-time, and temporary employees. The OMB is responsible for maintaining user access to the NJCFS, which includes adding new users, changing the user ID's security access, and removing users who no longer require access.

Separated employees' user IDs were still active in the NJCFS security table, and their ACF2 user accounts were not suspended timely after separation.

We tested all 2,578 entries in the STAB table and found 294 active user accounts with access to the NJCFS that were associated with individuals who have separated from state service. Although a user may be active in the STAB table, an ACF2 account that has been suspended or retired would prevent the person from accessing the mainframe environment, in turn preventing access to the NJCFS. Accounts that are suspended maintain their date of suspension in the ACF2 record until the account is retired, after which there is no record available to document the suspension date. We looked up the 294 employees' ACF2 accounts in the live system to determine if they still had access to the mainframe environment and found one separated employee with both an active NJCFS and ACF2 account. Of the remaining 293 users, 65 were still in suspended status and had a suspension date in ACF2 that could be used to test the amount of time between their separation and suspension dates. We found that 62 of the 65 user accounts were suspended more than 30 days after their separation date, with an average of 116 days between separation and suspension. As mentioned, although the risk of not disabling the NJCFS user account could be mitigated by the ACF2 suspension, the ACF2 accounts were not suspended timely upon separation, thereby leaving a window where the separated employee could potentially access NJCFS. We performed an analysis of 12 user IDs from the 294 on the STAB table who were still active after their separation date. We found that none of the users processed any transactions between their separation and suspended dates.

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 a best practice is to maintain evidence of the completed reviews. OMB personnel informed us that they are supposed to review a STAB/ACF2 comparison report to identify inactive NJCFS users; however, this review was not

completed during the pandemic because many users were inactive during this period. Relying on the ACF2 control that automatically disables ACF2 accounts after 90 days of inactivity as a compensating control to removing access to the NJCFS for separated users does not comply with the SISM requirements and could lead to unauthorized access to the NJCFS by user IDs belonging to separated employees.

Recommendation

We recommend the OMB review all active NJCFS user accounts and disable and/or remove all accounts for users that have separated from state service. The OMB should also perform the required periodic review of user accounts to ensure that the accounts of future separated employees are being disabled or removed immediately upon termination.

Controls over model accounts should be strengthened.

The NJCFS does not allow for the creation of accounts in the STAB table for users without a state employee ID number. To accommodate temporary employees, model accounts are created for these users to obtain access to the NJCFS. Written permission from the OMB is required for the account to be established for a six-month period, after which the OMB contacts the state agency to obtain confirmation to either extend or delete the model account.

We identified 89 model accounts for temporary employees listed in the STAB table. We examined the ACF2 profile for all the model accounts to determine if the account had been suspended or retired. Of the 89 accounts, 42 still had an active ACF2 profile. We reviewed the ALOG table to determine if any of the 42 accounts had processed transactions and found 20 accounts that had done so. Because these accounts had existed for longer than six months, we requested proof of the approval for the six-month extension from the OMB and found that 12 of the 20 accounts with active access had no proof of extension. Seven of the remaining accounts were for temporary employees who had become full-time employees, though at that point the model account should have been expired and a new standard account using the person's state employee number created, rather than continuing to use the model account.

The OMB is responsible for monitoring these accounts. Prior to the pandemic, there was a manual process consisting of a physical folder containing the temporary employee profiles and their creation dates. Subsequently, the tracking of these accounts has not taken place because, according to the OMB, the process was not updated.

Recommendation

We recommend the OMB update its process regarding model accounts to ensure they are properly disabled or renewed for an extension to access the NJCFS. Also, the OMB should enforce the

requirement that agencies notify the OMB when temporary employees become full-time employees so the user account can be properly set up to access the NJCFS.

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 prevent authorized users from intentionally or unintentionally reading, adding, deleting, modifying, or removing data or executing changes that are outside their span of authority. The NJCFS security is table-driven and allows the tailoring of system access by individual user ID at the agency and organization level and with various inquiry, change, and approval abilities for specific areas of functionality. The STAB table is the primary table used to control access to NJCFS data, and all security restrictions are implemented through a user ID. The user can scan, enter, correct, and/or delete transactions as well as apply various levels of approvals for different transaction types. Each state agency's Information Security Representative (ISR) completes a security access form with all requested authorization privileges and sends it to the OMB. The OMB reviews the security profile request to determine if the access requested should be authorized and, if so, approves the security profile.

Segregation of duties controls should be implemented for NJCFS users who can create, change, and approve all levels of a transaction.

Effective segregation of duties starts with entity-wide policies and procedures that are implemented at the system and application levels. Work responsibilities should be segregated so that no one individual can control all critical stages of a business process. Agencies should define access authorizations to support segregation of duties to prevent the bypassing of internal controls without collusion. Where possible, information technology controls should be preventive and be configured to prevent the bypassing of internal controls.

When assessing the controls over transaction processing in NJCFS, we identified that users with the ability to enter, change, and approve all levels of a transaction could control the entire business process of that transaction without outside intervention. Analyzing the STAB table, we identified 77 users having the ability to enter, change, and approve all levels of at least one transaction type. There are 46 employees of the Department of the Treasury who require these abilities for certain transaction types to perform their job function, and the OMB monitors their use of this ability. Therefore, they were excluded from our testing. However, we also identified 31 non-Treasury user IDs with these abilities, which were selected for testing.

Because user access to transactions can be assigned at the individual transaction type or to security groups that include multiple transaction types, the 31 individuals we selected for testing comprised 50 STAB table entries for different transaction types. Our test disclosed that all 50 STAB table entries for the 31 users gave them the ability to enter, change, and approve all levels of a particular transaction type.

The NJCFS maintains a log of transaction approvals for every transaction in the ALOG table. This allowed us to determine all instances where the ability to approve all levels of a transaction was utilized. The NJCFS does not record the user ID of the user who created the transaction, therefore we were only able to determine situations where controls may have been bypassed. It should be noted, however, that the NJCFS has the capability of preventing this bypassing of controls by removing the create and change ability for those with all levels of approval.

Of the 31 users, we selected the 14 users who could perform this bypassing of controls for fiscal/accounting transactions such as cash receipts, cash disbursements, and expenditure modifications. Of the 14 users, there were 6 who applied all levels of approval to a total of 671 transactions totaling $964,159 between July 1, 2020, and December 31, 2021. Of these transactions, we found that one of these users had approved multiple payments to themselves, for a total of $1,351. These transactions were miscellaneous expense reimbursements, and our review of the transactions did not indicate any improper activity.

From 1995 until the end of fiscal year 2018, the OMB maintained Treasury Circular No. 95-11 that addressed this control weakness. It stated that, to achieve a better level of internal control, it is not acceptable for individuals with all levels of approval to also have the ability to enter or change transactions in the NJCFS, which is a proper basic internal control. The OMB stated that it checks the approvals levels requested upon granting an individual's access to NJCFS, and that the controls previously outlined in the circular are now included in an NJCFS Security Manual. This manual has been in draft status since 2018 and does reference the removed circular and the controls required by it; however, the manual has not been completed and adopted. Without a current circular or security manual in place, no written policy exists to deter users from entering, changing, and approving transactions without additional intervention. Also, the OMB is not using its internal procedures or the preventive controls available in the NJCFS to mitigate this control weakness.

Recommendation

We recommend the OMB review the users who currently can bypass controls related to transaction processing and use the technical controls in the NJCFS to remove this ability unless the agency can justify an exception. If the agency and the OMB accept the risk associated with granting this exception, then monitoring should be in place for transactions where the user approves all levels. In addition, to inform the user community and enforce the importance of segregation of duties, the OMB should finalize and adopt a written policy to make users aware of the internal control requirements.

Change Control

Change control procedures related to verifiable approval signatures should be improved.

The SISM states that all technology changes to production environments must follow a standard process to reduce the risk associated with the change. Agencies shall involve key business stakeholders in the change process to ensure changes are appropriately tested, validated, and documented before implementing any change on a production system. Change control consists of 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.

Industry standards are consistent that approvals from appropriate individuals are necessary at various stages of the change control process. The OMB and the OIT collect the signatures of appropriate personnel in both agencies using a sign-off sheet that requires those signatures at pre-defined stages in the change control process. This sheet requires appropriate signatures to be obtained during the design, code walkthrough, and system test stages. A final signature confirms that the change that was requested, developed, and tested as part of the process is the correct change put into production for the application.

We reviewed all nine changes to the NJCFS for fiscal year 2021 and found that the signature fields for all changes were typed into the form, rather than containing authentic written or verifiable electronic signatures for both OMB and OIT personnel. Our review of associated documentation for all nine changes found that eight did not contain supplemental approval documentation to offset the lack of verifiable signatures on the approval forms. With the increase in remote collaboration, there is a need for approval signatures to either be electronically verifiable or be supplemented by additional documentation from the approver verifying their approval to demonstrate the veracity of the signatures provided on the change control documentation. It should be noted that, despite the lack of verifiable signatures on the fiscal year 2021 changes we reviewed, we did not find any inappropriate or improper changes that would affect the integrity of the NJCFS application.

This control weakness could allow a change to be implemented without the signature of appropriate personnel in the process. Inadequate controls over the development and modification of programs could result in improper or unauthorized changes being made to the production environment.

Recommendation

We recommend the OMB, together with the OIT, institute a control that either verifies the approval signatures on the form or requires additional confirmation be provided from the

authorized approver.

Disaster Recovery Plan

The NJCFS Disaster Recovery plan needs to be updated.

The SISM states that the agency and OIT management are required to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions on behalf of the state. Specifically, it states that the agency should update the contingency plan to address changes to the agency, system, or environment of operation, as well as identify critical information system assets supporting agency missions and business functions.

In June 2020, the NJCFS was moved to a new operating environment, which included physically relocating the mainframe servers where the application resides. After reviewing the disaster recovery plan provided by the OIT we found that the current plan, which was last revised in June 2018, had not been updated and continues to reference the old environment. The disaster recovery plan also does not include diagrams of the supporting infrastructure of the application, including critical information system assets and logical connections.

The OIT has acknowledged that the plan requires updating for the new operating environment. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. Despite the lack of an updated disaster recovery plan, the OIT and the OMB did organize and conduct a successful disaster recovery test of the NJCFS application in October 2021 within the new operating environment.

Recommendation

We recommend the OMB, together with the OIT, update the NJCFS disaster recovery plan for the change in the environment of operations, as well as include necessary information on the infrastructure, including critical information assets and logical connections.

Appendix

Methodologies to Achieve Audit Objectives

In addition to the procedures outlined in the findings, we performed the following audit procedures to reach our conclusions.

Logical Access

To determine the process and control environment over user account creation, modification, and deletion, we first reviewed and documented the process and any relevant policies and procedures with the OMB. We analyzed the complete STAB table to identify active user IDs and to determine if there were any duplicate user IDs or users with incorrect state employee numbers.

Change Control

To determine the appropriateness and completeness of the change control environment, we documented all policies and procedures from the OIT related to change control and assessed them for completeness and applicability to state and industry standards, as well as determined the methodology by which users are made aware of them. We also documented and assessed the experience and knowledge of the personnel involved in the NJCFS change control process. We reviewed and verified the list of mainframe batch jobs to determine whether all jobs were accounted for in the run schedules; verified the version dates of all transaction processing, system assurance, and job control code; and determined whether any versions that had changed were supported by a formal change request.

Disaster Recovery

To determine if the OMB had identified critical data and operations, we documented the business impact analysis for the application and assessed its contents. We documented the current disaster recovery plan for the NJCFS and assessed its contents. Because the FY 2021 disaster recovery test took place during the audit period, we observed and documented the live test, as well as documented the 2021 Disaster Recovery Exercise Report published by OIT internal audit.

Data Integrity

We documented the job schedule for the NJCFS transaction processing environment at day, week, month, calendar year, and fiscal year and determined the current jobs running in each processing stream. We also tested the entire ACF2 security ruleset for the NJCFS production and development libraries to determine if access to the libraries was restricted to appropriate personnel and that all critical activities are logged.

State of New Jersey
DEPARTMENT OF THE TREASURY
OFFICE OF MANAGEMENT AND BUDGET
P. O. BOX 221
TRENTON, NEW JERSEY 08625-0221

PHILIP D. MURPHY
Governor

ELIZABETH MAHER MUOIO
State Treasurer

SHEILA Y. OLIVER
Lt. Governor

LYNN AZARCHI
Acting Director

Telephone (609) 292-6746 / Facsimile (609) 633-8179

May 23, 2022

Mr. Brian M. Klingele
Assistant State Auditor
Office of the State Auditor
125 South Warren St.
PO Box 067
Trenton, New Jersey 08625-0067

Dear Mr. Klingele:

The Office of Management and Budget (OMB) appreciates the efforts of you and your staff in your review of the New Jersey Comprehensive Financial System (NJCFS). We are working to resolve the findings noted in the audit report and would like to thank you for giving us an opportunity to comment on the report. The response to the audit team's recommendations is as follows:

Separated employees' user IDs were still active in the NJCFS security table, and their ACF2 user accounts were not suspended timely after separation.

Audit Recommendation - We recommend the OMB review all active NJCFS user accounts and disable and/or remove all accounts for users that have separated from state service. The OMB should also perform the required periodic review of user accounts to ensure that the accounts of future separated employees are being disabled or removed immediately upon termination.

Response - To address this issue, OMB Centralized Payroll will send a separation of service report to the NJCFS Security Administrator on a monthly basis. Using the report, the Security Administrator will contact the appropriate Agency Information Security Representative and disable and/or remove all accounts for the user.

Controls over model accounts should be strengthened.

Audit Recommendation - We recommend the OMB update its process regarding model accounts to ensure they are properly disabled or renewed for an extension to access the NJCFS. Also, the OMB should enforce the requirement that agencies notify the OMB when temporary employees become full-time employees so the user account can be properly set up to access the NJCFS.

Response - This recommendation has been implemented. To address this issue, the NJCFS Security Administrator developed an Excel spreadsheet to record the start date and end date (180 days from start

date) for temporary employee security access. The Security Administrator will review the spreadsheet on a weekly basis and notify the Agency of the need to either request an extension or terminate access.

Segregation of duties controls should be implemented for NJCFS users who can create, change, and approve all levels of a transaction.

Audit Recommendation - We recommend the OMB review the users who currently can bypass controls related to transaction processing and use the technical controls in the NJCFS to remove this ability unless the agency can justify an exception. If the agency and the OMB accept the risk associated with granting this exception, then monitoring should be in place for transactions where the user approves all levels. In addition, to inform the user community and enforce the importance of segregation of duties, the OMB should finalize and adopt a written policy to make users aware of the internal control requirements.

Response - To address this issue, OMB will require updated requests from the Agencies who have staff with all levels of approval. Regarding OMB staff with all levels of approval, to remove all levels of approval would cause OMB to incur undue inefficiency in operations without an appreciable benefit for the increased personnel effort needed to process these transactions. Additionally, OMB plans to formalize guidance by adopting a written policy as recommended.

Change control procedures related to verifiable approval signatures should be improved.

Audit Recommendation - We recommend the OMB, together with the OIT, institute a control that either verifies the approval signatures on the form or requires additional confirmation be provided from the authorized approver.

Response - OIT is investigating the development of the form as a PDF document where each signature would be a digital signature. This would allow verifiable signatures to be made online and the forms emailed instead of needing them to be printed, manually signed, scanned, and emailed or faxed, which was a difficulty during COVID when we all worked from home.

The NJCFS Disaster Recovery plan needs to be updated.

Audit Recommendation - We recommend the OMB, together with the OIT, update the NJCFS disaster recovery plan for the change in the environment of operations, as well as include necessary information on the infrastructure, including critical information assets and logical connections.

Response - The OIT/NJCFS Support Team and OMB are presently working with the OIT Disaster Recovery team to update the document.

Sincerely,

Lynn Azarchi

Lynn Azarchi
Acting Director