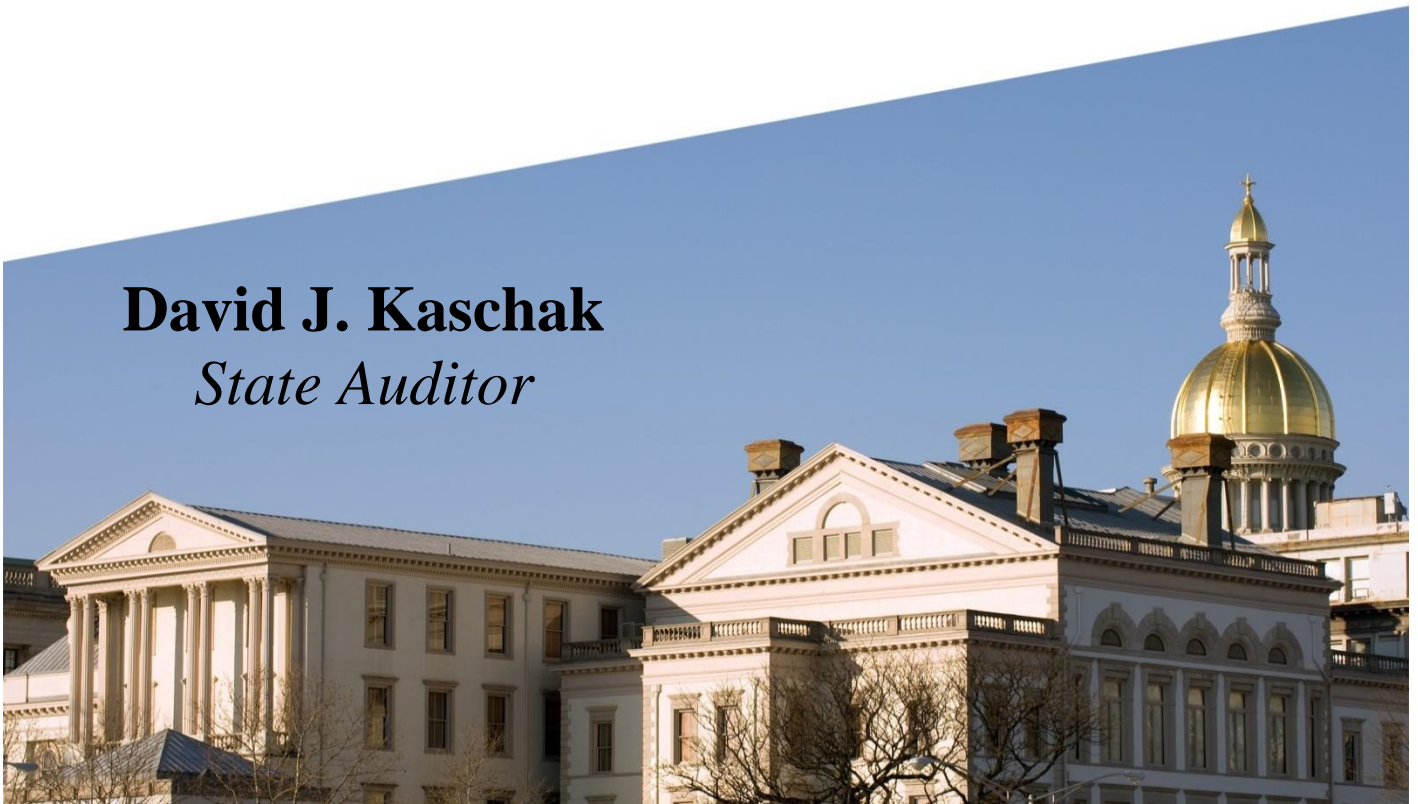


New Jersey Legislature
★ *Office of* LEGISLATIVE SERVICES ★
OFFICE OF THE STATE AUDITOR

Department of Labor and Workforce Development
Unemployment Systems - Information Technology Operations

July 1, 2019 to May 31, 2022

David J. Kaschak
State Auditor



LEGISLATIVE SERVICES COMMISSION

Assemblyman
Craig J. Coughlin, Chair

Senator
Steven V. Oroho, Vice-Chair

SENATE

Christopher J. Connors
Kristin M. Corrado
Sandra B. Cunningham
Linda R. Greenstein
Joseph Pennacchio
M. Teresa Ruiz
Nicholas P. Scutari

GENERAL ASSEMBLY

Annette Chaparro
John DiMaio
Louis D. Greenwald
Nancy F. Muñoz
Verlina Reynolds-Jackson
Edward H. Thomson
Harold J. Wirths



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
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of Labor and Workforce Development, Unemployment Systems – Information Technology Operations for the period of July 1, 2019 to May 31, 2022. If you would like a personal briefing, please call me at (609) 847-3470.

A handwritten signature in blue ink that reads "Brian Klingele".

Brian M. Klingele
Assistant State Auditor
November 16, 2022

Table of Contents

Scope.....	1
Objectives	1
Methodology	1
Data Reliability	2
Conclusions.....	2
Background	3
Observation	
Information Technology Service Management	5
Findings and Recommendations	
Change Control	7
Logical Access – Authentication	9
Contingency Planning.....	11
Appendix	
Methodologies to Achieve Audit Objectives.....	13
Auditee Response.....	15

Scope

We have completed an audit of the Department of Labor and Workforce Development (department), Unemployment Systems – Information Technology Operations, for the period July 1, 2019 to May 31, 2022. The scope of our audit included the department’s information technology (IT) service management, change control, logical access, and contingency planning of the unemployment insurance claims processing environment. Where possible, we focused on these areas as they related to the surge in unemployment claims as a result of the COVID-19 pandemic. Our audit addressed the IT environment and IT service management only.

Objectives

The objective of our audit was to determine if the department maintained an adequate information technology service management level during the increase in claims processing related to the COVID-19 pandemic. An additional objective was to determine if the selected general controls were working properly to ensure the confidentiality, integrity, and availability of the applications and data in the claims processing environment.

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 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 System Controls 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 controls and performance were measured.

In preparation for our testing, we studied legislation, administrative code, department 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 department documentation, analysis of department data, and other tests we determined necessary to achieve our audit objectives. Additional detail regarding our methodology and work performed can be found in the Appendix, as well as in the findings and the observation 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 items 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 Access Control Facility (ACF2) by accessing and extracting the data directly from the source mainframe. We assessed the reliability of data related to remote access for department users by requesting the data for two separate dates and comparing the record set for consistency and reasonableness. We assessed the reliability of various log data provided to us through discussions with department management concerning selected records. We determined that the data was sufficiently reliable for the purposes of this report. Certain other data in our report were used to provide background information. Data that we used for this purpose were obtained from the best available sources. *Government Auditing Standards* do not require us to complete a data reliability assessment for data used for this purpose.

Conclusions

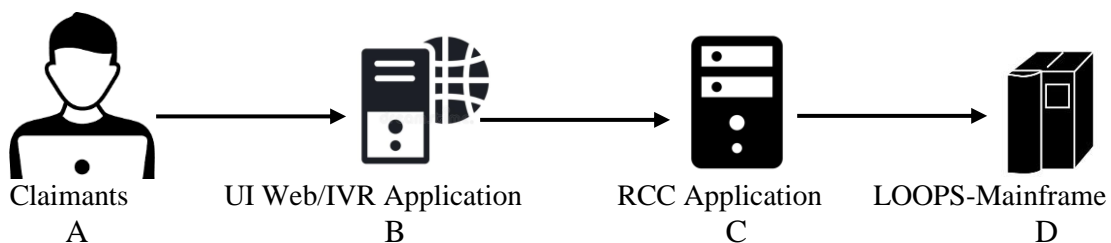
We found that the department provided a sufficient information technology service management level to claimants to meet the increased needs in the unemployment insurance (UI) claims processing environment, and we found no evidence that delays in the processing of initial claims or recertifications were caused by deficiencies in the information technology structure or operations. This is presented as an observation before the audit findings in the report.

We also found that, overall, the department has controls over logical access and contingency planning in place to ensure the confidentiality, integrity, and availability of the processing environment for UI claims, though we noted areas for improvement in controls and processes that are needed. In the area of change control, there was a breakdown in the controls during the audit period; however, our additional audit work found no instances where this caused errors or delays in the processing of claims.

Background

The filing of a new unemployment claim and the recertification (continuation) of an existing unemployment claim are both achieved through processes that include multiple technological components working together. For security reasons, we are not providing details about these components or their specific controls and connections. However, in order to understand the overall processing of unemployment transactions, the diagram below demonstrates the basic business process flow for new unemployment claims.

Claims Process (New Claims)



- A. Claimants access the UI filing processing environment through the web application, the telephone (IVR) system, or direct interaction with a department employee. The department has controls in place to restrict access to the web application by unauthorized users.
- B. When using the web or IVR, the claimant either creates an account or logs in to their existing account for the application, and the account is authenticated. Once this is successful, the claimant can file a new claim, recertify a previous claim, or inquire on the status of a previously filed claim.
- C. Once the claimant's actions are completed, if the claim is new, the claim information is stored in the department's RCC system after going through various edits and controls. According to the department, all new claims go through the RCC system before going to the mainframe Local Office Online Payment System (LOOPS). If the new claim requires additional intervention by a department employee, it is in the RCC system that the intervention takes place and any initial additions or corrections are done. The RCC system records the date the claim was received by it as well as the date the claim was moved to LOOPS.
- D. Once the claim is completed in the RCC system, it is moved to the LOOPS mainframe for processing. If a claim requires no intervention, it is typically moved to the LOOPS at the end of the same day it is filed. If it requires intervention, once the appropriate action has been taken and the claim is considered completed, it is moved to the LOOPS at the end of that day. If for any reason the claim is not accepted into the LOOPS, the claim is

labeled with the reason for the rejection in the RCC system, and the claim is addressed by an authorized department employee.

The scope of our audit included the period before the pandemic through the initial claims surge related to the pandemic and into the post-pandemic surge period. For comparison purposes, below are the New Jersey claims volume in eight-month increments, according to the U.S. Department of Labor:

Time Period	Initial Claims Filed	Continued Claims (Recertifications)	Total Transactions
6/30/2019 to 2/29/2020	332,335	3,200,108	3,532,443
3/1/2020 to 10/31/2020	1,744,339	14,241,103	15,985,442
11/1/2020 to 7/3/2021	495,872	4,644,128	5,140,000
7/4/2021 to 3/5/2022	326,260	3,633,217	3,959,477
Total Transactions	2,898,806	25,718,556	28,617,362

The pandemic caused a 425 percent increase in the number of initial claims filed (332,335 to 1,744,339) and a 345 percent increase in recertifications (3,200,108 to 14,241,103) from the eight months prior to the pandemic to the first eight months of it. In addition, various new federal and state mandates created an increased need for changes to the LOOPS application. Below is the number of LOOPS program changes between July 1, 2019 and February 28, 2022 in eight-month increments:

Time Period	LOOPS Program Changes
7/1/2019 to 2/29/2020	30
3/1/2020 to 10/31/2020	120
11/1/2020 to 6/30/2021	76
7/1/2021 to 2/28/2022	70
Total	296

Increases of that size put an additional burden on not only the technological infrastructure of the unemployment application but also on the department's information technology staff to manage the claims processing environment and its components.

Observation

Information Technology Service Management

Entities create value by providing services to their customers in an effective and efficient manner. Information technology service management is a comprehensive program that allows an organization to ensure that it provides services to its customers with confidentiality, availability, and integrity of the processing environment. Aspects of service management include availability, business analysis, capacity and performance management, incident management, and monitoring and event management.

The U.S. Department of Labor reported that New Jersey had approximately 1.0 million new unemployment claims between March 1, 2020 and May 2, 2020 and approximately 3.0 million claims recertifications during this same period for a total of 4.0 million transactions entering the UI processing environment during that time. This represents a 993 percent increase in new claims and a 201 percent increase in recertifications from the previous period of the same length. Based on this increase, we used the period March 1, 2020 through May 1, 2020 as the period to evaluate the information technology service management level of the department during the initial pandemic surge in unemployment insurance claims. We considered three major questions when evaluating the department's information technology service management:

1. Did the department have a comprehensive understanding of its claims processing environment prior to the pandemic?

We documented the department's understanding of the processing environment for unemployment insurance claims from the initiation of the transactions through the processing of the claims in the LOOPS system. We found that the department had a comprehensive understanding of its processing environment. Although we did note some deficiencies in the disaster recovery and business continuity plans as noted in a later finding, we also noted that no outage of any component of the processing environment lasted long enough to require either of these plans to be initiated; therefore, these deficiencies did not have an impact on the processing environment.

2. Did the department analyze and plan for the potential increase in claims volume, identify potential weaknesses in its environment that could impact its ability to deal with the increase, and adjust the environment to address weaknesses identified?

The department stated that it did not do any dedicated planning or make configuration adjustments in preparation for the pandemic surge in claims but rather took a reactive approach to changing the web portion of the processing environment as the monitoring mechanisms in place informed the department of potential issues. There were 29 changes made to various configuration settings in this aspect of the processing environment between March 17, 2020 and April 14, 2020 to address issues with performance. We identified that eleven of these changes were increases to the capacity of various

components of the web processing application and could have potentially been done prior to the pandemic surge; however, all of the issues were addressed and completed over a six-day period during the initial weeks of the surge and caused no significant delays to claims processing. In the mainframe portion of the processing environment, there was a performance analysis and processor upgrade performed in April 2020 to prevent delays in claims processing in that environment.

The other project that took place during this time to increase security and provide other processing benefits was moving components of the UI processing environment behind a web application firewall. Most of those components were moved in mid-March 2020. In addition, to help address the increased volume, the department enhanced the filing application to enforce required time periods for users to file for new or recertify existing unemployment benefits. The department previously provided a schedule for claimants to log on to the system based on their social security number. However, claimants did not always follow the suggested schedule and continued to attempt to access the application outside of their suggested time period. This enhancement enabled the department to enforce the schedule and deny access to users who were not within their designated time period. An error message was returned to users who attempted to access the system outside of their assigned time period.

3. Did the department monitor the environment and respond effectively to issues that arose to ensure that processing of customer transactions was not excessively delayed?

We reviewed system activity logs and other monitoring documentation related to the period March 1, 2020 through May 1, 2020 for the unemployment insurance processing environment to determine if issues occurred that would have affected the processing of claims. During this 62-day period, there were 12 incidents over 8 of the days that may have affected a customer's ability to file or recertify an unemployment claim, with the average incident lasting 84 minutes. Assuming a window of 7 a.m. to midnight each day during the period for the application to be available for filing and recertification while providing the department time for overnight maintenance and upgrades of components, we calculated that the total outage time caused by these incidents accounted for a maximum of 1.6 percent of the available filing/recertification time during the period reviewed. This percentage could be smaller when factoring in days when the maintenance window was not needed. In addition, ten of the twelve incidents were related to components of the unemployment processing environment that were migrated to other devices by May 2020.

The other aspect of unemployment claims processing at the department is the mainframe programs that process LOOPS data overnight. Our analysis of the mainframe error logs for the period March 1, 2020 through May 1, 2020 identified 67 incidents affecting the successful completion of 121 individual programs during that time. The average recovery time for these issues was approximately seven hours, which is within the overnight window when the LOOPS is offline for processing. Therefore, most incidents were resolved the same night. Eight of the incidents affecting 29 programs did take more than

24 hours to resolve, one of which took longer than 48 hours to resolve. Further analysis found that four of the eight incidents taking longer than 24 hours to resolve occurred on a single day, and the one incident taking longer than 48 hours affected a program that was not related to claims processing.

We identified 1,096 jobs on the daily program schedule for the LOOPS, which calculates to approximately 68,000 total daily mainframe programs run during the 62-day review period. Therefore, the 121 affected programs represented only 0.18 percent of the total daily programs run during the period, of which the programs that took more than 24 hours to resolve represented only 0.04 percent of the total programs. Based on this analysis, we found no evidence that there was an increased number of errors in mainframe program processing caused by the increase in claims from the pandemic, and we found no evidence that the errors that did occur in the mainframe processing during the review period caused any significant delay in the processing of claims by the LOOPS.



Findings

Change Control

The department had deficiencies in its change control process.

According to the *Statewide Information Security Manual* (SISM), all technology changes to production environments must follow a standard process to reduce the risk associated with the change. Agencies should 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; completion and review of all test results; 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 computing environment, and maintain necessary documentation of all changes.

The department has a change management policy that requires proper separation of duties between development and production environments and personnel; documentation of the impact and a detailed testing plan for the change; adequate testing of the change to determine that it operates effectively; documentation and review of the results of the testing; and proper approval by the business area before the change is moved. The change management policy is currently under revision, but this version has not been finalized. However, the version that is in use addresses the necessary controls. Early discussions with the department acknowledged that there was no formal documentation related to the changes that were made. Based on this, we expanded our analysis to include a larger number of changes and additional sources of potential information

about the changes, including hard-coded program comments and detailed conversations about the changes with department staff.

The department provided us with a list of changes, which included the program being changed, the date that the changed program was compiled into production and by whom, and a brief description of the change. From this, we selected 35 individual changes to various LOOPS mainframe programs related to pandemic unemployment during the period July 1, 2019 to June 9, 2021. We found two changes that were backed out and reverted to their previous versions, which indicated weaknesses in the change control process. Not only were the steps in the change control process not documented, but they were not performed, which resulted in issues with the production versions. We obtained additional information about these two changes and found that for one, sufficient testing was not performed, test results were not reviewed, nor was approval obtained before the change was compiled into production. The other did not have a formal change request, proper planning, testing performed, test results reviewed, or approval obtained before it was compiled into production. Although none of the other changes we analyzed needed to be backed out, without documentation of the various control points in the process, there is less assurance that the appropriate process was followed for those changes, even if they were without issue once implemented. It should be noted that neither of the changes that had to be backed out were directly related to the processing of claims.

During the audit period, the number of LOOPS changes required increased significantly because of the additional requirements related to unemployment claims and payments brought on by the pandemic and subsequent federal unemployment programs. However, we found a lack of documentation for changes completed prior to the pandemic, and the department did not begin producing the required documentation even after the number of changes required decreased significantly by 2022.

Having a change control policy that outlines proper controls and procedures is only effective if it is adhered to. Failure to properly request, design, test, review, and obtain approval before compiling changes into production can cause improper or unauthorized changes to be implemented. This can cause the application to perform incorrectly or improperly.

Recommendation

We recommend the department enforce its existing change control policy and ensure all steps of the procedure are being followed and properly documented. Also, when the new policy currently in draft is completed, we recommend the department implement any additional controls and procedures contained within it and continue to ensure that all aspects of the process are completed and documented.



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 can 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 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 department uses various authentication methods to access resources, including Access Control Facility (ACF2), a mainframe security software that handles access control and permission requirements to resources, for LOOPS authentication and virtual private network (VPN) and remote desktop software for access to internal resources for users working remotely.

Mainframe user IDs belonging to separated users were not disabled in a timely manner.

We compared the listing of users who had either separated from state service or no longer worked for the department between July 1, 2019 and June 9, 2021 with all department ACF2 user accounts as of June 9, 2021 and found nine user accounts for separated or transferred employees that were still active. Six of these users had been separated longer than 30 days, and seven had access to some function in the LOOPS application. We also identified 151 user accounts that had been previously either suspended or retired and had some level of LOOPS access. Although a user may be listed in ACF2 with a LOOPS role, an ACF2 account that has been suspended or retired would prevent the person from accessing the mainframe environment, thereby preventing access to the LOOPS. 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 identified 75 accounts that were suspended but not retired that we could test for timely suspension of the ACF2 account and found 41 had been suspended more than 30 days after separation. In addition, there were three ACF2 accounts that had been accessed after the employee's separation date, though that does not mean that the LOOPS application was accessed, only the mainframe environment. All three were employees of other agencies, and two of the three had inquiry access only.

We also matched all user accounts for separated employees, regardless of LOOPS access status, to the RCC system records to see if any claims had been changed by the user IDs after the employee's separation. The RCC system does not use ACF2 for authentication, but uses the same user ID naming convention, which allowed for the analysis. We found no instances where a separated user ID was tied to an RCC system record after the employee's separation date.

The SISM requires agencies to immediately disable access to systems for any separated users, as well as review users' access rights at least every six months, and best practice is to maintain evidence of the completed reviews. One of the aspects of this review is to identify and revoke access for user IDs assigned to terminated users with active access that may not have been

immediately disabled. During the pandemic, the department's information technology area received a large increase in the number of requests for the granting and modification of access to accommodate the increased claims volume. This increased activity often did not use the standard access request process established by the department and reduced the resources available to do a periodic review.

The ACF2 automatically suspends accounts after 90 days of inactivity as a compensating control to removing access to the LOOPS for separated users, but this does not comply with the SISM requirements regarding separated employees and could lead to unauthorized access to the LOOPS application by user IDs belonging to separated employees.

Recommendation

We recommend the department perform a detailed review of LOOPS access, removing user access that is no longer needed, and include LOOPS access in its future periodic reviews. In addition, the department should review and amend its procedure for terminated and separated employees to ensure that both internal and external users' access are removed timely.

Procedures and controls over remote access to state resources need to be strengthened.

Department users needing access to state resources remotely use either a virtual private network (VPN) connection or a remote desktop application. The VPN connection allows the user to create a secure connection to the executive branch internal network, while the remote desktop application allows remote access to the user's computer physically located at the department. The department is moving away from the remote desktop product in favor of the VPN.

We compared active department VPN user accounts as of May 15, 2021 to a listing of employees who had separated from service between July 1, 2019 and June 9, 2021 and found 18 separated users with active accounts. Of those, one had been accessed after separation. However, because the VPN is only access to the network, we cannot determine if any department resources were accessed. As of the date of the listing, 15 of the 18 accounts were more than 30 days past separation. We obtained a follow-up list of active VPN user accounts as of May 12, 2022 and found that 16 of the 18 accounts were still active, and all 16 were more than 30 days from separation. We also compared the follow-up list to a listing of users separating from state service between June 9, 2021 and May 12, 2022 and identified an additional 152 new separated users with active VPN accounts. These users were brought to the attention of the department, and the accounts were disabled.

We compared the active department remote desktop user accounts as of May 15, 2021 to a listing of employees who had separated from service between July 1, 2019 and June 9, 2021 and found 41 separated users with active accounts, 4 of which had been accessed after the user's separation date. As with the VPN, this only allows access to the user's computer, and we were unable to determine if any resources were accessed. As of the date of the listing, 37 of these accounts were more than 30 days past separation. We obtained a follow-up list of remote desktop users on May 12, 2022 and found that all 41 accounts were no longer active.

The SISM requires agencies to strictly control remote access to non-public state networks, as well as terminate remote access privileges upon a user's separation from state service. Remote access privileges should also be reviewed in conjunction with other regularly scheduled periodic user account reviews.

There was an increased need for remote access to department resources during the pandemic because of the requirement for remote work during this time, and this need continues as the department maintains a remote work policy. During the pandemic, the department's information technology area received a large increase in the number of requests for remote access, and the department has not subsequently completed a review of remote access users as of May 31, 2022.

Inadequate remote access controls could allow unauthorized access to department resources, potentially diminishing the reliability of computerized information and increasing the risk of unauthorized disclosure, modification, and destruction of information and disruption of service.

Recommendation

We recommend the department perform a detailed review of remote access users, removing any access that is no longer needed, and include remote access in its future periodic reviews. In addition, the department should review and amend its procedure for terminated and separated employees to ensure that both internal and external users' remote access are removed timely.



Contingency Planning

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. The SISM requires agency and OIT management 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. It also requires the agency to update the contingency plans to address changes to the agency, system, or computing environment.

The business continuity plan for the department and the disaster recovery plan for the LOOPS application need to be updated.

We tested three elements of the business continuity plan and found:

1. Processing Environment: We documented all device names and network locations found in the continuity plan and found that 6 of 55 devices noted in the processing environment of the contingency plan did not match the current environment.

2. Staffing: We identified 37 unique staff members in the continuity plan and found that 15 of them are separated from state service. These roles and functions need to be assigned to new individuals.
3. Network Environment: We identified 98 network locations and device names in the continuity plan that we could independently verify. Of the 98, we identified 16 device names that did not match the name in the plan. In addition, we reviewed the remaining network range assigned to the department and identified 31 devices that were not in the plan but existed on the network.

Regarding the disaster recovery plan, in June 2020 the LOOPS application was moved to a new operating environment, which included using mainframe servers in a new physical location. The OIT contacted the department in March 2022 with a new disaster recovery template and asked the department to complete the new plan and schedule a test. Therefore, the current LOOPS disaster recovery plan includes incorrect physical locations, and the application has not been tested in the new environment.

Since the mainframe environment migration in June of 2020, the OIT disaster recovery team has been working to update the plans for all applications hosted in that new environment. The volume of work that the department had at the time of the migration made updating the plan not feasible, and without an updated plan a test could not be performed. 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.

Recommendation

We recommend the department review the business continuity plan and update all necessary components, as well as complete the update of the LOOPS disaster recovery plan and perform and test in the new environment.



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 whether controls regarding logical access were appropriate, we:

- obtained a copy of the data/information flow for the application;
- reviewed and documented system interfaces that required authentication and/or authorization of accounts or devices in the interface;
- documented our discussions with department management and the policies, procedures, and supporting documents related to granting, modifying, and removing user access, and analyzed the information provided to determine compliance with applicable security requirements;
- documented a list of “superusers” in the LOOPS application and determined if they were appropriate;
- identified if any emergency system access was granted and that proper controls were followed;
- reviewed documentation pertaining to the procedures for granting remote access to the application and compared them against applicable security standards; and
- documented the password requirements for various systems and compared them against SISM requirements.

Change Control

To determine the appropriateness and completeness of the change control environment, we:

- documented and reviewed all change control policies and procedures, as well as determined whether these items were available to appropriate staff;
- assessed the qualifications and experience of those individuals involved in the change control process;
- documented and reviewed the change logs for the LOOPS application and determined the potential impact of the changes;
- extracted and reviewed job schedules, job control programs, and source code for selected unemployment mainframe programs to determine the nature of each program’s function;
- determined if the programs outlined in the previous step had been changed during the audit period but were not on the department’s change control listing; and
- documented all last maintenance dates for job control programs to determine if these programs were changed during the audit period.

Service Management

To determine the level of information technology service management, we:

- documented the unemployment claim workflow as well as related devices and connections, and met with department personnel to clarify our understanding of the workflow;
- reviewed the department's business continuity and the LOOPS disaster recovery plans;
- documented and reviewed the business impact analyses for all components of the claims processing environment;
- documented and discussed with management the planning for, and changes to, the processing environment in response to the pandemic claims surge; and
- documented and discussed with management the controls and monitoring mechanisms in place in the processing environment and obtained and reviewed any documentation about, and results of, those mechanisms.





PHILIP D. MURPHY
Governor

SHEILA Y. OLIVER
Lieutenant Governor

State of New Jersey

DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT
P.O. BOX 110, TRENTON, NEW JERSEY 08625-0110

ROBERT ASARO-ANGELO
Commissioner

November 14, 2022

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

Dear Mr. Klingele:

Thank you for providing the audit report for New Jersey Department of Labor and Workforce Development (NJDOLE), Unemployment Systems – Information Technology Operations. We generally agree with the issues identified in the report as they pertain to the audit period. We believe these issues have been resolved in 2022. See our detailed responses to the findings below.

Finding: Change Control - The department had deficiencies in its change control process

NJDOL Response: The Office of Information Management, Services and Solutions (OIMSS) utilizes the Numara Foot Prints tool to document changes to all NJDOLE environments, mainframe and distributed, on premise, cloud and OIT managed. This procedure was introduced as a division standard in the summer of 2022 with the appointment of a change manager responsible for compiling change requests from various sources internally as well as by OIT.

Weekly meetings are held to review the scope of the change, systems impacted, identify the change owner, the staff needed to support the change and the required communication to the business areas, customers, management team and general public. Initially the process was developed to manage infrastructure changes to the different environments but has expanded to include application changes across the portfolio.

A ticket is created in the Foot Prints system for every change required. It is the repository for the lifetime of the change. This includes the change requested, programmatic work performed, testing and approval of the effort for promotion to the production environment. The Foot Prints application documents all actions taken, the signoffs by the application development staff, the testing efforts by Quality Assurance (QA) testing staff and the business area sign off and approval of the change. The teams will continue to improve the documentation by using the attachment features within Foot Prints for the inclusion of relevant documents, notes and emails associated with change control requests. This will ensure that all documentation to support the testing and approval of system changes is archived.

The OIMSS Change Management Policy and procedures within the policy were reviewed during the summer of 2022 to ensure they followed the requirements and recommendations of the Statewide



“Opportunity. Stability. Dignity.”

ROBERT ASARO-ANGELO
COMMISSIONER

*New Jersey is an Equal Opportunity Employer
Printed on Recycled and Recyclable Paper*

AD-18B (2/20)

Information Security Manual (SISM).

Finding: Logical Access - Mainframe user IDs belonging to separated users were not disabled in a timely manner - Procedures and controls over remote access to state resources need to be strengthened

NJDOL Response: The Office of Information Management, Services and Solutions is currently reviewing the Department's onboarding and offboarding processes to ensure that only requested and required access levels are maintained on individuals. Currently the Foot Prints system is being utilized for the onboarding and offboarding processes. The Security Team is working with the Office of Human Capital Strategies (HCS) and the individual program areas to ensure access requests are accurate. All documented requests are attached to the Foot Prints tickets. Upon the notification of departed user from HCS, parent and child tickets are created for the termination of network access, mainframe access and remote access. The Security team is working with the ISRs in the other Departments and partner agencies to ensure that all external user's access is terminated timely.

Weekly meetings are held with the Security team lead to review all outstanding security related tasks. An item will be added to that meeting to review user access across all systems managed by OIMSS on a monthly basis and the policy will be updated accordingly.

Finding: Contingency Planning - The business continuity plan for the department and the disaster recovery plan for the LOOPS application need to be updated

NJDOL Response: The UI operations was aware of the need to update its contingency and disaster recovery plan. However, the update took a backseat to addressing the enormous volume of claims filed as a result of the pandemic.

NJDOL Emergency Management Chief worked with NJ OIT to bring the Contingency and Continuity of Operations plans up to date for NJDOL. An updated NJDOL Continuity of Operations Plan was completed in March 2020. WAN Network Diagrams, Core Network Diagrams and LOOPS Interface Diagrams were reviewed and updated in 2022. An updated LOOPS Business Impact Analysis (BIA) was completed in May 2022. An approved LOOPS Disaster Recovery Plan was completed on June 28, 2022, to reflect the Hot Site established for the filing of UI Claims online in the event of a disruption of normal services as well as the IBM Data Center established in Triangle Park, North Carolina for mainframe LOOPS operations and the IBM Recovery Center that was established in Sterling Forest New York.

An Unemployment Insurance LOOPS Disaster Recovery Exercise Guide and project plan were developed and approved to be used for the 2022 LOOPS DR Exercise that was held during the week of October 17, 2022. The Team is working on the After Actions Report.

The NJ Office of Homeland Security released in February 2021 an updated publication of the Statewide Information Security Manual (SISM). Section CP- Contingency Planning includes Policy, Contingency Plan, Contingency Plan testing, Contingency Training, Alternate Processing and Storage sites and System Backup and Recovery which have been considered in the annual review and updating of the Department's UI IT Contingency Plan.

All Security Policies and Administrative Directives (ADs) are undergoing their annual reviews and updates. This is being done in compliance with the recommendations of the NJ SISM.

If you have any questions or concerns, please contact Theresa Vallely, Director, Office of Internal Audit at Theresa.Vallely@dol.nj.gov.

Sincerely,

A handwritten signature in black ink, appearing to read 'R. Asaro-Angelo', with a long horizontal flourish extending to the right.

Robert Asaro-Angelo
Commissioner

c: Julie Diaz
Sharon Pagano
Gordon V. Horvath Jr.
Kathleen Bencivengo
Ron Marino
Theresa Vallely