

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-169
March 2021

DEPARTMENT OF ECONOMIC OPPORTUNITY

Reemployment Assistance Claims
and Benefits Information System
(CONNECT)



Sherrill F. Norman, CPA
Auditor General

Executive Director of the Department of Economic Opportunity

The Department of Economic Opportunity is established by Section 20.60, Florida Statutes. The head of the Department is the Executive Director who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, the following individuals served as Executive Director:

Dane Eagle From September 14, 2020
Ken Lawson Through September 1, 2020

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Suzanne B. Varick, CPA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

DEPARTMENT OF ECONOMIC OPPORTUNITY

Reemployment Assistance Claims and Benefits Information System (CONNECT)

SUMMARY

This operational audit of the Department of Economic Opportunity (Department) focused on evaluating selected information technology (IT) application and general controls applicable to the Reemployment Assistance Claims and Benefits Information System (RA System, also known as CONNECT) and following up on the findings noted in our report No. 2019-183, as applicable to the scope of this audit. The results of our follow-up procedures found that many of the findings disclosed in prior audits of the RA System, most recently in our report No. 2019-183, remain uncorrected. Our audit disclosed the following:

Finding 1: The Department continued to lack processes and procedures for identifying, analyzing, and correcting technical system errors and other RA System defects that prevent or hinder the processing of RA System data.

Finding 2: RA System application edits for postmark dates and related date sequencing continue to need improvement.

Finding 3: Procedures for document intake, indexing, and tracking processes continue to need improvement to ensure that all documents received for processing in the RA System are timely and accurately indexed to the appropriate claimant, claim, and claim issue.

Finding 4: RA System processes related to system-generated claim issues continue to need improvement to ensure that claims are accurately and timely processed.

Finding 5: RA System processes related to the creation and distribution of claimant and employer claim notices continue to need improvement to ensure claim notices are timely distributed.

Finding 6: Processing defects related to claimant benefit payments, claimant overpayments, and employer charges still exist in the RA System.

Finding 7: Language translations for RA System claimant communications continue to need improvement.

Finding 8: The Department continues to lack current RA System application design documentation to facilitate the efficient and effective modification of the RA System and ensure that changes to the original application design continue to align with Department business requirements.

Finding 9: Department password controls for RA System claimants continue to need improvement to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

Finding 10: Department change management controls continue to need improvement to ensure that only authorized, tested, and approved RA System program code and data changes are implemented into the production environment.

Finding 11: The reports used by the Department to conduct periodic RA System user access privilege reviews did not promote an effective review of all user accounts as the reports included information that was inaccurate and did not match RA System access records.

Finding 12: Some RA System users had inappropriate and unnecessary access privileges to high-risk functions.

Finding 13: RA System user accounts were not always promptly deactivated when access was no longer required.

Finding 14: Certain security controls related to logical access, user authentication, and logging and monitoring for the RA System and related IT resources continue to need improvement to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

BACKGROUND

The Department of Economic Opportunity (Department) administers the Reemployment Assistance (RA) Program that provides temporary, partial wage replacement benefits to qualified workers who are unemployed through no fault of their own. The Program's primary goals are to connect claimants to reemployment services, pay RA benefits to qualified workers in an accurate and timely fashion, provide an efficient first level appeals process to claimants and employers, and promptly register employers liable for the repayment of RA taxes.

The Department launched the Reemployment Assistance Claims and Benefits Information System (RA System) on October 15, 2013. The RA System is an integrated Web-based claims management system that includes the following RA Program functions: initial and continued claims, wage determination, adjudication, appeals, benefit payment control, and program integrity. Claimants, employers, and third-parties can access information about filed claims and communicate with Department staff through the RA System. Six types of users access the RA System: claimants, employers, Department staff, Third-Party Representatives, Third-Party Administrators, and other State and Federal agency staff. The RA System interfaces with various State and Federal systems as needed to process and report RA Program data.

Individuals who file for RA Program (unemployment) benefits with the State are referred to as claimants and employers for whom the claimants previously worked are referred to as employers. Generally, claimants can file an automated claim for RA benefits as a first-time claimant if they have not filed for RA benefits before or as a repeat claimant if they previously filed for RA benefits. When filing a claim, the claimant is required to provide specific information in the RA System through an automated series of questions, messages through the claimant's inbox, screens, and forms to complete the claim application. Additionally, the RA System is designed to verify the identity of claimants prior to the completion of a claim application. Once a claim application has been completed in the RA System by the claimant, a notice of claim filed (claim notice) is distributed to the employer(s). A monetary determination is then issued indicating whether, and in what amount, a claimant is eligible for benefits based on the claimant's employment during the base period of the claim.

Depending on the nature of the claim and the data entered by the claimant, the RA System may generate one or more claim issues denoting a data deficiency that needs to be reviewed or resolved before a claimant is considered eligible to receive benefit payments. The review of a claimant's application when claim issues are raised is referred to as adjudication and the resolution of claim issues for eligibility is referred to as determination.

Claim issues are automatically or manually created in the RA System and can either be auto-adjudicated based on predefined functionality in the RA System or reviewed by an adjudicator to determine whether the claim issues have been resolved and whether the claimant's application may be approved to receive RA benefit payments. Once a claimant has been determined monetarily eligible, any nonmonetary claim issues, such as reason for separation, separation pay, ability to work, or availability for work will be adjudicated and the claimant and affected employers will receive copies of the nonmonetary determination. The claimant may appeal any adverse monetary or nonmonetary benefit determinations and employers have the right to appeal adverse nonmonetary or charge-related benefit determinations to which they are a party.

State law¹ requires the Department to notify claimants and employers that claims applicable to them are being processed. Throughout the claims process, the Department must timely receive fact-finding documents requested from claimants and employers for claimants to receive RA benefits payments. Various dates in the RA System are important for determining compliance with State law and the timely payment of benefits. For example, for appeals, the postmark date if mailed through the United States Postal Service is considered the date the appeal was filed, dates documents are received by the Department are used to determine if requested documents are timely received, the date the Department mailed written requests for information is used to calculate System-determined due dates, and claim issue beginning and ending dates are used to determine the period of time a claimant may not be eligible to receive benefits.

The Coronavirus Disease 2019 (COVID-19) was declared a pandemic by the World Health Organization on March 11, 2020. In response, the Families First Coronavirus Response Act was signed into Federal law² on March 18, 2020, to, among other things, adjust the unemployment insurance program to temporarily waive certain eligibility requirements and provide more Federal financial support to the states. The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into Federal law³ on March 27, 2020, to expand the states' ability to provide unemployment insurance for many workers impacted by the COVID-19 pandemic, including workers who were not ordinarily eligible for unemployment benefits. The CARES Act included the following unemployment insurance benefit programs:

- Federal Pandemic Unemployment Compensation (FPUC) which provided an additional \$600 weekly benefit to individuals eligible for State or Federal Reemployment Assistance benefits.

¹ Section 443.151(3)(a) and (b), Florida Statutes.

² Public Law 116-127.

³ Public Law 116-136.

- Pandemic Unemployment Assistance which provided up to \$275 in weekly benefits to individuals not ordinarily eligible for Reemployment Assistance, including self-employed individuals and contract employees. This benefit was in addition to FPUC benefits.
- Pandemic Emergency Unemployment Compensation which provided individuals who had exhausted their Reemployment Assistance claim up to \$275 in weekly benefits for up to an additional 13 weeks. This benefit was in addition to FPUC benefits.

Beginning in March 2020, the Department experienced a significant increase in initial and ongoing claims for RA benefits due to the COVID-19 pandemic. According to Department records, for the week ended July 6, 2019, through the week ended March 7, 2020, the Department received 204,828 initial RA claims (an average of 5,690 initial claims per week) and 1,330,569 continuing RA claims (an average of 36,960 continuing claims per week). At the onset of the COVID-19 pandemic, from the week ended March 14, 2020, through the week ended June 27, 2020, the Department received 3,045,610 initial RA claims (an average of 190,351 initial claims per week) and 10,218,588 continuing RA claims (an average of 638,662 continuing claims per week).

FINDINGS AND RECOMMENDATIONS

Finding 1: Analysis of System Errors

Application controls include processes established to prevent or minimize interruption to critical systems and ensure system availability. Effective application controls include a process for gathering information on system defects, including technical system errors⁴ and processing exceptions, and performing root cause analysis of potential underlying system defects to facilitate the timely adjustment of procedures and automated controls to prevent future technical system errors and processing exceptions. Analyzing technical system errors and processing exceptions is crucial to determining the number of errors and exceptions, types of errors and exceptions, and trends to facilitate the correction of system defects.

In prior audits of the Department, most recently in our report No. 2019-183 (Finding 9), we noted that RA System users encountered technical system errors and other RA System defects (processing exceptions) that prevented or hindered the processing of RA System data. We also noted that the Department had not established a proactive approach to identify and analyze these system errors and defects. As part of our audit, we conducted inquiries of Department management and staff and examined Department records to evaluate Department processes for identifying, analyzing, and correcting technical system errors and other RA System defects. Our examination of Department records disclosed that the RA System has experienced technical system errors and other defects as far back as 2014 and, as of September 11, 2020, there were 742 outstanding defect tickets related to technical system errors and other RA System defects that at times prevented RA claimants from either logging on to the system, successfully submitting RA claims, or receiving accurate payments. While the Department recorded the issues in defect tickets, the Department still had not established procedures to analyze the defect tickets and gain an understanding of error frequency, error spike rates, shared commonalities, potential aggregate criticality, or total number of users affected.

⁴ A technical system error is a software program code error or hardware error that causes application processing to suspend or cease.

The Department purchased a performance monitoring tool in July 2020 to monitor application performance and facilitate analyses of RA System errors, including application mapping, dynamic baselining, and program code-level diagnostics. According to Department management, while configuration of the performance monitoring tool was completed in September 2020 and Department staff were using the tool to identify RA System errors, implementation of the tool was still in progress and procedures for using the tool had not been developed due to other priorities.

Identifying, analyzing, and correcting technical system errors and other RA System defects would ensure that technical system errors and other defects are timely resolved, the RA System is available, and processing is not hindered.

Recommendation: To facilitate the timely resolution of technical system errors and other RA System defects, ensure RA System availability, and limit processing interruptions, we recommend that Department management establish documented processes and procedures for identifying, analyzing, and correcting technical system errors and other RA System defects.

Finding 2: Application Edits

Effective application controls include edits to reasonably ensure that data is valid and recorded in the proper format and include field format controls, required field controls, limit and reasonableness controls, valid combination of related data field values, and master file matching.

In prior audits of the Department, most recently in our report No. 2019-183 (Finding 4), we noted that RA System application edits for received and postmark dates and related date sequencing needed improvement. Specifically, the *Date Received* field erroneously updated automatically to the current date and did not prevent a user from manually entering a future date, and RA System application edits did not ensure that the *Date Received* and the *Date Postmarked* fields sequenced correctly. As part of our audit, we conducted inquiries of Department management and staff and examined Department records to evaluate the adequacy of application edits over received and postmark dates and related date sequencing in the RA System. Our examination of defect tickets and related documentation found that, while the Department had made progress in correcting many of the identified date errors, on March 13, 2020, the Department identified another date sequencing error that would allow a user to enter a future date in the *Date Postmarked* field. According to Department management, while a new defect ticket had been created to correct the date sequencing error, work to correct the defect had not begun because of other priorities in response to the COVID-19 pandemic.

Absent adequate RA System application edits, the risk is increased that the appropriateness of claims, benefit payments, and employer chargeability may be compromised, and benefit payments and employer charges may be based on incorrect information.

Recommendation: We recommend that Department management continue to improve application edits to ensure the accuracy and integrity of postmark dates and related date sequencing in the RA System.

Finding 3: Document Intake, Indexing, and Tracking

Effective input controls include procedures that provide reasonable assurance that all inputs into the application have been authorized, accepted for processing, and accounted for and any missing or unaccounted for source documents or input files have been identified and investigated. As part of the claimant application process, claimants, employers, and third parties may be required to submit certain documents and information to the Department or respond to fact-finding documents issued by the Department. Response due dates are determined by the RA System or Department staff based on the document type. For appropriate processing, documents and information received by the Department should be timely linked (indexed) to the appropriate claimant, claim, and claim issue to avoid unnecessary delays or cause the system to inappropriately process a claim or claim issue without consideration of documentation received but not yet indexed or processed.

As part of our audit, we conducted inquiries of Department management and staff and examined Department records to evaluate the adequacy of RA System document intake and indexing processes. In prior audits of the Department, most recently in our report No. 2019-183 (Finding 6), we found that the Department lacked procedures that provide reasonable assurance that all received documents are timely and accurately indexed to the appropriate claimant, claim, and claim issue, including procedures for reconciling documents received through the intake mail and fax process to documents indexed to the claimant, claim, and claim issue in the RA System. We also previously noted that documents received by the Department missing the information necessary for proper indexing were saved for future investigation but were ultimately purged after 30 days of unsuccessful research, and that the lack of procedures prevented the Department from demonstrating that appropriate research efforts were conducted prior to purging the documents. In response to our current audit inquiries, Department management indicated that, while defect tickets to improve document intake, indexing, and tracking controls had been initiated, program code changes had not been implemented to correct the defects. Department management further indicated that a myriad of indexing issues continued because of a defect in the RA System core component program code and limitations in the functionality of the barcode reading software. Additionally, over time, the Department has lost key staff with institutional knowledge of the RA System core component program code, further limiting management's ability to correct the processing defects.

The lack of adequate procedures for document intake, indexing, and tracking processes, and the limitations of the RA System and barcode reading software, limit Department management's assurance that all documents received for processing in the RA System are investigated and timely and accurately indexed to the appropriate claimant, claim, and claim issue. Such limitations also increase the risk of inaccurate claim determinations that may result in erroneous benefit payments and employer charges.

Recommendation: We again recommend that Department management improve procedures for document intake, indexing, and tracking processes and improve RA System and barcode reading software functionality to ensure that all documents received for processing in the RA System are timely and accurately indexed to the appropriate claimant, claim, and claim issue.

Finding 4: Generation of Claim Issues

Transaction data processing controls include processes to ensure the completeness, accuracy, and validity of data as the data is processed within the application. The RA System was designed to automatically generate issues for a claim during claims processing based on predefined parameters, and Department staff were responsible for resolving the identified claim issues to avoid a delay in eligibility determinations and benefit payments.

We evaluated the adequacy of RA System generation of claim issues controls and found that, while processing errors (e.g., system-generated claim issues were not generated, were not generated at the appropriate point in the claims process, or were generated when a claim issue was unnecessary) were identified as early as December 2014 and the Department had researched the processing errors for 6 years, an adequate solution had not been identified. In response to our audit inquiry, Department management indicated that the processing errors were believed to be due to an RA System processing defect. Department management further indicated that, prior to correcting the claims processing errors, additional analysis was required to identify and resolve the root cause of the processing errors. While Department management planned to create a historical database table to record the claim processing errors to aid in resolution, due to COVID-19 pandemic priorities, creation of the historical database table was postponed.

The appropriate generation of claim issues by the RA System would promote data completeness, accuracy, and validity and provide assurance that determination decisions are based on correct data and claims will be accurately and timely processed. A similar finding has been noted in prior audits of the Department, most recently in our report No. 2019-183 (Finding 8).

Recommendation: We recommend that Department management continue efforts to identify and correct RA System processes related to the appropriate generation of claim issues to ensure that claims are accurately and timely processed.

Finding 5: Creation and Timely Distribution of Claim Notices

Effective application processing controls include controls for ensuring that data is processed completely and accurately and retains its validity during processing with minimal manual intervention.

State law⁵ requires the Department to notify claimants and employers regarding monetary and nonmonetary determinations of eligibility and to promptly provide a notice of claim to the claimant's most recent employer and all employers whose employment records are liable for benefits under the monetary determination. The employer must respond to the notice of claim within 20 days after the mailing date of the notice, or in lieu of mailing, within 20 days after delivery of the notice. If a contributing employer or its agent fails to timely or adequately respond to the notice of claim or request for information, the employer's account may not be relieved of benefit charges. Further, State law⁶ requires each employer who is liable for reimbursements in lieu of contributions for payment of the benefits to be notified, at the address on file with the Department or its tax collection service provider, of the initial determination of the

⁵ Section 443.151(2)(a) and (3)(a), Florida Statutes.

⁶ Section 443.151(5)(a), Florida Statutes.

claim and be given 10 days to respond. A contributing employer who responds within the allotted time may not be charged for benefits paid under an erroneous determination if the decision is ultimately reversed.

In prior audits of the Department, most recently in our report No. 2019-183 (Finding 7), we noted that controls related to the creation and distribution of written claimant and employer claim notices needed improvement to:

- Update the status of resolved claim issues during nightly processing after a determination or redetermination was recorded so claimant and employer claim notices would be timely created and distributed.
- Timely create and distribute employer claim notices for claims determined to be monetarily eligible.
- Distribute claim notices to claimants determined ineligible due to a claimant identity issue identified by the Fraud Initiative Rules and Rating Engine (FIRRE) process.

As part of our audit, we conducted inquiries of Department management and staff and examined Department records to evaluate the adequacy of RA System application processing controls related to the distribution of claim notices. While our audit procedures found that the Department had taken corrective action for the FIRRE processing defect, the other defects were not resolved because the necessary RA System corrections were significant and could negatively impact other RA System processes, including claims processing. According to Department management, while these defects had not been resolved and continued to intermittently occur, manual processes using scripts and reports had been implemented to help identify these claim notice defects.

Without appropriate application processing controls over the creation and timely distribution of claimant and employer claim notices, the Department cannot demonstrate compliance with State law and the risk is increased that claimants and employers may be denied due process or determination decisions may be made based on incorrect data, causing benefit payments and employer charges to be inappropriately processed.

Recommendation: To ensure written claim notices are promptly provided in accordance with State law, we recommend that Department management continue efforts to correct RA System defects related to the creation and distribution of claimant and employer claim notices.

Finding 6: Overpayments and Erroneous Charges

Automated application controls promote the consistent treatment of data and help ensure that data processing consistently adheres to management's intention and requirements. Information systems process groups of identical transactions similarly; therefore, any inaccuracies arising from erroneous computer programming or design will occur consistently in similar transactions.

In prior audits of the Department, most recently in our report No. 2019-183 (Finding 12), we noted that deficiencies existed in RA System automated application controls and data processing which resulted in inaccurate claimant benefit payments, claimant overpayment charges, and erroneous employer charges. To evaluate the adequacy of RA System application processing controls in preventing overpayments and erroneous charges, we conducted inquiries of Department management and staff and examined

Department records. Our examination of Department defect tickets found that the Department opened a high priority defect ticket for a defect detected on March 13, 2015, related to the creation of an uncollectable claimant overpayment. This defect erroneously increases the claimant's available balance by the amount of the overpayment, permitting the claimant to collect the amount of the overpayment twice. While the defect ticket has been intermittently worked on since March 2015, and the severity level was changed to severe in February 2018, the last action taken was in April 2019, and the defect ticket remained open (in process) as of January 2021. Additionally, we noted other defect tickets for erroneous employer charges caused by claimant overpayments that were created in 2018 and remained unresolved as of January 2021. Although we inquired, Department management was unable to provide records demonstrating the monetary impact of the overpayment defect and the related employer charge errors.

According to Department management, while processes and reports existed to help identify and manually correct claimant overpayments and erroneous employer charges, processing defects in the RA System continue to cause errors, resulting in inaccurate claimant benefit payments and employer charges. Department management further indicated that, due to the large-scale effort and extensive changes necessary to the RA System core component program code to resolve these defects, changes had not been implemented and a resolution date had not been determined.

Effective system controls that promote the consistent and accurate processing of data would prevent inaccurate claimant benefit payments and erroneous employer charges that may affect the integrity of RA System data.

Recommendation: To prevent inaccurate claimant benefit payments and erroneous employer charges from being generated by the RA System, we continue to recommend that Department management correct the RA System processing defects related to claimant benefit payments, claimant overpayments, and employer charges.

Finding 7: Language Translation

Effective application output controls ensure effective and timely distribution of correspondence from the system, including providing accurate and sufficient information to system users to facilitate timely and effective communication. State law⁷ requires the Department to provide printed bilingual instructional and educational materials in the appropriate language in those counties in which 5 percent or more of the households in the county are classified as a single-language minority and develop estimates of the percentages of single-language minority households for each county by using data from the United States Bureau of the Census (Census Bureau). Based on the Census Bureau's 2014 American Community Survey, the Department identified Spanish and Haitian Creole as the primary languages spoken by Limited English Proficiency (LEP) individuals residing in the State. The Department also determined that Spanish and Haitian Creole were the two significant languages spoken by LEP individuals accessing reemployment services and, as such, the Department's LEP Plan specified that the entire RA System was to be available in Spanish and Haitian Creole.

In prior audits of the Department, most recently in our report No. 2019-183 (Finding 5), we noted that language translation errors on forms and claimant documents, as well as error messages in the

⁷ Section 443.151(8)(a) and (c), Florida Statutes.

RA System, continued to exist. As part of our audit, we conducted inquiries of Department management and staff and examined the RA System program code changes implemented to correct the language translation errors on forms and claimant documents and the RA System error messages and found that, while the Department had corrected the previously identified RA System language translation errors and error messages, certain RA System claimant screens and the *Notice of Hearing* document were not translated to the claimant's primary language of Spanish or Haitian Creole as required by State law and the LEP Plan. In response to our audit inquiry, Department management indicated that, while the claimant screens and the *Notice of Hearing* document had not been translated when the RA System was initially designed, a defect ticket was established to accumulate, and later group into multiple work units, a list of all claimant screens that potentially needed to be translated into Spanish or Haitian Creole and another defect ticket was established to address translating the *Notice of Hearing* document. Although the defect tickets had been established, the defect tickets were pending assignment to a programmer due to COVID-19 pandemic priorities.

Without accurate bilingual claimant communications as required by State law and the LEP Plan, language barriers may exist that limit claimant access to reemployment assistance benefits.

Recommendation: We recommend that Department management continue to improve language translation for RA System claimant communications to ensure compliance with State law and the LEP Plan.

Finding 8: Application Design Documentation

Application design documentation provides the basis for validating that the processing design of the application meets management's requirements and includes the controls necessary to ensure the confidentiality, integrity, and availability of the IT resources and data. Continued maintenance of application design documentation helps facilitate the timely and accurate modification and troubleshooting of the system and helps ensure that changes to the original application design continue to align with management's business requirements. High-level design documentation includes business process flows that reflect a complete and accurate representation of the current state of all business processes. Detailed-level design documentation includes screen layouts, business rules, and process diagrams necessary to ensure the system aligns with business requirements.

As similarly noted in prior audits of the Department, most recently in our report No. 2019-183 (Finding 1), we found that the application design documentation for the RA System remained out-of-date and did not reflect the current design of the RA System, and that two of the seven main RA System process areas, *Calculate Payment* and *Process Interface File*, lacked data flow diagrams. We also noted that, while Department management initiated a process in August 2016 for business unit staff to update the use case documentation for new RA System enhancements, IT staff were not required to update the functional requirements documentation (technical specifications) associated with the enhancements. Department management acknowledged in response to our audit inquiries that the process to update the use case documentation was never documented, nor was there any assurance that use case documentation was updated as required. Subsequently, the Department reengineered the process and developed process flow documents that required IT staff to update functional requirements documentation beginning in March 2019 and business unit staff to update use case documentation

beginning in early 2020. However, the updated documentation requirements were applicable only to new RA System enhancements.

Without complete and accurate data flow diagrams and application design documentation that represent the current state of RA System business process flows and up-to-date technical specifications, the risk is increased that the RA System may not align with management's business requirements and that outdated information will impede software development and maintenance. The lack of complete and accurate design documentation for the RA System may have contributed to the ongoing deficiencies noted in Findings 1 through 7.

Recommendation: We again recommend that Department management ensure that RA System data flow diagrams and application design documentation, including use case and functional requirements documentation, are updated and maintained to completely and accurately represent the current state of all processes within the RA System and that the RA System aligns with Department business requirements.

Finding 9: Claimant Passwords

Effective IT security controls include mechanisms, such as personal passwords, for authenticating a user's identity to the system. To reduce the risk of compromise, the confidentiality of a password is more effectively protected by requiring passwords to be at least eight characters in length and include the complexity of alphanumeric and special characters.⁸

As part of our audit, we conducted inquiries of Department management and staff and examined RA System claimant logon screens and related documentation to evaluate the adequacy of password length and complexity requirements for claimants in the RA System. We found that the RA System allowed claimants to use a four-digit numeric password (PIN) to authenticate to the RA System. As such, the RA System password settings did not require a minimum password length of eight characters or enforce complexity requirements, such as the use of upper or lower-case letters or special characters, to help prevent the password from being easily guessed. According to Department management, to facilitate claims filing, the Department made a business decision when the RA System was designed to allow claimants to use a four-digit PIN to authenticate to the RA System.

The use of passwords of at least eight characters that include the complexity requirements of alphanumeric and special characters reduces the possibility that an unauthorized individual may inappropriately gain access to the RA System and compromise the confidentiality, integrity, and availability of RA System data and related IT resources. Similar findings were noted in prior audits of the Department, most recently in our report No. 2019-183 (Finding 3).

Recommendation: We again recommend that Department management establish adequate password length and complexity requirements for RA System claimant passwords to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

⁸ Chapter 3 - Evaluating and Testing General Controls, 3.2. Access Controls, *Federal Information System Controls Audit Manual*, February 2009, p. 220.

Finding 10: Change Management Controls

Effective change management controls are intended to ensure that all program code and data changes are properly authorized, tested, and approved for implementation into the production environment. Change management controls also promote the accuracy of data changes made in the production environment. Effective change management controls ensure that the established change management process is followed when program code and data changes are implemented into the production environment and that only approved changes are implemented into the production environment.

To evaluate the appropriateness of Department change management controls for program code and data changes implemented into the RA System production environment, we requested a system-generated list of the program code changes implemented into the production environment during the period July 1, 2019, through May 22, 2020, and the data changes implemented into the production environment during the period July 2019 through June 2020. However, the Department was unable to provide system-generated lists of the implemented program code and data changes. Instead, for the program code changes, the Department provided a list of the RA System program change tickets from the ticketing system with a status of either closed or implemented into production during the period July 1, 2019, through May 22, 2020, and for the RA System data changes, a list of the data change tickets from the ticketing system with a status of either closed or implemented into production during the period July 2019 through June 2020. Although the Department used a change management system for managing program code and data changes, the Department had not established controls, such as the use of a reconciliation process, to ensure that all program code and data changes implemented into the production environment followed the Department's change management process. Department management acknowledged in response to our audit inquiry that, due to higher priority issues and limited resources, the Department had not reconciled the program code and data changes implemented into the production environment to the ticketing system records and thus, the Department could not demonstrate that all program code and data changes implemented into the RA System production environment were recorded in the ticketing system.

While the ticketing system lists provided may not have included all the program code changes implemented into the RA System production environment during the period July 1, 2019, through May 22, 2020, and all the data changes implemented into the RA System production environment during the period July 2019 through June 2020, the lists included 170 program change tickets and 1,592 data change tickets. We selected 23 of the program change tickets and 35 of the data change tickets and examined available Department records supporting the tickets and the respective program and data changes.

For each of the 23 program change tickets selected for audit, we requested documentation evidencing that the ticket was authorized and the program code changes to address the ticket were tested by the programmer and user, approved to be implemented into the production environment, and implemented into the production environment by someone other than the programmer who made the changes. Our examination found that Department records did not:

- Demonstrate programmer testing sign off for the program code changes for 22 tickets.
- Demonstrate user testing sign off for the program code changes for 10 tickets.

- Demonstrate that program code changes for 20 tickets were approved for implementation.
- Identify for each program change addressed by the 23 tickets that an appropriate separation of duties existed between the programmer and implementor of each program change.

Eight of the 23 program change tickets tested were for significant COVID-19 pandemic-related program changes to online screens and claims processing for initial and continued claims. For these 8 program change tickets, we also examined Department records of programmer and user testing and independent program code reviews to determine whether the program code changes authorized on the tickets were appropriately tested and reviewed prior to implementation into the production environment. Our examination found that 7 of the program change tickets lacked detailed programmer testing documentation, 5 program change tickets lacked detailed user testing documentation, and all 8 program change tickets lacked evidence of required program code reviews by the Technical Change Control Committee (TCCC), thereby limiting Department management's assurance that the program code changes functioned as intended.

For the 35 data change tickets selected for audit, we requested documentation evidencing that the data change was authorized, tested by the programmer, reviewed and approved by the user, approved for implementation, and that the data change implementor was appropriate. Our examination found that Department records did not:

- Demonstrate that the data changes to address 3 tickets were tested by the programmer.
- Demonstrate that testing by the programmer for the data changes to address 14 tickets was reviewed and approved by the user.
- Demonstrate that the data changes to address 13 tickets were approved before being implemented into the production environment.
- Identify for each data change addressed by the 35 tickets that an appropriate separation of duties existed between the data change programmer and implementor.

In response to our audit inquiry, Department management indicated that the Department was transitioning to a new process for recording program code and data changes and that, previously, evidence of testing, approvals, and implementors was not always recorded. Additionally, programmers were not required to specifically document that a program code change was tested and TCCC program code reviews were sometimes conducted during TCCC and programmer meetings that were not documented. Further, Department management indicated that documentation for data changes was not always maintained due to the volume of data changes resulting from the COVID-19 pandemic and expansion of unemployment insurance benefits.

Without an effective reconciliation process that ensures all program code and data changes implemented into the RA System production environment are recorded in the ticketing system, and documentation of the testing and approval of program code and data changes, the Department has limited assurance that all program code and data changes are appropriately authorized, tested, approved, and implemented and do not bypass the Department's change management process. Similar findings were noted in prior audits of the Department, most recently in our report No. 2019-183 (Finding 16).

Recommendation: We again recommend that Department management improve change management controls to ensure that all implemented RA System program code and data changes are managed by, and do not bypass, the Department's change management process. We also

recommend that Department management ensure that Department records evidence that RA System program code and data changes are appropriately authorized, tested, approved, and implemented into the production environment.

Finding 11: Periodic Review of Access Privileges

Department of Management Services (DMS) rules⁹ require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of access privileges help ensure that only authorized users have access and that the access privileges provided to each account remain appropriate. An effective periodic review consists of identifying the current access privileges of system users and services and evaluating the assigned access privileges to ensure that they align with user job responsibilities. To facilitate the periodic review of the appropriateness of RA System access privileges for Department employees and other State and Federal agency users, semiannually, the Department generated user access reports and provided the reports to the appropriate supervisors for review.

To evaluate the adequacy of the periodic Department RA System access privilege reviews, we conducted inquiries of Department management and staff and examined RA System user access reports and related RA System access records. Our examination of the user access reports used by the Department to conduct the July 2019 through December 2019 access review found that the reports were inconsistent with RA System access records and, therefore, did not facilitate an effective or accurate access review. Specifically, we found that the user access reports included inaccurate information such as erroneous account statuses (e.g., accounts were listed as active that were not active) and missing or inaccurate last logon dates. According to Department management, the Department was not aware of issues with the user access reports but acknowledged that the reports' information was inaccurate and did not match RA System access records.

Without accurate reports of RA System user access privileges, Department management's assurance that semiannual access reviews effectively ensure that assigned access privileges remain appropriate is limited.

Recommendation: We recommend that Department management reevaluate the RA System user access privilege reports to ensure that the access reports are consistent with RA System access records and promote an effective review of the appropriateness of user access privileges.

Finding 12: Appropriateness of Access Privileges

Effective access controls include measures that limit a user's access privileges to only those functions necessary to perform their assigned job duties and promote an appropriate separation of duties. DMS rules¹⁰ require each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties.

According to Department records as of June 10, 2020, 94 Department employees had an active RA System user account with access to two or more of the six high-risk functions identified by the

⁹ DMS Rule 60GG-2.003(1)(a)6., Florida Administrative Code.

¹⁰ DMS Rule 60GG-2.003(1)(d), Florida Administrative Code.

Department. We evaluated RA System access for 25 of the 94 Department employees to determine whether the access privileges were appropriately assigned and found that 19 employees had been assigned access to two or more high-risk functions that were not required for the users' assigned job duties. Specifically, we found that:

- 19 employees had inappropriate access to update claimant payment information, including direct deposit information.
- 6 employees had inappropriate access to update claimant authentication information such as social security numbers.
- 12 employees had inappropriate access to claim weeks on an existing claim and, therefore, the ability to request claimant payments.
- 3 employees had inappropriate access to issue and authorize (release) manual payments.

In response to our audit inquiry, Department management acknowledged that user access was assigned through access roles that combined many functions and, therefore, access in excess of that needed for the users' required job duties was sometimes assigned.

Department records as of June 10, 2020, also showed that 12 other State and Federal agency users had an active RA System user account with access to one or more of the six high-risk functions. We evaluated the RA System access for these 12 users and noted that 4 Federal agency users were assigned access to a high-risk function that allowed the users to claim weeks on an existing claim and, therefore, request claimant payments. Such access is inappropriate for Federal agency users of the RA System. Department management was unable to explain why the Federal agency users were assigned this access and acknowledged the access was inappropriate.

Assigning access privileges to high-risk functions that are inappropriate or not required for the user's job duties increases the risk of unauthorized modification, loss, or disclosure of claimant data. Similar findings were noted in prior audits of the Department, most recently in our report No. 2019-183 (Finding 15).

Recommendation: We again recommend that Department management limit RA System user access privileges to only those functions that are appropriate and necessary for the users' assigned job duties.

Finding 13: Timely Deactivation of Access Privileges

DMS rules¹¹ require State agencies to ensure that IT access privileges are removed when access to an IT resource is no longer required. Prompt action is necessary to ensure that the access privileges are not misused by former employees, former contractors, or others to compromise data or IT resources.

For the 64 Department RA System users who separated from Department employment during the period July 1, 2019, through May 23, 2020, we examined Department access records as of June 10, 2020, to determine whether RA System access privileges were timely deactivated upon employment separation. Our examination found that 43 user accounts were not timely deactivated. Specifically, 33 user accounts assigned to 32 former employees were deactivated 1 to 232 days (an average of 22 days) after the

¹¹ DMS Rule 60GG-2.003(1)(a)8., Florida Administrative Code.

employees' separation dates and 10 user accounts assigned to 10 former employees remained active as of June 10, 2020, although 26 to 321 days (an average of 149 days) had elapsed since the employees separated from Department employment.

We also examined Department access records as of June 10, 2020, for the 2,329 contracted staff who ceased providing services to the Department during the period November 5, 2019, through June 5, 2020, to determine whether RA System access privileges were timely deactivated. Our examination found that 2,056 user accounts assigned to 2,056 former contractors were deactivated 1 to 51 days (an average of 2 days) after the contractors ceased providing services to the Department and 238 user accounts assigned to 238 former contractors remained active as of June 10, 2020, although 5 to 55 days (an average of 29 days) had elapsed since the contractors ceased providing services.

Through other audit procedures, we identified 680 active user accounts in Department access records as of June 10, 2020, that had not been used since prior to January 1, 2020. According to Department management, access removal requests were not always timely received and that, while periodic reviews of access privileges were conducted, Internal Security Unit (ISU) staff only deactivated accounts when the appropriate supervisor notified them that an account was no longer necessary.

While ISU management indicated that Department guidelines allowed 1 day (excluding weekends and holidays) upon receipt of an access removal request to deactivate a user account,¹² as unauthorized access can occur at any time, access to the RA System should be promptly deactivated when the access privileges are no longer required. Timely deactivation of RA System user accounts immediately upon employment separation or when no longer necessary reduces the risk that access privileges may be misused by former employees, former contractors, or others.

Recommendation: We recommend that Department management ensure that RA System user accounts are promptly deactivated upon employment separation or when no longer necessary.

Finding 14: Other Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, and logging and monitoring for the RA System and related IT resources continue to need improvement. We are not disclosing the specific details of the issues in this report to avoid the possibility of compromising RA System data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to logical access, user authentication, and logging and monitoring for the RA System and related IT resources, the risk is increased that the confidentiality, integrity, and availability of RA System data and related IT resources may be compromised. Similar findings were communicated to Department management in connection with prior audits of the Department, most recently in connection with our report No. 2019-183.

¹² Under Department guidelines, 22 of the 33 former employee user accounts and 276 of the 2,056 former contractor accounts were deactivated late.

Recommendation: We again recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring for the RA System and related IT resources to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report No. 2019-183.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from March 2020 through January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant Department of Economic Opportunity (Department) IT controls applicable to the Reemployment Assistance Claims and Benefits Information System (RA System) during the period July 2019 through June 2020 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, Findings 1, 3 through 9, 12, and 15 through 17 noted in our report No. 2019-183, as applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)¹³ and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

¹³ The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Governor and Department Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	<ul style="list-style-type: none"> • Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	<ul style="list-style-type: none"> • Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	<ul style="list-style-type: none"> • Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	<ul style="list-style-type: none"> • Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	<ul style="list-style-type: none"> • Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all components of internal control were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- Governor and management commitment to integrity and ethical values.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the Department's goals and objectives.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management consideration of the potential for fraud.
- Management design of control activities to achieve the Department's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the Department's objectives.
- Management communication of information internally necessary to achieve the Department's objectives.
- Management communication of information externally necessary to achieve the Department's objectives.
- Management activities to monitor the Department's internal control system and evaluate the results.

- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines and interviewed Department personnel to obtain an understanding of selected Department IT application and general controls applicable to the RA System.
- Interviewed Department personnel and examined Department records to obtain an understanding of Department processes for approving, assigning, reviewing, and deactivating access to the RA System application; processes for authenticating to the RA System network domain, application, and database; and RA System logging and monitoring of controls.
- Interviewed Department personnel and examined Department records to obtain an understanding of RA System business process flows and interfaces and the process for requesting, authorizing, testing, approving, implementing, and reconciling RA System program code and data changes.
- Interviewed Department personnel and examined Department records to determine whether the Department had corrected deficiencies related to RA System application input, processing, and output errors, specifically related to the:
 - Accuracy and completeness of received and postmark dates, and related date sequencing.
 - Accuracy of language translations on forms and claimant documents and error messages in the RA System.

- Adequacy of RA System document intake and indexing processes.
- Accuracy and timeliness of the generation of claim issues in the RA System.
- Timely creation and distribution of written claimant and employer claim notices.
- Timely distribution of claimant notifications for claims identified by the Fraud Initiative Rules and Rating Engine (FIRRE) processes, including evaluating the 2,943 determination letters distributed during the period July 2, 2019, through June 14, 2020, to determine whether claimant notifications for claims locked by the RA System FIRRE processes were timely distributed.
- Accuracy of RA System claimant benefit payments and claimant and employer charges as related to overpayment processing.
- Interviewed Department personnel and examined Department records to determine whether the Department maintained complete and accurate RA System application design documentation.
- Interviewed Department personnel and examined Department records to determine the status of corrective actions regarding the timely identification and analysis of technical system errors and other RA System defects.
- Evaluated the adequacy of authentication controls for the RA System network domain, application, and database.
- Interviewed Department personnel and examined Department records for assigning, periodically reviewing, and timely deactivating RA System user accounts. Specifically, we:
 - Evaluated Department procedures and examined Department records to determine whether the Department conducted semiannual reviews of the appropriateness of RA System user access privileges.
 - Evaluated the appropriateness of RA System user access privileges as of June 10, 2020, for 25 of the 94 Department employees and the 845 contractors and other State and Federal agency users assigned selected high-risk functions within the RA System.
 - Evaluated the timeliness of RA System user access privilege deactivations for the 64 Department users who separated from Department employment during the period July 1, 2019, through May 23, 2020.
 - Evaluated the timeliness of RA System user access privilege deactivations for the 2,329 contracted staff who ceased providing services to the Department during the period November 5, 2019, through June 5, 2020.
 - Identified 680 active RA System user accounts as of June 10, 2020, that were last used prior to January 1, 2020, and inquired as to why the unused user accounts had not been deactivated.
- Interviewed Department personnel and examined Department records for assigning administrative-level service and user accounts for the RA System network domain and database. Specifically, we evaluated:
 - The appropriateness of the 7 administrative service accounts and the 13 administrative user accounts as of June 4, 2020, with membership in the *Enterprise Admins*, *Schema Admins*, *Domain Admins*, or *Administrators* security groups.
 - The appropriateness of the 17 active database accounts as of June 12, 2020, allowing access to the RA System database.
 - The adequacy of password changes for 6 of the 10 RA System shared database accounts as of June 12, 2020.

- Interviewed Department personnel and examined Department policies, procedures, and processes for program code and data changes to the RA System, including change reconciliation processes. Specifically, we examined:
 - 23 of the 170 program change tickets for program code changes implemented into the production environment during the period July 1, 2019, through May 22, 2020, to determine whether the program change tickets evidenced authorization, programmer and user testing sign offs, approval for implementation into the production environment, and an appropriate separation of duties between the programmer and the implementor.
 - 8 significant COVID-19 pandemic-related program change tickets as of May 22, 2020, and supporting Department records to also determine whether the records evidenced detailed programmer and user testing and review by the Technical Change Control Committee prior to implementing the program changes into the production environment.
 - 35 of the 1,592 data change tickets for data changes implemented into the production environment during the period July 2019 through June 2020 to determine whether the data change tickets evidenced authorization, testing, approval, and an appropriate separation of duties between the programmer and the implementor.
- Evaluated the effectiveness of Department logging and monitoring controls.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENT'S RESPONSE**.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

Ron DeSantis

GOVERNOR



Dane Eagle

EXECUTIVE DIRECTOR

March 22, 2021

Ms. Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Enclosed is the Department of Economic Opportunity's response to the preliminary and tentative findings resulting from your audit of the Reemployment Assistance Claims and Benefits Information System (CONNECT). We thank you and your staff for the recommendations.

Please contact Jim Landsberg at (850) 245-7135 if you need additional information.

Sincerely,

Dane Eagle

DE/jl

Florida Department of Economic Opportunity | Caldwell Building | 107 E. Madison Street | Tallahassee, FL 32399
850.245.7105 | www.FloridaJobs.org
www.twitter.com/FLDEO | www.facebook.com/FLDEO

An equal opportunity employer/program. Auxiliary aids and service are available upon request to individuals with disabilities. All voice telephone numbers on this document may be reached by persons using TTY/TTD equipment via the Florida Relay Service at 711.

**Florida Department of Economic Opportunity (DEO)
Reemployment Assistance Information Technology Operational Audit
Responses to Preliminary and Tentative Findings**

Finding 1: Analysis of System Errors

Auditor Recommendation: To facilitate the timely resolution of technical system errors and other RA System defects, ensure RA System availability, and limit processing interruptions, we recommend that Department management establish documented processes and procedures for identifying, analyzing, and correcting technical system errors and other RA System defects.

DEO Response: The Department concurs with the finding. The Department continues working to establish documented processes and implement procedures for identifying, analyzing, and correcting technical system errors. As noted in the finding, the Department purchased a performance monitoring tool in July 2020 to monitor application performance and review of system errors. Once fully implemented, the Department will be able to timely identify, analyze and remediate system errors.

Anticipated Completion Date: October 2021

Finding 2: Application Edits

Auditor Recommendation: We recommend that Department management continue to improve application edits to ensure the accuracy and integrity of postmark dates and related date sequencing in the RA System.

DEO Response: The Department concurs with the finding. The Department continues to evaluate system enhancements to eliminate the need for a manual process when scanning and indexing documents into the RA System. Most of the edits identified during the prior audit were implemented between September 2019 and February 2020. The remaining application edits were not completed due to the Department's response to the COVID-19 pandemic and will be implemented by the end of 2021.

Anticipated Completion Date: December 2021

Finding 3: Document Intake, Indexing, and Tracking

Auditor Recommendation: We again recommend that Department management improve procedures for document intake, indexing, and tracking processes and improve RA System and barcode reading software functionality to ensure that all documents received for processing in the RA System are timely and accurately indexed to the appropriate claimant, claim, and claim issue.

DEO Response: The Department concurs with the finding. The Department continues to develop improved procedures for the document intake and indexing processes. Due to the COVID-19 pandemic, certain changes need to be incorporated into the Department's Standard Operating Procedures (SOP) for document intake and indexing, which is currently in development.

Anticipated Completion Date: December 2021

Finding 4: Generation of Claim Issues

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct RA System processes related to the appropriate generation of claim issues to ensure that claims are accurately and timely processed.

DEO Response: The Department concurs with the finding. The Department will continue to identify and correct any RA System processes related to appropriate generation of claim issues as encountered. Due to the increased workload the Department experienced as a result of the COVID-19 pandemic, the system issues identified in prior audits for resolution were not fully implemented. In response to the COVID-19 pandemic, the Department identified several strategic initiatives that are necessary to be completed in order to position the RA program for long-term optimization. The System Development Lifecycle (SDLC) - DevOps project will assist the Department in improving the completeness and correctness of the application design documentation, related artifacts, and dataflow diagrams for the RA system and will enable the Department to have additional processes in place that aligns RA system functionality with management's business requirements.

Anticipated Completion Date: June 2022

Finding 5: Creation and Timely Distribution of Claim Notices

Auditor Recommendation: To ensure written claim notices are promptly provided in accordance with State law, we recommend that Department management continue efforts to correct RA System defects related to the creation and distribution of claimant and employer claim notices.

DEO Response: The Department concurs with the finding. The Department will continue to develop improved procedures and identify and correct RA System defects regarding distribution of written claimant and employer claim notices. Due to the increased workload the Department experienced as a result of the COVID-19 pandemic, the system issues identified in prior audits for resolution were not fully implemented. In response to the COVID-19 pandemic, the Department identified several strategic initiatives that are necessary to be completed in order to position the RA program for long-term optimization. The System Development Lifecycle (SDLC) - DevOps project will assist the Department in improving the completeness and correctness of the application design documentation, related artifacts, and dataflow diagrams for the RA system and will enable the Department to have additional processes in place that aligns RA system functionality with management's business requirements.

Anticipated Completion Date: June 2022

Finding 6: Overpayments and Erroneous Charges

Auditor Recommendation: To prevent inaccurate claimant benefit payments and erroneous employer charges from being generated by the RA System, we continue to recommend that Department management correct the RA System processing defects related to claimant benefit payments, claimant overpayments, and employer charges.

DEO Response: The Department concurs with the finding. The Department will continue to identify and implement enhancements to the RA System's automated controls to improve the processing of data. The Department has identified several strategic initiatives required to be completed in order to position the RA program for long-term optimization. The System Development Lifecycle (SDLC) - DevOps project will assist the Department in improving the completeness and correctness of the application design documentation, related artifacts, and dataflow diagrams for the RA system and ensure that a process is in place to align RA system functionality with business requirements. This project is expected to assist the Department with implementing more effective system controls to promote more consistent and accurate processing of data regarding claimant benefit payments and employer charges.

Anticipated Completion Date: June 2022

Finding 7: Language Translation

Auditor Recommendation: We recommend that Department management continue to improve language translation for RA System claimant communications to ensure compliance with State law and the LEP Plan.

DEO Response: The Department concurs with the finding. The Department continues to review and improve language translations within the CONNECT system. The Department initiated a four-phased project to address this issue. Phase one, relating to monetary determination correspondence, was completed January 2020. Phase two, Appeal correspondence, is in progress. Due to the increased workload the Department experienced as a result of the COVID-19 pandemic, the system issues identified in prior audits for resolution were not fully implemented, and as a result, the Department has initiated a Cloud Migration project that will assist with remediation of this finding.

Anticipated Completion Date: June 2023

Finding 8: Application Design Documentation

Auditor Recommendation: We again recommend that Department management ensure that RA System data flow diagrams and application design documentation, including use case and functional requirements documentation, are updated and maintained to completely and accurately represent the current state of all processes within the RA System and that the RA System aligns with Department business requirements.

DEO Response: The Department concurs with the finding and continues to update RA System design documentation and complete dataflow diagrams of the RA System. Due to the increased workload the Department experienced as a result of the COVID-19 pandemic, some efforts to update application design documentation were placed on hold. As mentioned previously, due to the COVID-19 pandemic, the Department identified several strategic initiatives necessary to be completed in order to position the RA program for long-term optimization. The System Development Lifecycle (SDLC) - DevOps project will assist the Department in improving the completeness and correctness of the application design documentation, related artifacts, and dataflow diagrams for the RA system and will enable the Department to have additional processes in place that align RA system functionality with management's business requirements.

Anticipated Completion Date: June 2022

Finding 9: Claimant Passwords

Auditor Recommendation: We again recommend that Department management establish adequate password length and complexity requirements for RA System claimant passwords to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

DEO Response: The Department concurs with the finding. The Department is currently developing additional criteria to require claimants to use passwords with more complexity. Passwords would meet the requirements to be defined as complex passwords. Currently, the claimant PIN number is utilized in both the RA CONNECT system and Interactive Voice Response (IVR) phone system, and the Department is reviewing options for administering this large infrastructure change.

Anticipated Completion Date: June 2022

Finding 10: Change Management Controls

Auditor Recommendation: We again recommend that Department management improve change management controls to ensure that all implemented RA System program code and data changes are managed by, and do not bypass, the Department's change management process. We also recommend that Department management ensure that Department records evidence that RA System program code and data changes are appropriately authorized, tested, approved, and implemented into the production environment.

DEO Response: The Department concurs with the finding. The Department will continue working to improve change management controls by implementing a change process that captures approval of the program implementation package prior to migration. These approvals will be stored, and the Department will continue to improve the documentation process throughout the system change process. The Department plans to improve the Team Foundation Server (TFS) workflow so that approvals are captured, either by saving documentation within TFS or through the workflow itself. The Department will also continue to improve TFS reports so information can be more accessible.

Anticipated Completion Date: September 2021

Finding 11: Periodic Review of Access Privileges

Auditor Recommendation: We recommend that Department management reevaluate the RA System user access privilege reports to ensure that the access reports are consistent with RA System access records and promote an effective review of the appropriateness of user access privileges.

DEO Response: The Department concurs with the finding. The Department will continue working to improve and reevaluate the RA System user access privileges so the access reports are consistent and accurate. Due to the capacity issues experienced by the Department during the COVID-19 pandemic, the Department has identified several strategic initiatives necessary to be completed in order to position the

RA program for long-term optimization. The Department is actively underway with a Cloud Migration project that will assist with transferring program infrastructure to the Cloud, and provide improvements to business processes and application architecture.

Anticipated Completion Date: June 2022

Finding 12: Appropriateness of Access Privileges

Auditor Recommendation: We again recommend that Department management limit RA System user access privileges to only those functions that are appropriate and necessary for the users' assigned job duties.

DEO Response: The Department concurs with the finding. The Department continues to work to establish and implement procedures that will document the review process and limit access privileges in the RA System. The Department has identified an Identity Management and Access Control project to establish procedures to restrict system users to only functions necessary for assigned job duties. Additionally, the Department is working to develop a Standard Operating Procedure (SOP) to identify role-specific job duties.

Anticipated Completion Date: December 2022

Finding 13: Timely Deactivation of Access Privileges

Auditor Recommendation: We recommend that Department management ensure that RA System user accounts are promptly deactivated upon employment separation or when no longer necessary.

DEO Response: The Department concurs with the finding. The Department continues working to establish and implement a different process for the timely deactivation according to the system modernization efforts.

The Department has identified two corrective actions:

1. The Department's Internal Security Unit (ISU) will update the Universal Security Officers Guide (USOG) to incorporate additional security procedures in relation to timely deactivation of accounts, as well as provide ongoing Security Officer Training to Departmental Security Officers (DSOs) to ensure business area's DSOs and Supervisors follow the procedures documented in the USOG.
2. Due to the capacity issues experienced by the Department during the COVID-19 pandemic, the Department has identified strategic initiatives necessary to be completed in order to position the RA program for long-term optimization. The Department is actively underway with a Cloud Migration project to assist with the migration of infrastructure to the Cloud, and provide improvements to business processes and application architecture.

Anticipated Completion Date: December 2021

Finding 14: Other Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Auditor Recommendation: We again recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring for the RA System and related IT resources to ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

DEO Response: The Department concurs with the finding. The Department will continue to evaluate and improve security controls to ensure the confidentiality, integrity, and availability of RA System data and IT resources. The Department has identified a Security Architecture Review Project to help ensure the RA application, underlying platform, associated operations, and development processes meet modern application security standards.

Anticipated Completion Date: March 2022