STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-183
March 2019

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, Theresa "Cissy" Proctor served as Executive Director.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

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 included in our report No. 2017-039. The results of our follow-up procedures disclosed that many of the findings in our report No. 2017-039 were not corrected. Our audit disclosed the following:

Finding 1: The Department continues to lack current RA System application design documentation to help ensure that changes to the original application design continue to align with management's business requirements.

Finding 2: Despite restrictions in State law, the Department continues to permit the use of a social security number as the claimant user identification code for claimants using the RA System.

Finding 3: Department authentication 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 4: RA System application edits for postmark and received dates and related date sequencing continue to need improvement.

Finding 5: RA System control deficiencies causing language translation errors on forms and documents and incorrect error messages continue to exist.

Finding 6: Procedures for the document intake and indexing processes continue to need improvement to help 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 7: Controls over the distribution of written claimant and employer claim notices continue to need improvement to help ensure that claim notices are timely distributed.

Finding 8: RA System processes related to System-generated claim issues continue to need improvement to help ensure that claims are accurately and timely processed.

Finding 9: The Department lacked a proactive approach to identify and analyze RA System technical system errors and other RA System defects that may prevent or hinder the processing of RA System data.

Finding 10: Department management had not completed the implementation of interface reconciliation procedures for all data exchange interfaces.

Finding 11: RA System controls related to screens and reports continue to need improvement to help ensure accurate and adequate reporting of claims data.

Finding 12: Deficiencies continue to exist in the RA System automated controls and processing of data that result in claimant benefit overpayments and erroneous claimant and employer charges.

Finding 13: Certain security controls related to access authorization documentation and access control procedures continue to need improvement.

Finding 14: The Department continues to lack documented procedures for conducting periodic reviews of privileged network user accounts within the Department and RA System domains and failed to maintain evidence that the periodic reviews performed were conducted in accordance with management's directives.

Finding 15: Some access controls related to RA System user access privileges continue to need improvement to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.

Finding 16: The Department's change management controls continue to need improvement to ensure that only authorized, tested, and approved RA System program and data changes are implemented into the production environment.

Finding 17: Certain security controls related to logical access, user authentication, and logging and monitoring for the RA System data and related IT resources continue to need improvement to help ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

BACKGROUND

The Department of Economic Opportunity (Department) administers Florida's Reemployment Assistance (RA) Program which provides temporary, partial wage replacement benefits to qualified individuals who are out of work 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 payment of RA taxes or the reimbursement of claims.

Pursuant to State law,[1] the Department launched the Reemployment Assistance Claims and Benefits Information System (RA System) on October 15, 2013. The RA System is a fully 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 (TPRs), Third-Party Administrators (TPAs),

[1] Section 443.1113, Florida Statutes.

and other State agency staff. The RA System interfaces with various State and Federal systems as needed to process and report data applicable to the RA Program.

Individuals who file for RA Program (unemployment) benefits with the State of Florida 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 have previously filed for RA benefits. When filing a claim, the claimant is guided by the RA System through an automated series of questions, messages, screens, and forms to enter required information in the System to complete the claim application. In addition, the RA System is designed to verify the identity of claimants as part of the completion of a claim application. Once a claim application has been completed in the RA System by the claimant, notices of claims (claim notices) are distributed to employers. 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. The Department uses the term "claim issue" to denote something that will need to be reviewed or resolved before a claimant is considered eligible to receive benefit payments. The review of claim issues 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 may be required to be reviewed by adjudicators to determine if 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 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.

Throughout the RA process, there are a variety of activities that are required by law for claimants to timely receive RA benefit payments. These activities include timely Department notifications to claimants and employers that claims applicable to them are being processed in the RA System and timely receipt by the Department of fact-finding documents requested from claimants and employers. Various dates in the RA System are important in the determination of compliance with 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, received dates 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.

In performing our audit work and analyses, we determined, in some instances, that the Department logged a technical issue related to the control deficiency noted by our audit. Once a technical issue was logged, the Department referred to it as a defect ticket.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Design Documentation

Application design documentation provides the basis for validating that the processing design of the business application meets management's requirements and includes controls to ensure the confidentiality, integrity, and availability of the information technology (IT) resources and data. High-level design documentation includes business process flows that reflect a complete and accurate representation of the current state of all business processes aligned with management's requirements. Detailed-level design documentation represents business process activities and work flows in association with the high-level business process flows. Continued maintenance of application design documentation helps management ensure that changes to the original application design continue to align with management's business requirements.

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 1, we disclosed that the Department had not maintained current application design documentation for the RA System and was only able to provide a partially completed draft dataflow diagram of the RA System. In response to our audit inquiries regarding the Department's corrective actions for this finding, Department IT management indicated that the Department contracted with a consulting firm to assess the Department's current application design documentation. The recommendation from the assessment indicated that most of the application design documentation and related artifacts were not up-to-date and the effort to bring all existing artifacts to a current state would be quite large even if the goal was to simply update documentation. While the consulting firm provided a list of recommendations on June 30, 2017, for updating the RA System documentation, as of November 13, 2018, Department IT management indicated that a formal decision had not been made to implement the complete list of recommendations and that while some of the recommendations have been completed others continue to be in the backlog of requests to be fulfilled. Also, while the Department had initiated a process in August 2016 to update use case documentation for new RA System enhancements, no process existed for updating the outdated use case documentation that was not updated by the original vendor. As a result, certain aspects of the application design documentation remained out-of-date and the documentation did not reflect the current design of the RA System. Department IT management further stated that the effort to complete the dataflow diagrams was suspended while the consultant was assessing the RA System documentation and was not subsequently resumed. Consequently, two of the seven RA System main process areas, *Calculate Payment* and *Process Interface File* lacked dataflow diagrams.

Without complete and accurate RA System application design documentation, related artifacts, and dataflow diagrams that represent the current state of RA System business processes, the risk is increased that the RA System may not align with management's business requirements and outdated information will impede software development and maintenance.

Recommendation: We recommend that Department management continue to update and maintain the RA System application design documentation, related artifacts, and dataflow diagrams to help management ensure that the RA System continues to align with management's business requirements.

Finding 2: Use of Social Security Numbers

At its inception, the only purpose of the social security number (SSN) was to enable the Social Security Board to maintain accurate records of the earnings of individuals who worked in jobs covered under the Social Security program.[2] However, over time the SSN has been used extensively for identity verification and other legitimate business purposes. In an effort to curtail identity theft, the Social Security Administration initiated a public information program[3] to encourage the use of alternate identifiers in place of the SSN and strongly advise all organizations that use SSNs as the identifier in their record keeping systems to employ alternative identifiers and to avoid the use of SSNs as computer logon identification codes.

The Legislature has acknowledged in State law[4] that a person's SSN was never intended to be used for business purposes. Recognizing that an SSN can be used to perpetrate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the Legislature specified[5] that State agencies may not collect an individual's SSN unless the agency is authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law. Additionally, State agencies are required to provide each individual whose SSN is collected written notification regarding the purpose for collecting the number and the specific Federal or State law governing the collection, use, or release of the SSN for each purpose for which the agency collects the SSN. The SSNs collected may not be used by the agency for any purpose other than the purposes provided in the written notification. State law further provides that SSNs held by an agency are confidential and exempt from public inspection and requires each agency to review its SSN collection activities to ensure the agency's compliance with the requirements of State law and to immediately discontinue SSN collection upon discovery of noncompliance.

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 2, we noted that the Department continued to permit claimants to use SSNs to log on to the RA System and had not established an imperative need to use SSNs as claimant user identification codes (user IDs) for the RA System. Our audit follow-up procedures disclosed that, while the Department developed and implemented an RA System program change that allowed existing claimants to use a unique RA System-generated claimant ID instead of their SSN to log on, the program change did not eliminate

[2] *The Story of the Social Security Number*, Social Security Bulletin, Vol. 69, No. 2, 2009.

[3] United States Social Security Administration, Philadelphia Region, *Avoid Identity Theft: Protect Social Security Numbers*.

[4] Section 119.071(5)(a)1.a., Florida Statutes.

[5] Section 119.071(5)(a)2.a., Florida Statutes.

the use of an SSN as the claimant user ID but merely provided the claimant the option of using either the RA System-generated claimant ID or their SSN to log on. In addition to the RA System claimant ID or SSN, the claimant must provide a four-digit personal identification number (PIN) that serves as a password to authenticate to the RA System. However, if the claimant forgets their PIN or it expires after 90 days of inactivity, regardless of whether they have a claimant ID or not, the claimant must enter their SSN and select the 'Forgot PIN' button to reset their four-digit PIN. In response to our audit inquiry, Department management stated that they have a Federally mandated[6] need for the SSNs for the administration of its program. However, the Department has not demonstrated that the use of SSNs as RA System claimant user IDs and to reset claimant four-digit PINs is Federally mandated.

The use of SSNs as RA System claimant user IDs and to reset claimant PINs increases the risk of improper disclosure of SSNs, does not comport to the statutory restrictions on the use of SSNs, and does not heed the advice of the Social Security Administration's public information program to limit the use of SSNs.

Recommendation: We again recommend that, in the absence of establishing an imperative need for the use of SSNs as RA System claimant user IDs and to reset claimant PINs, Department management take appropriate steps to eliminate the use of SSNs for these purposes.

Finding 3: Passwords

Effective IT security controls include mechanisms, such as personal passwords (i.e., personal identification numbers), 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.[7]

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 3, our review of the RA System claimant logon screens and documentation provided by Department staff disclosed that the RA System authentication controls did not require a minimum password length of eight characters or complexity such as the use of upper or lower-case letters or special characters to help prevent the password from being easily guessed. Instead, the RA System continued to allow claimants to use a four-digit numeric password (PIN) to authenticate to the RA System.

The use of complex passwords helps limit 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.

[6] Title 42, Section 1320b-7, United States Code, provides that the State shall require, as a condition of eligibility for benefits under the unemployment compensation program, that each applicant for or recipient of benefits furnish to the State his social security account number (or numbers, if he has more than one such number), and the State shall utilize such account numbers in the administration of the program so as to enable the association of the records pertaining to the applicant or recipient with his account number.

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

Recommendation: We again recommend that Department management establish appropriate authentication controls for RA System claimants to help ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

Finding 4: Application Edits

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

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 4, the controls over postmark and received dates and related date sequencing in the RA System continued to need improvement. Specifically, the *Date Received* field erroneously updated automatically to the current date each time the document was assigned, reassigned, or indexed[8] in the RA System. Also, when Department and contractor employees made manual entries to the *Date Received* field to correct the automatic updating as discussed above or to the *Date Received* or the *Date Postmarked* fields in the normal course of work, no system edits existed to ensure that the dates sequenced correctly. For example, the RA System did not prevent the user from entering a date in the *Date Received* field that was prior to the date in the *Date Postmarked* field. Also, no edit existed to prevent the user from manually entering a future date in the *Date Received* field. While Department management issued a program change request to prevent the RA System from automatically updating the *Date Received* field to the current date, the program change request had not been prioritized for implementation. Department management also indicated that there had been no program changes to the RA System to ensure dates sequenced correctly and that the Department would address the date sequencing issues after the program changes for the *Date Received* field have been implemented.

The lack of appropriate application edits increases the risk that the accuracy of claims, benefit payments, and employer chargeability may be compromised and that benefit payments and employer charges may be based on incorrect information.

Recommendation: We again recommend that Department management improve application edits to help ensure the accuracy and integrity of the dates in the RA System.

Finding 5: Input Forms, Documents, and Messages

Effective application input controls during data entry include system-generated error messages that provide timely and useful information and error handling procedures to reasonably ensure that errors and irregularities are timely and accurately detected, reported, and corrected. As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 5, control deficiencies in the RA System causing language translation errors on forms and documents and incorrect error messages continued to exist.

[8] Indexing is the data entry of claimant or employer information that will identify the incoming correspondence if the document does not contain a bar code.

In response to our audit inquiries regarding language translations on claim application forms and fact-finding documents, Department management indicated that some language translation corrections had been implemented and provided screen prints from the RA System as evidence of implemented corrections. While the Department had corrected some of the previously noted language translation deficiencies, other previously noted deficiencies had not been prioritized for implementation and additional language translation deficiencies had been subsequently identified but not corrected.

In response to our audit inquiries regarding inaccurate error messages, Department management indicated that an error message correction had been implemented and provided screen prints from the RA System as evidence of the correction implemented for the previously noted inaccurate training break error message. Department management also indicated that there was no occasion to correct another previously noted error message that prevented both the claimant and Department staff from entering accurate employment dates because the issue could not be reproduced and there have been no additional instances of the issue. However, another previously noted error message provided in response to a claimant's failure to fully complete the *Discharged-Intoxication and Use of Intoxicants During Working Hours* questionnaire had not been corrected and the existing ticket to correct the problem had not been prioritized. We also noted that an incorrect error message that prevented the submission of a straight *Disaster Unemployment Assistance* application was subsequently identified but not corrected.

Effective controls related to language translations on forms and documents and appropriate error messages are essential to the timely and accurate detection, reporting, and correction of errors and irregularities and to ensure the completeness, accuracy, and validity of input data.

Recommendation: To help ensure the completeness, accuracy, and validity of the RA System input data, we again recommend that Department management continue efforts to implement effective controls related to language translations on forms and documents and enhance the appropriateness of error messages.

Finding 6: Timely Review and Processing of Received Documents

Effective input controls include procedures to 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 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.

Our audit procedures disclosed that, as similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 6, the Department continued to lack procedures to provide reasonable assurance that all received documents were timely and accurately indexed to the appropriate claimant, claim, and claim issue, including the reconciliation of received documents through the intake mail and fax processes with the documents indexed to the claimant, claim, and claim issue in the RA System. Also, documents received by the Department that did not contain sufficient information to index the document to the appropriate claimant, claim, or claim issue were placed in a folder on a shared drive for further investigation by adjudication staff and subsequent indexing to the appropriate claimant, claim, or claim issue in the RA System. However, if the investigation was unsuccessful after 30 days, adjudication staff purged the document from the shared drive. Due to the lack of procedures, the Department could not demonstrate that it made good faith efforts to investigate and identify source documents received prior to purging them. While Department management had submitted program change requests in March 2015 and May 2015 related to accurate indexing and document tracking, efforts to remediate the indexing and document tracking issues had not been implemented.

The lack of adequate procedures for the document intake and indexing processes limits Department management's assurance that all documents received for processing in the RA System were sufficiently investigated and timely and accurately indexed to the appropriate claimant, claim, and claim issue thereby increasing 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 the document intake and indexing processes to help ensure that all documents received for processing in the RA System are timely and accurately indexed to the appropriate claimant, claim, and claim issue to improve the accuracy of claim determinations, benefit payments, and employer charges.

Finding 7: Timely Distribution of Claim Notices

Effective application processing controls include procedures to identify, analyze, and correct the incomplete execution of transactions, and monitoring procedures to ensure that data is timely and accurately processed. State law[9] requires the Department to notify claimants and employers regarding monetary and nonmonetary determinations of eligibility. State law[10] also requires the Department to promptly provide a notice of claim to the claimant's most recent employing unit 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. Furthermore, State law[11] 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 claim and must

[9] Section 443.151(2)(a), Florida Statutes.

[10] Section 443.151(3)(a), Florida Statutes.

[11] Section 443.151(5)(a), Florida Statutes.

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

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 9, we noted that controls related to the distribution of written claimant and employer claim notices needed improvement. Specifically, we noted that:

- During nightly processing, some claim issues remained in an "in progress" status after a determination or redetermination was recorded in the RA System for the claim issue. As a result, some written claimant and employer claim notices were not created and distributed.
- For claims that were determined to be monetarily eligible, some employer claim notices were not generated. As a result, the claim notices were not distributed on the following business day.
- Contrary to Federal regulations,[12] written claim notices for claimants who were determined ineligible due to a claimant identity issue identified by the Fraud Initiative Rating and Rules Engine (FIRRE) process were not distributed to the claimants and claimants' records were indefinitely locked.

In response to our audit inquiry, Department management indicated that certain work-arounds, which included running daily scripts, were created to bypass system defects related to the distribution of claim notices. While the work-arounds forced the RA System to create and distribute certain claimant and employer claim notices, the work-arounds did not correct the original system defect and the failure of the RA System to timely distribute some claimant and employer claim notices persisted.

As part of our audit procedures, we also evaluated the RA System FIRRE processes to determine whether the Department timely distributed written determination letters to claimants when claimants' records were locked due to claimant identity issues being identified by the FIRRE processes. The Department's standard for timely distribution of the determination letters was within 48 hours of the response due date that was stated within the Suspicious Activity Notification Delivery (SAND) letter previously sent to the claimant. We evaluated 40 of the 5,086 determination letters distributed from July 1, 2017, through September 13, 2018, to determine whether the letters were timely distributed to the claimants. Because of the absence of documentation, we were unable to determine whether the letters were timely distributed for 2 of the 40 determination letters evaluated. For 8 of the remaining 38 determination letters evaluated, we concluded that the letters were not timely distributed and ranged from 2 to 376 days late.

Without appropriate controls over the distribution of written claimant and employer claim notices, the risk is increased that claimants 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: We recommend that Department management continue efforts to identify and correct RA System defects and improve the controls over the distribution of written claimant and employer claim notices to help ensure that claim notices are timely distributed.

[12] Title 20, Chapter V, Code of Federal Regulations, Appendix B to Part 625 – Standard for Claim Determinations – Separation Information.

Finding 8: Generation of Claim Issues

Data processing controls include procedures to ensure that data is processed completely, accurately, and timely, and retains its validity during processing. The RA System is designed to automatically generate issues for a claim based on predefined parameters in the System. Department staff are responsible for resolving the claim issues to avoid a delay in eligibility determinations and benefit payments. In prior audits of the Department, most recently in our report No. 2017-039, Finding 10, we noted that the Department encountered processing defects where claim issues were not generated, were not generated at the appropriate point in the claim process, or were generated when a claim issue was not needed.

As part of our follow-up procedures, we reviewed documentation and defect tickets initiated by the Department to correct the defects related to the appropriate generation of claim issues in the RA System. While the Department has remediated some of the defects identified during our prior audit, the RA System continues to encounter processing defects related to the appropriate generation of claim issues. In response to our audit inquiry, Department management indicated that, initially, they were unable to reproduce the circumstances of the defect that prevented the generation of claim issues in the RA System and a data fix was performed to correct the claims. Subsequently, in May 2017, Department IT staff determined that the defect may be caused by paging back and forth by the claimant; however, Department management indicated that as of February 21, 2019, a solution was still being investigated to remediate the defect.

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 that claims will be accurately and timely processed.

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

Finding 9: Analysis of Technical System Errors

Application controls include a process for gathering information on system errors and exceptions to perform root cause analysis of any potential underlying system issues and adjusting procedures and automated controls to allow for the detection or prevention of future system errors. Analyzing system errors and exceptions is crucial to determining the number of exceptions, types of exceptions, trends, and potential anomalies in the data that may indicate a breach of control activities.

In our report No. 2017-039, Finding 11, we noted that RA System users encountered technical system errors that prevented or hindered the processing of RA System data. As part of our follow-up procedures, we reviewed defect tickets initiated by the Department to correct technical system errors identified in our prior audit that prevented users from completing certain functions within the RA System. In response to our audit inquiry, Department management provided us with status updates on each of the defect tickets and, where applicable, their resolution. We noted that some defects had been remediated and, according to Department management, others could not be reproduced.

Department management indicated that as of February 5, 2019, there were 630 outstanding defect tickets related to technical system errors and other RA System defects. While the Department initiated defect tickets to record technical system errors and other RA System defects, the Department did not have procedures or a process in place to identify and analyze data related to the technical system errors and other system defects to gain an understanding of error frequency, error spike rates, shared commonalities among system errors, potential aggregate criticality, or total number of users affected. As a result, the Department's process for identifying, analyzing, and correcting technical system errors and other system defects may cause duplicative work and prolong the timeframe for ensuring the completeness, accuracy, and availability of RA System data.

A proactive approach to identifying and analyzing RA System technical system errors and other defects would help ensure that technical system errors and other defects are timely resolved, and future RA System processing is not hindered.

Recommendation: We recommend that Department management continue efforts to identify and correct technical system errors and other RA System defects and implement procedures for analyzing system error and exception data to facilitate a root cause analysis of underlying system issues.

Finding 10: Interface Controls

Effective interface controls include reconciliations between the source and target systems to help ensure that interfaces are complete and accurate. As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 12, we noted that four key data exchange interfaces were not reconciled between the source and target systems to ensure that the data transfers were complete and accurate.

Our audit follow-up procedures disclosed that two of the data exchange interfaces were no longer required and one data exchange interface was now being reconciled. While the other key data exchange interface had the needed header and trailer records on the interface file, reconciliation procedures did not prevent the file from being processed when the header and trailer records did not match. In response to our audit inquiries, Department management indicated that they had begun the initial process of reviewing interface reconciliation procedures and implementing needed changes but, due to the large volume of interfaces and limited resources, they had not completed the implementation of interface reconciliation procedures for all data exchange interfaces.

The lack of reconciliation procedures for data exchange interfaces increases the risk that incomplete or inaccurate data may be exchanged with the RA System and not be timely detected.

Recommendation: We recommend that Department management continue to review reconciliation procedures for the RA System data exchange interfaces and, as appropriate, implement changes.

Finding 11: RA System Screens and Reports

Effective output controls include procedures to ensure that output is provided timely and in compliance with applicable laws and regulations and is reviewed for reasonableness and accuracy prior to distribution. As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 12, we noted that some RA System online screens and reports continue to contain information that was inaccurate or inadequate for its intended purpose. Specifically, we found that although the Department identified a defect in which adjudicator names were being inappropriately removed from a claim issue after the issue had been determined and updated to a determined or distributed status, the defect ticket had not been prioritized.

Department staff also provided examples of the claim issue summary screen incorrectly displaying the name of the Department employee originally assigned a claim issue instead of the name of the employee who processed the claim issue. The removal of the name or incorrect identification of the responsible employee affects the completeness and accuracy of RA System screens and related reports, limiting the Department's ability to use these reports for their intended purposes.

Also, in response to our audit inquiries, Department management indicated that display issues were no longer occurring; however, our cursory review of open defect tickets identified seven defect tickets related to RA System display issues. Appropriate controls for RA System screens and reports are essential for accurate and appropriate reporting of claims data.

Recommendation: We recommend that Department management continue efforts to identify and correct defects related to the accuracy and completeness of information included in RA System screens and reports.

Finding 12: Overpayments and Charges

Automated application controls help ensure consistent treatment of data and 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. 2017-039, Finding 13, we noted that the Department experienced deficiencies in the automated controls and processing of data in the RA System causing inaccurate and erroneous claimant benefit payments, claimant overpayment charges, and employer charges in the RA System. In response to our audit inquiry regarding the status of corrective actions for this finding, Department management provided documentation of program changes implemented to correct the RA System functionality defects related to employer chargeability processing issues, appeal decisions that resulted in erroneous claim benefit payments and employer charges, and other erroneous employer charges above the maximum charge amount or for benefit payments made in error. While the Department made progress in correcting some identified RA System functionality defects, not all identified defects had been corrected. Department management acknowledged that

RA System claim processing deficiencies continue and that such deficiencies result in inaccurate claimant benefit payments, claimant overpayment charges, and excess employer charges.

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

Recommendation: To prevent inaccurate and erroneous claimant benefit payments, claimant overpayment charges, and excess employer charges from being generated by the RA System, we continue to recommend that Department management enhance RA System automated controls and improve the processing of data.

Finding 13: Security Control Documentation and Procedures

Agency for State Technology (AST) rules[13] require each agency to manage the identities and credentials for authorized devices and users and establish control measures that address information steward responsibilities that include administering access to systems and data based on documented authorizations. Effective access authorization practices include, among other things, the use and maintenance of access authorization forms to document the user access privileges authorized by management. AST rules[14] also require information system owners to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits. Effective security controls include the establishment and ongoing review of security policies and procedures to manage and protect IT resources.

As similarly noted in prior audits of the Department, most recently in our report No. 2017-039, Finding 17, certain controls related to security control documentation and procedures need improvement. Specifically, we noted that:

- The Department used the *CONNECT Security Agreement* (*Agreement*) as the authorization form for supervisors to request access privileges to the RA System for Department and contractor employees. However, the *Agreement* did not provide for specific role-level authorization and did not list or otherwise identify the RA System access roles available for the supervisor to authorize for assignment to the RA System user accounts. Consequently, the roles authorized by the supervisor were not documented. In response to our audit inquiry, Department management indicated that the Department Security Officer conferred with the user's supervisor to determine which roles to assign a user based on the user's position and primary functions. To corroborate our understanding, we selected and reviewed five *Agreements* to determine whether the access roles granted to Department and contractor employees assigned RA System access were appropriately authorized and documented. For the five *Agreements* we reviewed, the specific access authorized and assigned was not included on the *Agreements* and the information contained on the *Agreements* was not specific enough to identify the multiple access roles assigned to each user. In response to our audit inquiry, Department management indicated that they initially used the position description as the role designation, but, now that there are new and multiple RA System roles assigned to Department and contractor employees, the position

[13] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[14] AST Rule 74-2.003(5)(g)5., Florida Administrative Code.

description does not sufficiently identify the relevant roles and the *Agreement* has not been updated to reflect the roles.

- The RA System had a predefined set of access roles for each business unit security officer to select from to assign to the Department and contractor employees in the applicable business unit. While the Department developed the *Departmental Security Officer Quick Reference Guide* (*Security Guide*), neither these procedures nor any other security procedures identified the appropriate access roles or the incompatible access role combinations for each position within each business unit. Also, neither the *Security Guide* nor any other security procedures provided guidance for assigning a business unit access role to a user in a different business unit or to an external user. In response to our audit inquiry, Department management indicated that the conflicting RA System roles and functions have not been identified and the procedures cannot be updated until the conflicting roles and functions have been identified.
- The Department had not developed and implemented procedures for conducting Department security investigations of suspicious activities that may be indicative of identity theft or other fraud. The Department uses the FIRRE System in conjunction with the track data access function in the RA System to investigate suspicious claim activities. While Department management developed three guides related to the FIRRE System: *FIRRE Procedure Quick Reference Guide*, *Verification Quick Reference Guide*, and *Investigator Quick Reference Guide,* Department management had not developed procedures for:
  - Performing the investigations that identified responsibilities for working with the FIRRE System and the track data access function.
  - How to use the track data access function to research suspicious events that may be indicative of claimant fraud.
  - The actions to take when evidence of fraudulent activity or patterns were found.
  - How to document the investigation.

  In response to our audit inquiry, Department management indicated that Department reorganization and the rewrite and updating of security policies and procedures had delayed the development of the FIRRE System procedures.

Adequate security control documentation and appropriate security control procedures help ensure that Department staff will follow the intent of management regarding the appropriate RA System access role assignment and that all suspicious activities of RA System claimants will be thoroughly investigated.

Recommendation: We again recommend that Department management enhance the access authorization forms used to authorize RA System access roles to ensure that the access authorized is sufficiently documented. In addition, Department management should enhance security guides and procedures to identify the access roles applicable to each position as well as the access roles that cannot be combined for the purpose of maintaining an appropriate separation of duties. We also recommend that Department management continue efforts to develop procedures for performing security investigations of suspicious events that may be indicative of claimant fraud.

Finding 14: Periodic Access Reviews

AST rules[15] require agency information owners to review access rights (privileges) periodically based on assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. Policies and procedures should be established to reasonably assure that periodic access reviews are effective.

In prior audits of the Department, most recently in our report No. 2017-039, Finding 18, we noted that the Department had not established or implemented appropriate procedures for the periodic review of user accounts within the privileged access groups of the Department and RA System domains.[16] In response to our audit inquiry regarding the status of corrective actions related to periodic reviews of user access privileges, Department management indicated that they used an administrator tool to conduct a yearly access review of privileged network accounts for the Department's network domain to determine whether access is still required. Department management indicated that they also used the administrator tool to conduct weekly access reviews of privileged network accounts within the RA System production domain. However, the procedures for conducting the annual and weekly access review activities were not documented and the results of the annual or weekly review activities were not retained.

The lack of documented procedures for conducting periodic reviews of privileged network user accounts and evidence of the review activities reduces management's assurance that the periodic reviews are conducted in accordance with management's directives.

Recommendation: We again recommend that Department management document the procedures for periodic reviews of privileged network user accounts within the Department and RA System domains and retain evidence of all review activities.

Finding 15: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. AST rules[17] require that all users be granted access to agency IT resources based on the principles of least privilege and a need-to-know determination. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. Our examination of user access privileges for the RA System disclosed, as similarly noted in prior audits of the Department, mostly recently in our report No. 2017-039, Finding 19, that some access controls need improvement.

As part of our audit procedures, we reviewed the accounts for 50 RA System users assigned one or more of the five roles identified as high-risk by Department management to determine the appropriateness of the access privileges assigned. Our review disclosed that users had been assigned three of the five

[15] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[16] A domain is a form of computer network in which all user accounts, computers, printers, and other security principles, are registered with a central database located on one or more clusters of central computers known as domain controllers.

[17] AST Rule 74-2.003(1)(d)3., Florida Administrative Code.

high-risk roles that were not required for the users' assigned job duties. Based on these role assignments:

- 33 RA System users could update claimant contact information including claimant addresses.
- 3 RA System users could update claimant payment information including check and direct deposit information.
- 43 RA System users could request claimant payments.
- 3 RA System users could update claimant authentication information such as social security numbers.
- 16 RA System users could issue and authorize (release) manual payments.

Assigning access privileges to high-risk functions within the RA System that are inappropriate or not required for the user's job duties increases the risk of unauthorized modification, loss, or disclosure of claimant data.

Recommendation: We again recommend that Department management limit access privileges to the RA System to promote an appropriate separation of duties and to restrict users to only those functions necessary for their assigned job duties.

Finding 16: Change Management Controls

Effective controls over program and data changes ensure that only authorized, tested, and approved changes are implemented into the production environment. Data change management controls promote the accuracy of data fixes, which may consist of data change requests and data support requests. Effective change management controls incorporate the conduct of reconciliations to ensure that the established change management process is followed when the program and data changes are implemented into the production environment.

As part of our audit, we evaluated the Department's program change management controls, data change management controls, and related reconciliations to ensure that all program changes implemented into the production environment followed the Department's change management process. Specifically, we:

- Selected 36 of the 1,057 production application program changes during the period July 11, 2017, through August 30, 2018, and evaluated the adequacy of Department program change management controls. We found that the program change management controls need improvement as documentation was not maintained or available documentation did not contain sufficient information to:
  - Demonstrate that the 36 changes recorded were appropriately authorized.
  - Demonstrate that the 36 changes were appropriately tested.
  - Demonstrate that the 36 program changes were subject to quality assurance testing and by whom.
  - Demonstrate that 33 changes were appropriately approved before being implemented into the production environment.
  - Identify who moved 11 changes into the production environment.

- Selected 21 of the 70 production data change requests (requests for changes to application program code to correct data) made during the period August 1, 2017, through August 16, 2018, to evaluate the adequacy of Department data change management controls. We found that the data change management controls for data change requests need improvement as documentation was not maintained or available documentation did not contain sufficient information to:
    - Demonstrate that 18 change requests were appropriately authorized.
    - Identify the programmer who tested 20 changes.
    - Demonstrate that 18 changes were subject to quality assurance testing and by whom.
    - Demonstrate that 19 changes were appropriately approved before being implemented into the production environment.
    - Identify who moved 20 data changes into the production environment.
- Selected 22 of 3,535 production data support requests (requests for direct changes to production data) made during the period July 3, 2017, through September 11, 2018, to evaluate the adequacy of Department data change management controls. We found that the data change management controls for data support requests need improvement as documentation was not maintained or available documentation did not contain sufficient information to:
    - Demonstrate that 21 data support requests were appropriately authorized.
    - Identify the programmer who tested 22 data support request changes.
    - Demonstrate that 19 data support request changes were subject to quality assurance testing and by whom.
    - Demonstrate that 22 data support request changes were appropriately approved before being implemented into the production environment.
    - Identify who moved 22 data support request changes into the production environment.
- Inquired of Department management regarding the status of corrective actions for findings in previous audits, most recently in our report No. 2017-039, Finding 21, in which we noted that, although the Department used a change management system for managing program changes, the Department had not established controls, such as the use of a reconciliation process, to ensure that all program changes implemented into the production environment followed the Department's change management process. In response to our audit inquiries, Department management indicated that a procedure was implemented on June 5, 2018, to have a change authorization verification meeting every Tuesday to review production program code and data changes previously implemented into the production environment by the database administration (DBA) staff. Department management further stated that the review was accomplished by inspecting the log that records the DBA that used the schema account to move the code into the production environment. The review included asking the DBAs to substantiate their actions while logged into the system with evidence that the change implemented was authorized by a change ticket. In response to our inquiry regarding the completeness of the review, Department management indicated that, while the log is voluminous, they attempt to review as many log entries as possible, as time permits. Notwithstanding this, the procedure was not documented, and Department records did not evidence the weekly reviews conducted.

The absence of appropriate program and data change controls, including documented reconciliations of the program and data changes implemented, increases the risk that program and data changes may not be implemented in a manner consistent with management's expectations.

Recommendation: We recommend that Department management improve change management controls to ensure that only authorized, tested, and approved RA System program and data changes are implemented into the production environment and that reconciliations of the implemented program and data changes are documented.

Finding 17: 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. Similar issues were communicated to Department management in connection with prior audits of the Department, most recently in our report No. 2017-039.

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.

Recommendation: We 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. 2017-039.

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 IT operational audit from March 2018 through October 2018 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 IT controls applicable to the RA System during the period July 2017 through October 2018 and selected actions subsequent thereto*.* The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control 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, all deficiencies disclosed in our report No. 2017-039.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; 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 and controls 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 the IT systems and 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:

- Interviewed Department personnel and reviewed related documentation to obtain an understanding of:
  - The data and business process flows for the RA System, including key sources of data input, interfaces, key application transactions and processes, and key types of application data output.
  - Key security software and processes used to grant, limit, and administer access to the RA System.

  - Key processes and tools used to ensure that RA System program and data change management is adequately implemented.
  - The various methods for user authentication to the RA System (e.g., claimants, employers, staff, etc.) and the logging and monitoring of system and user activity.
  - The RA System crossmatch process for comparing claims with the National Directory of New Hires file as required for the Benefits Accuracy Measurement case investigations.
- Evaluated selected transaction data input controls to determine the status of corrective actions for prior application input audit findings. Specifically, we:
  - Examined defect tickets and inspected RA System screens and documents regarding the accuracy and completeness of postmark and received dates, date sequencing, and mandatory notes fields.
  - Examined defect tickets and inspected RA System screens and documents regarding translation issues on claim applications and fact-finding documents and incorrect error messages.
  - Examined the *Daily Overrides Review* procedures and a daily *Forced Override Report* for evidence of the corrective actions implemented to monitor manual overrides in the RA System.
- Evaluated selected RA System transaction data processing controls to determine the status of corrective actions for prior application processing audit findings. Specifically, we:
  - Examined defect tickets and inspected screen prints and documents for the timely review and indexing of received documents.
  - Examined defect tickets and inspected manual monitoring and review procedures, implemented and planned, related to identifying and correcting claim issues.
  - Examined defect tickets and inspected test documents, other documentation, and correspondence for the timely distribution of written claimant and employer claim notices.
  - Evaluated 40 of the 5,086 determination letters distributed from July 1, 2017, through September 13, 2018, to determine whether claimant notifications for claims locked by the RA System FIRRE processes were timely distributed.
  - Examined defect tickets and inspected test documents and correspondence for the timely and accurate generation of claim issues.
  - Examined defect tickets and inspected related documents for the timely identification and analysis of technical system errors.
  - Examined defect tickets and inspected related documents regarding inaccurate claimant benefit payments, claimant overpayments, and employer charges.
  - Examined defect tickets and inspected related documents regarding inaccurate date calculations during claims processing.
  - Evaluated the current procedures and processes in place and examined documentation and online history audit trails related to resolution of processing errors and data fixes.
  - Examined defect tickets and related test documents and inspected transaction claim logs and related e-mail correspondence for evidence of corrective actions implemented to accurately log claim issues and to ensure that claim issues added to or removed from the Hold Indefinite report were included in the claim logs.

- Examined RA System screen prints, e-mail correspondence, and defect tickets related to the replication of output data displayed on screens or used in reports to determine the status of corrective actions for prior application output audit findings.
- Examined RA System interface documentation, interface file header and trailer records, interface processing messages, the interface defect ticket, and related e-mail correspondence to determine the status of corrective actions for prior application interface audit findings.
- Evaluated RA System application design documentation, related artifacts, and data flow diagrams to determine whether the Department maintained complete and accurate documentation representing the current state of the RA System business processes.
- Evaluated selected access controls for restricting, reviewing, and logging and monitoring access privileges to the Department's network. Specifically, we:
  - Examined Department records regarding periodic reviews of users with privileged network accounts.
  - Evaluated whether effective logging and monitoring controls were in place for network administrator activity on the Department's network.
  - Evaluated the appropriateness of access to administrative accounts (service and user accounts). Specifically, we examined the 14 network accounts with membership in the *Enterprise Admins*, *Schema Admins*, *Domain Admins*, or *Administrators* security groups for the Department domain as of June 14, 2018, to determine whether the administrative account access was appropriate.
- Evaluated the appropriateness of selected RA System access privileges and review procedures. Specifically, we:
  - Evaluated whether RA System access privileges were appropriately documented and authorized, and that access procedures were established to reasonably ensure an appropriate separation of duties and that application security logging and monitoring were effective.
  - Evaluated the appropriateness of the 50 RA System users assigned one or more of five high-risk roles. Specifically, we examined all user accounts assigned the *SuperUser*, *RACB Super*, *SuperRole*, *SuperStaff*, or *BOPS Super* roles as of June 8, 2018, to determine whether RA System user access to the sensitive roles was appropriate.
  - Examined Department procedures and processes for monitoring the assignment of RA System user access.
  - Examined Department procedures and processes for monitoring activity performed by users assigned one high-risk RA System access role.
  - Examined Department procedures and processes to assess whether RA System owners periodically reviewed access to ensure continued appropriateness and compared the list of 343 employees who separated from Department employment during the period July 4, 2017, through June 7, 2018, to the list of user accounts defined in the RA System as of June 8, 2018, to determine whether the list included former employee user accounts that remained active after the employees' separation dates.
- Examined RA System program and data change procedures and processes and evaluated the effectiveness of program and data change controls to ensure that program and data changes are authorized, tested, and approved for the production environment. Specifically, we:
  - Examined 36 of 1,057 production deployment logs indicating changes to the application during the period July 11, 2017, through August 30, 2018, to determine whether application changes

    were appropriately authorized, tested by the programmer, tested by quality assurance, approved before being moved into the production environment, and moved into the production environment by an appropriate individual.

  - Examined 21 of 70 data change requests during the period August 1, 2017, through August 16, 2018, and 22 of 3,535 support requests from July 3, 2017, through September 11, 2018, to determine whether data fixes were appropriately authorized, tested by the programmer, tested by quality assurance, approved before being moved into the production environment, and moved into the production environment by an appropriate individual.

- Evaluated identification and authentication controls for the Department's network and the RA System and the underlying infrastructure.

- Evaluated the adequacy of controls that protect sensitive RA System resources. Specifically, we evaluated:

  - The five database administrative accounts with update access privileges to the database as of May 3, 2018, to determine whether access privileges to the production database were appropriate.

  - The appropriateness of access privileges to three shared database administrative accounts including whether access was timely removed as of May 16, 2018, for former employees, contractors, and reassigned staff.

  - Logging and monitoring controls for database administrative accounts.

- 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***.

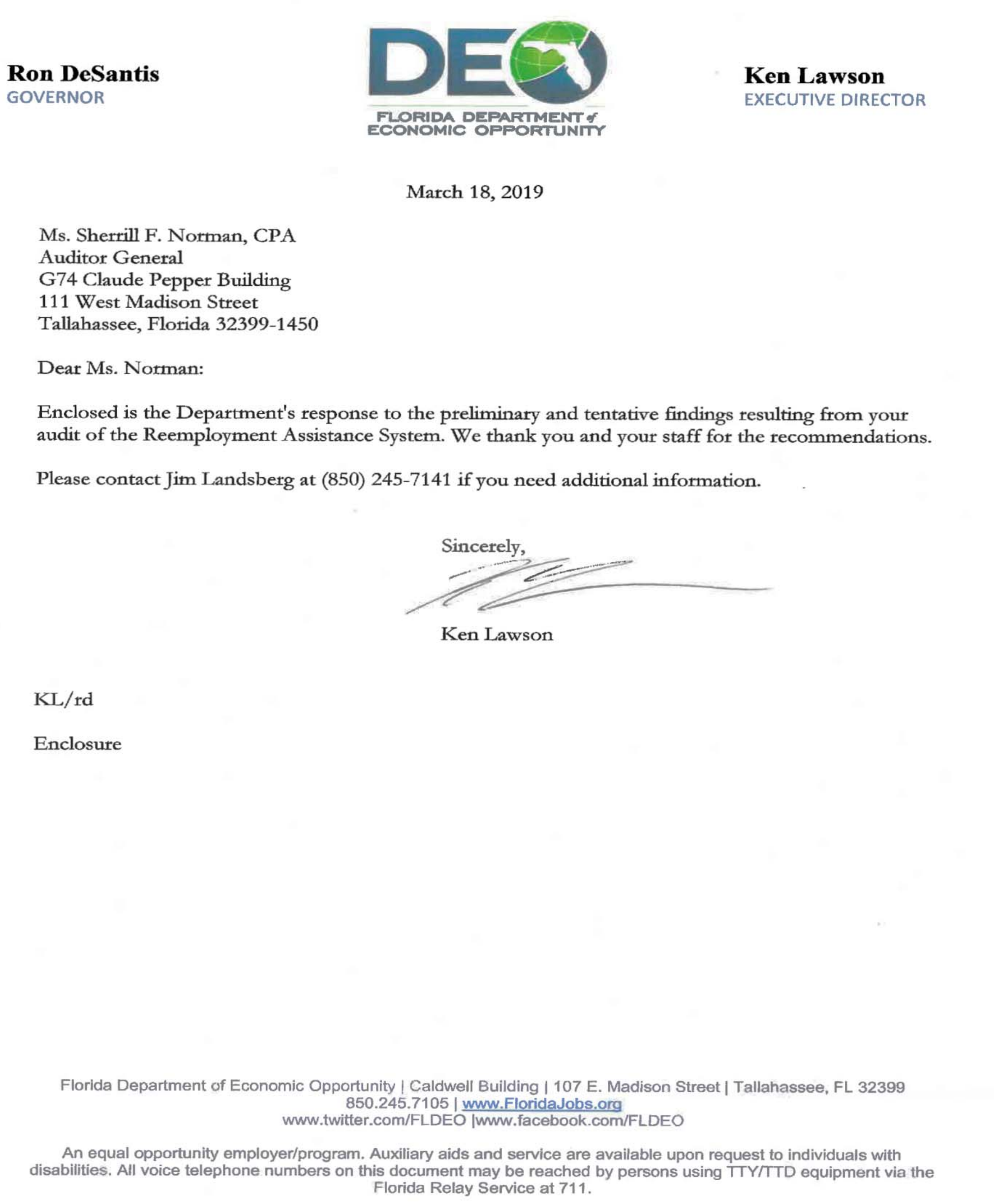
AUTHORITY

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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



Ron DeSantis
GOVERNOR

DEO
FLORIDA DEPARTMENT of
ECONOMIC OPPORTUNITY

Ken Lawson
EXECUTIVE DIRECTOR

March 18, 2019

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's response to the preliminary and tentative findings resulting from your audit of the Reemployment Assistance System. We thank you and your staff for the recommendations.

Please contact Jim Landsberg at (850) 245-7141 if you need additional information.

Sincerely,

Ken Lawson

KL/rd

Enclosure

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 (FDEO)
Reemployment Assistance Information Technology Operational Audit
Responses to Preliminary and Tentative Findings

Finding 1: Application Design Documentation

Auditor Recommendation: We recommend that Department management continue to update and maintain the RA System application design documentation, related artifacts, and dataflow diagrams to help management ensure that the RA System continues to align with management's business requirements.

FDEO Response: The Department will continue to update RA System design documentation and complete dataflow diagrams of the RA System.

Finding 2: Use of Social Security Numbers

Auditor Recommendation: We again recommend that, in the absence of establishing an imperative need for the use of SSNs as RA System claimant user IDs and to reset claimant PINs, Department management take appropriate steps to eliminate the use of SSNs for these purposes.

FDEO Response: The Department will continue to evaluate system enhancements to potentially eliminate the use of SSNs for login purposes and to reset claimant PINs.

Finding 3: Passwords

Auditor Recommendation: We again recommend that Department management establish appropriate authentication controls for RA System claimants to help ensure the confidentiality, integrity, and availability of RA System data and related IT resources.

FDEO Response: 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.

Finding 4: Application Edits

Auditor Recommendation: We again recommend that Department management improve application edits to help ensure the accuracy and integrity of the dates in the RA System.

FDEO Response: The Department will continue to evaluate system enhancements to eliminate the need for a manual process when scanning and indexing documents into the RA System.

Finding 5: Input Forms, Documents, and Messages

Auditor Recommendation: To help ensure the completeness, accuracy, and validity of the RA System input data, we again recommend that Department management continue efforts to implement effective controls related to language translations on forms and documents and enhance the appropriateness of error messages.

FDEO Response: The Department continues to review and update language translations on forms and documents as needed, as well as address the appropriateness of error messages. This project has been prioritized to be completed in 2019.

Finding 6: Timely Review and Processing of Received Documents

Auditor Recommendation: We again recommend that Department management improve procedures for the document intake and indexing processes to help ensure that all documents received for processing in the RA System are timely and accurately indexed to the appropriate claimant, claim, and claim issue to improve the accuracy of claim determinations, benefit payments, and employer charges.

FDEO Response: The Department will continue to develop improved procedures for the document intake and indexing processes.

Finding 7: Timely Distribution of Claim Notices

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct RA System defects and improve the controls over the distribution of written claimant and employer claim notices to help ensure that claim notices are timely distributed.

FDEO Response: The Department will continue to develop improved procedures and identify and correct RA System defects regarding distribution of written claimant and employer claim notices. The Department has identified a manual process for distribution of claim notices. This manual process does not negatively impact RA claimants or employers.

Finding 8: Generation of Claim Issues

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

FDEO Response: The Department will continue to identify and correct any RA System processes related to the appropriate generation of claim issues as encountered.

Finding 9: Analysis of Technical System Errors

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct technical system errors and other RA System defects and implement procedures for analyzing system error and exception data to facilitate a root cause analysis of underlying system issues.

FDEO Response: The Department is continuing to establish and implement procedures for identifying systems errors when they occur.

Finding 10: Interface Controls

Auditor Recommendation: We recommend that Department management continue to review reconciliation procedures for the RA System data exchange interfaces and, as appropriate, implement changes.

FDEO Response: The Department will continue working to implement reconciliation reports for key data exchange interfaces with the RA System.

Finding 11: RA System Screens and Reports

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct defects related to the accuracy and completeness of information included in RA System screens and reports.

FDEO Response: The Department will continue efforts to identify and correct any inaccurate or incomplete information included in screens and reports.

Finding 12: Overpayments and Charges

Auditor Recommendation: To prevent inaccurate and erroneous claimant benefit payments, claimant overpayment charges, and excess employer charges from being generated by the RA System, we continue to recommend that Department management enhance RA System automated controls and improve the processing of data.

FDEO Response: The Department will continue to identify and implement enhancements to the RA System's automated controls to improve the processing of data. This project has been prioritized to be completed in 2019.

Finding 13: Security Control Documentation and Procedures

Auditor Recommendation: We again recommend that Department management enhance the access authorization forms used to authorize RA System access roles to ensure that the access authorized is sufficiently documented. In addition, Department management should enhance security guides and procedures to identify the access roles applicable to each position as well as the access roles that cannot be combined for the purpose of maintaining an appropriate separation of duties. We also recommend that Department management continue efforts to develop procedures for performing security investigations of suspicious events that may be indicative of claimant fraud.

FDEO Response: The Department is updating the authorization forms for RA System access and continues to enhance procedures to identify the access roles for RA positions. The Department will continue working to implement procedures and review processes to identify fraudulent activities.

Finding 14: Periodic Access Reviews

Auditor Recommendation: We again recommend that Department management document the procedures for periodic reviews of privileged network user accounts within the Department and RA System domains and retain evidence of all review activities.

FDEO Response: The Department continues working to establish and implement procedures that will provide a monthly review of privileged network user accounts, which will include documenting the review process and steps taken during each monthly review.

Finding 15: Appropriateness of Access Privileges

Auditor Recommendation: We again recommend that Department management limit access privileges to the RA System to promote an appropriate separation of duties and to restrict users to only those functions necessary for their assigned job duties.

FDEO Response: The Department continues working to establish and implement procedures that will document the review process and limit access privileges in the RA System.

Finding 16: Change Management Controls

Auditor Recommendation: We recommend that Department management improve change management controls to ensure that only authorized, tested, and approved RA System program and data changes are implemented into the production environment and that reconciliations of the implemented program and data changes are documented.

FDEO Response: The Department will continue working to improve change management controls by implementing a change process that captures approval of the deployment package prior to migration. These approvals will be stored, and the Department will continue to improve our documentation throughout the system change process.

Finding 17: Other Security Controls – Logical Access, User Authentication, and Logging and Monitoring

Auditor Recommendation: We 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.

FDEO Response: The Department will continue efforts to ensure that the current security measures are reviewed and tested on a regular schedule. The Department strives to improve security controls to ensure confidentiality, integrity, and availability of RA System data and related IT resources.