STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-039
November 2016

DEPARTMENT OF ECONOMIC OPPORTUNITY

Reemployment Assistance Claims and Benefits Information System

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.

Theresa “Cissy” Proctor	From January 9, 2016
Jesse Panuccio	To January 8, 2016

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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

www.myflorida.com/audgen

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

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. 2015-107. Our audit disclosed the following:

Finding 1: The Department did not maintain current RA System application design documentation to help management 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 require the use of a social security number (SSN) as the user identification code (user ID) 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 input edits continue to need improvement to ensure the validity and reliability of RA System data.

Finding 5: Standardized input forms and documents and error messages within the RA System continue to need improvement to ensure the completeness, accuracy, and validity of the RA System data.

Finding 6: The Department lacked adequate document intake and indexing procedures to provide assurance that documents received by the Department for processing in the RA System were timely and accurately indexed to the appropriate claimant, claim, and claim issue.

Finding 7: The Department had not implemented appropriate procedures to monitor manual overrides applied to transactions in the RA System to ensure that the overrides were restricted to authorized personnel and were appropriate.

Finding 8: The Department had not implemented appropriate monitoring procedures for claim issues to promote the timely resolution and processing of benefit claim issues and payments and to ensure that determinations were based on accurate data.

Finding 9: RA System processes and Department monitoring procedures related to written claimant and employer claim notices continue to need improvement.

Finding 10: RA System processes related to system-generated claim issues continue to need improvement.

Finding 11: RA System users encountered technical system errors that prevented or hindered the processing of RA System data.

Finding 12: Department controls related to RA System reports and interfaces continue to need improvement.

Finding 13: RA System automated controls and processes continue to need improvement to reduce the risk of inaccurate and erroneous claimant benefit payments and employer charges that may affect the integrity of RA System data.

Finding 14: RA System-generated dates were not always calculated accurately, which may adversely affect claimant and employer required response times.

Finding 15: RA System application controls continue to need improvement to reduce the necessity for data fixes.

Finding 16: RA System transactions were not always recorded completely and accurately. Specifically, some transactions were not recorded in the RA System claim logs or the information recorded in the RA System claim logs was not an accurate reflection of the transactions.

Finding 17: Certain security controls related to access authorization documentation and access control procedures continue to need improvement.

Finding 18: The Department had not established or implemented procedures for the periodic review of certain user access privileges related to the RA System. Therefore, management's assurance that user access privileges related to the RA System are authorized and appropriate is limited.

Finding 19: Some access controls related to RA System and Department domain 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 20: Department controls related to shared access accounts continue to need improvement to provide for individual accountability for system activities.

Finding 21: RA System program change controls continue to need improvement to ensure that all program changes follow the Department's change management process when moved into the production environment.

Finding 22: Certain security controls related to user authentication, access controls, and logging and monitoring for the RA System data 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 Florida's Reemployment Assistance (RA) Program[1] which provides temporary 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

[1] The RA Program replaced the former Unemployment Compensation Program.

an efficient first level appeals process to claimants and employers, and register employers liable for the payment of RA taxes or the reimbursement of claims.

Pursuant to State law,[2] the Department launched the Reemployment Assistance Claims and Benefits Information System (RA System, also known as CONNECT), 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), and other State and Federal agency staff. The RA System interfaces with various State and Federal systems as needed to process and report data applicable to the RA Program.

RA Program Process

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, notices of claims (claim notices) are distributed to employers.

Depending on the nature of a claim and the data entered by the claimant, the RA System may generate one or more claim issues. *Claim issue* is a term used by the Department to denote something that will need to be reviewed or resolved before a claimant is considered eligible to receive benefit payments. The review or resolution of the claim issue is referred to as adjudication.

Claim issues are automatically or manually created in the RA System and can be auto-adjudicated based on the predefined functionality of 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. If a claim is not auto-adjudicated, Department adjudicators or other staff are required to review the claim issues and determine if a claim may be approved or rejected. If the claim is approved, a monetary determination is made, a notice is distributed to the claimant and applicable employers, and the claim is processed for payment. If the claim is rejected, a nonmonetary determination is made, a notice is distributed to the claimant, and the claim is not processed for payment. The claimant or employer may request an appeal with the Department regarding both monetary and nonmonetary determinations.

Throughout the RA process, there are a variety of activities that are required by law in order 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

[2] Section 443.1113, Florida Statutes.

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, the postmark date if mailed through the United States Postal Service is considered the file date for an appeal, the received date is used to determine if requested documents are timely received, the date on which 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 analysis, 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.

In our report No. 2015-107 (finding No. 1), we disclosed that since the original business process flows design documentation was created in 2010, the Department had not updated high-level business process flows to reflect the current state of the overall RA System design. In response to our audit inquiries regarding the status of corrective actions taken by the Department, Department IT management provided a partially completed draft data flow diagram of the RA System.

Without complete and accurate RA System application design documentation that represents the current state of RA System business processes, the risk is increased that the RA System may not align with management's business requirements.

Recommendation: We recommend that Department management maintain current RA System application design documentation to help management ensure that the RA System continues to align with management's business requirements.

Finding 2: Use of Social Security Numbers

The Legislature has acknowledged in State law[3] that a person's social security number (SSN) was never intended to be used for business purposes. However, over time the SSN has been used extensively for identity verification and other legitimate 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[4] 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. 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.

In our report No. 2015-107 (finding No. 2), we noted that SSNs were required to be used as user identification codes (user IDs) by claimants to log on to the RA System; however, the Department had not established an imperative need to use SSNs as user IDs. Our audit follow-up procedures disclosed that the Department still requires claimants to use SSNs to log on to the RA System and has not established an imperative need to use SSNs as user IDs for the RA System. Additionally, our review of program change documentation disclosed that, although the Department was in the process of developing an RA System program change that would allow claimants to use a unique RA System-generated user ID instead of their SSN, the program change would not eliminate the use of an SSN as the user ID but merely provide the claimant the option of using either the unique RA System-generated user ID or their SSN as their user ID. Also, the Department did not provide a date by which the program change would be completed and implemented into the production environment.

The use of SSNs as claimant user IDs increases the risk of improper disclosure of SSNs and does not comport to the statutory restrictions on the use of SSNs.

Recommendation: We again recommend that, in the absence of establishing an imperative need for the use of SSNs as claimant user IDs for the RA System, Department management take appropriate steps to establish another identifier for claimant user IDs.

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

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

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

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.[5]

Our review of the RA System claimant logon screens and the *DEO CONNECT Claimant Guide* disclosed that the RA System was designed to require claimants to enter their SSN, as noted in Finding 2 of this report, and a four-digit numeric password in order to log on to the RA System. Thus, the RA System 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. A similar finding was communicated to Department management in connection with our report No. 2015-107.

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.

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

Finding 4: Application Input Edits

Effective input controls include application edits to provide reasonable assurance that erroneous data is detected before processing. Appropriate edits to reasonably assure that data is valid and recorded in the proper format include, among others, field format controls, required field controls, limit and reasonableness controls, valid combinations of related data field values, and master file matching.

In our report No. 2015-107 (finding No. 4), we disclosed that certain improvements were needed in the RA System application input edits. Specifically, we noted that:

- The postmark and received dates of documents submitted to the Department through the United States Postal Service (mail) or facsimile (fax) were being automatically updated to the current date whenever a document was assigned, reassigned, or indexed in the RA System.
- There were no system edits to ensure that the postmark date entered in the RA System preceded the received date for documents submitted by mail.
- The mandatory notes fields established to promote compliance with the United States Department of Labor (USDOL) Employment and Training (*ET*) *Handbook 301* did not have minimum data entry requirements and could be bypassed by entering a space in the fields.

Our audit follow-up procedures included a review of edits or other controls in each area noted. Specifically, we noted that:

- *Postmark and Received Dates.* In Central Intake, the RA System was populating the received date field with an erroneous default date and Central Intake staff were not recording postmark dates in the RA System or scanning and retaining the envelopes with the postmark dates. In response to our audit inquiry, Department management acknowledged that the RA System was erroneously using default dates as the received dates. Department management further stated that staff have since been instructed to manually enter the postmark date as the received date in

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

the RA System to prevent the RA System from using the default date until such time as the erroneous generation of received dates could be programmatically corrected but did not provide a date as to when the program change would be implemented into the production environment.

- *Postmark and Received Dates Sequencing.* In response to our audit inquiry, Department management indicated that there have been no programmatic changes to the RA System regarding edits to ensure that postmark dates precede received dates for documents submitted by mail.
- *Mandatory Notes Fields*. There continues to be no required minimum number of characters in the mandatory notes fields to prevent the fields from being bypassed. In response to our audit inquiry, Department management indicated that they have no plans to change the functionality of how staff are required to enter notes and that it is a training issue that should be addressed during quality reviews by Department management.

The lack of appropriate application input 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 controls related to application input edits to ensure the accuracy of RA System data and to ensure compliance with *ET Handbook 301*.

Finding 5: Input Forms, Documents, and Messages

Application input controls help ensure that data is valid and recorded in the proper format. Effective 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 detected, reported, and corrected. As similarly noted in our report No. 2015-107 (finding No. 6), our audit procedures disclosed that control deficiencies in the RA System regarding language translations on forms and documents and incorrect error messages exist. Specifically, we found that:

- Some standardized input forms contained inappropriate or inaccurate information. Although in response to our audit inquiries, Department management stated that translation issues noted in report No. 2015-107 (finding No. 6) have been corrected on all claimant pages, we noted subsequent instances where standardized RA claim applications and fact-finding documents were not provided to claimants in their selected language (English, Spanish, or Creole) and some document information was translated inaccurately.
- Error messages used to guide claimants and other users through the RA System, in some instances, were inappropriate or did not properly relate to the encountered input error. Some examples of incorrect error messages noted during our audit included:
    - o A claimant received an incorrect error message in response to completing the Discharged - Intoxication and Use of Intoxicants During Working Hours questionnaire. In completing the questionnaire, the claimant failed to respond to questions 6a and 7a. The error message the claimant received indicated that the claimant had failed to respond to questions 8a and 9a.
    - o A claimant received an error message instead of the appropriate RA System screen. In responding to training questions, the claimant indicated yes to the question regarding being on a scheduled break from training. The claimant received the error message “If you are covered by a training waiver, you cannot participate in a scheduled break. Please review your

answers." Instead, the RA System should have directed the claimant to the *Training Break Certification* screen.

- o A claimant received an error message when entering accurate employment dates during the initial claim process. The claimant received the error message "Employment begin date should be on or after recent application date 11/1/2015." This incorrect error message prevented both the claimant and Department staff from entering accurate employment dates.

Effective controls related to language translations on forms and documents and appropriate error messages are essential to the timely 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 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 proper processing, documents and information received by the Department should be timely linked to the appropriate claimant, claim, and claim issue.

In our report No. 2015-107 (finding No. 7), we disclosed that Department procedures for monitoring unidentified documents in the RA System workflow queues were not adequate to ensure that documents were being timely investigated, identified, and linked to the appropriate claimant, claim, and claim issue. We also identified examples of documents that were not timely and accurately linked to the appropriate claimant, claim, and claim issue, and that the documents scanned into the RA System through the Central Intake mail and fax processes were not being reconciled to the documents indexed[6] to provide reasonable assurance that all received documents were timely processed.

As part of our follow-up procedures, we reviewed the Department's document intake and indexing processes and determined that documents received by mail and fax were manually stored in either the document search folder (claimant documents) or correspondence folders (employer documents) for later indexing by the adjudicators. However, if a document relates to a claim issue that auto-adjudicates, the RA System may inappropriately process a claim or claim issue without consideration of the document since the received documents are not indexed prior to auto-adjudication. Additionally, our audit procedures disclosed that the Department continues to lack procedures to provide reasonable assurance that all received documents were timely and accurately indexed to the appropriate claimant, claim, and claim issue. In response to our audit inquiry, Department management indicated that they had submitted two program change requests related to accurate indexing and document tracking. Although Department

[6] Indexing is a method of cataloging or identifying documents in order to streamline data retrieval with a search algorithm.

management identified these program change requests, Department management provided no evidence to support that these changes and any related procedures were implemented as of March 7, 2016.

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 being timely and accurately indexed to the appropriate claimant, claim, and claim issue and increases the risk of inaccurate claim determinations that may result in erroneous benefit payments and employer charges.

Recommendation: We recommend that Department management improve procedures for the document intake and indexing processes 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 to improve the accuracy of claim determinations, benefit payments, and employer charges.

Finding 7: Manual Overrides

Effective input controls include procedures to monitor manual overrides applied to transactions to ensure that the overrides are restricted to authorized personnel and are appropriate. In our report No. 2015-107 (finding No. 9), we disclosed that the Department did not have procedures in place to monitor manual overrides related to claimant identity verification and that overrides had been made without or before appropriate evidence to verify a claimant's identity was obtained.

In response to our audit inquiries, Department management indicated that the Internal Security Unit (ISU) administrator had established a procedure for monitoring manual overrides in the RA System and ISU staff began reviewing the *Forced Override Report* in April 2016 daily to monitor the appropriateness of manual overrides applied to transactions.

Recommendation: We recommend that Department management continue to execute the newly implemented procedure for monitoring manual overrides applied to transactions in the RA System to ensure that the overrides are restricted to authorized personnel and are appropriate.

Finding 8: Monitoring of Claim Issues

Effective application processing controls include appropriate monitoring procedures to ensure that data is accurately and timely processed. In our report No. 2015-107 (finding No. 10), we disclosed that no one was assigned the responsibility of ensuring that all relevant claim issues were timely created and resolved to ensure that the related claim and benefits were timely processed. We recommended that the Department establish procedures to monitor the status of all claim issues to ensure timely resolution and processing of benefit claims and payments and to ensure that determination decisions are issued based on correct data.

In response to our audit inquiries regarding corrective actions taken by the Department, Department management indicated that they had worked on business process improvements but not a technical improvement related to work assignments. Department management further indicated that procedures were implemented to manually push to the adjudicators any claim issues that could potentially cause the Department to not meet first-pay requirements and that adjudicators could request that claim issues be assigned to them during the claim review process. Although Department management indicated that they had taken measures to improve the manual business processes, our audit procedures disclosed

that benefit claim issues were not always timely resolved and payments were not always timely and accurately processed.

For example, we noted that the Department's monitoring procedures and manual business processes did not timely detect an inaccurate claim processing error in October 2015. Due to an RA System defect that caused an erroneous employer chargeability determination, a claimant was inappropriately disqualified and, therefore, not timely paid benefits. Additionally, because of the erroneous determination, the claimant was charged overpayments for previously paid claim benefits. In response to our April 7, 2016, audit inquiry regarding the correction status of the claimant overpayment charge and the eligibility disqualification related to this claim, Department staff indicated that the issues had not been corrected, but correction attempts would be made. This inaccurate claim processing error may have been timely discovered and corrected with appropriate monitoring of all claim issues related to the claim.

The lack of appropriate monitoring procedures to ensure that data is accurately and timely processed increases the risk of unresolved benefit claim issues and inaccurate payment processing.

Recommendation: To ensure that claim determinations are based on accurate data, we recommend that Department management improve monitoring procedures for relevant claim issues and claims.

Finding 9: 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[7] specifies that the Department shall 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. State law also requires the Department to promptly provide an initial monetary determination notice to the claimant and each base period employer whose account is subject to being charged for its respective share of benefits on the claim.

As similarly noted in our report No. 2015-107 (finding No. 11), RA System processes and Department monitoring procedures related to written claimant and employer claim notice distributions need improvement. Specifically, we noted that:

- During nightly processing, some claim issues remained in an "in progress" status instead of "distributed" after a determination or redetermination was recorded in the RA System for the claim issue. The RA System does not create and distribute determination notices for claim issues that are "in progress." As a result, the RA System processes did not distribute written claimant and employer claim notices for some claim issues potentially denying due process for some claimants.
- Some employer claim notices were not generated and were, therefore, not distributed (electronically or by mail) on the following business day after the claim was determined to be monetarily eligible.
- Contrary to Federal regulations,[8] written claim notices for claimants who were determined ineligible due to a claimant identity issue, identified by the Fraud Initiative Rating and Rules Engine

[7] Section 443.151(3), Florida Statutes.

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

(FIRRE) process,[9] were not distributed to the claimants. We were unable to determine the number of written claim notices that were not distributed as a result of the FIRRE process.

In response to our audit inquiry, Department management indicated that although some defects related to the timeliness of claim notice distributions had been corrected, problems continue to occur. Department management further indicated that RA System functionality related to claimant and employer claim notice distributions is being reviewed to determine the improvements needed to the RA System.

Without appropriate RA System processes and Department monitoring procedures related to the timely distribution of 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 their efforts to identify and correct RA System processes and improve monitoring procedures to help ensure that claim notices are timely distributed to claimants and employers.

Finding 10: Generation of Claim Issues

Data processing controls include procedures to ensure that data is processed completely, accurately, 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. As similarly noted in our report No. 2015-107 (finding No. 12), some RA System claim issues were not system-generated and timely processed as designed.

As part of our follow-up procedures, we reviewed the change request documentation and related defect tickets identified by the Department as the corrective action for claim issues not generated. Our review disclosed that, although the Department had corrected some defects related to claim issues not generated, the Department continued to encounter 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. In response to our audit inquiry, Department management indicated that instances related to the nongeneration of claim issues continue to occur and the root cause had not been identified.

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.

[9] Claims identified as possible fraudulent claims by the FIRRE process that were determined ineligible due to a claimant identity issue were indefinitely locked in the RA System, preventing any future activity on the claims until the claimants contacted the Department. Federal regulations provide that the state agency is required to obtain facts to reasonably ensure the payment of benefits when due prior to a determination of an individual's right to benefits. It is the responsibility of the agency to initiate the discovery of information and this responsibility may not be passed on to the claimant or the employer. Information must be obtained promptly so that the payment of benefits is not unduly delayed. The agency must give each claimant a written notice of any determination that adversely affects his or her rights to benefits.

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 11: Technical System Errors

As similarly noted in our report No. 2015-107 (finding No. 13), claimant and Department users were unable to complete functions in the RA System because of technical system errors. Specifically, we noted RA System defects that:

- Caused a claimant and Department staff to receive technical system error messages when attempting to log on to the claimant's RA System account. The claimant had been unable to successfully log on to the RA System account for 3 days and the assisting Department staff were also unable to successfully log on to the claimant's account. Both the claimant and Department staff received a technical system error message each time they attempted to log on.
- Caused a claimant to receive a technical system error message when attempting to move to the next screen after completing the RA System work authorization information screen. As a workaround, Department staff purged the claimant's record and the claimant was able to successfully complete the application process.
- Caused claimants and Department staff to receive technical error messages when attempting to update and submit weekly wage verification information in response to the Earnings - Weekly Wage Verification Non Fraud questionnaire. As a result, neither the claimants nor Department staff were able to update and submit the weekly wage verification information through the RA System. As a workaround, the claimants faxed the information to the Department.
- Caused some employers to receive technical system error messages when attempting to respond to claim notices using the RA System employer response screens.
- Resulted in the inability of some Department users to view employer information when selecting the employer hyperlink in the eligibility issue details section of a Disaster Unemployment Assistance (DUA) issue.

When a user encountered a technical system error message, the user was required to log off the RA System and then log on again to continue. Generally, technical system errors encountered resulted in a technical system error message each time the user attempted the RA System functional task until the underlying system defect was corrected.

In response to our audit inquiry, Department management indicated that defects noted above were being addressed. Technical errors that prevent users from completing functions in the RA System may compromise the integrity of the data and result in data being processed in the System that is incomplete or inaccurate.

Recommendation: We recommend that Department management continue their efforts to identify and correct technical system errors in the RA System to ensure the completeness, accuracy, and integrity of RA System data.

Finding 12: Reports and Interfaces

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. Effective interface controls include reconciliations between source and target systems to

ensure that interfaces are complete and accurate. In our report No. 2015-107 (finding Nos. 15 and 16), we disclosed that certain key online screens and reports reflected incomplete or inaccurate information and certain key data exchange interfaces were not reconciled.

Our follow-up audit procedures disclosed that, although the Department has taken corrective actions for numerous defects related to RA System reports and interfaces, the Department's controls related to reports and interfaces continue to need improvement. Specifically, we found that:

- Although Department management indicated, in response to our audit inquiry, that the defects previously noted in our report No. 2015-107 (finding No. 15) related to online screens and reports were corrected, some additional screens within the RA System continue to display inaccurate or conflicting information. For example, a claim in the RA System was a non-Florida paying combined wage claim, but the claim was displayed on an RA System screen as a regular unemployment claim. According to Department staff, the program type field on the claimant profile always indicates regular unemployment on the RA System screen because the specific claim designations are only on the back end of the system for reporting and billing purposes. Another example was a claim that was displayed on two different RA System screens with two different type and sub-type designations for the same claim issue. Displaying inaccurate or conflicting information in online screens and reports increases the risk of inaccurate claim determinations.
- As similarly noted in our report No. 2015-107 (finding No. 16), although certain data exchange interfaces had job failure notifications, there were no reconciliations between the source and target systems to ensure that the data transfers were complete and accurate for the four data exchange interfaces we reviewed.

Appropriate controls related to reports and interfaces are essential for accurate claim determinations and complete and accurate data transfers.

Recommendation: We recommend that Department management continue efforts to identify and correct defects related to reports and interfaces and implement reconciliation controls for all data exchange interfaces with the RA System to ensure accurate claim determinations and complete and accurate data transfers.

Finding 13: Overpayments and Charges

Automated application controls help ensure consistent treatment of data and that data processing consistently adheres to management's intention and requirements. As similarly noted in our report No. 2015-107 (finding No. 17), the Department continues to experience deficiencies in the automated controls and processing of data in the RA System. Those deficiencies cause inaccurate and erroneous overpayments and charges to exist in the RA System.

In response to our audit inquiry, Department management stated that, in an effort to correct the prior findings, compensating controls were established to identify claim transactions that, if processed, would likely result in incorrect or erroneous benefit payments or overpayment charges based on Department business rules. However, we noted:

- Inaccurate or erroneous claimant benefit payments, for example:
  - A Claimant was erroneously paid benefits for a week that was after the period of benefit eligibility.

- As a result of a current claim issue being voided, the system erroneously reprocessed a prior claim and paid a claimant weekly benefit payments even though those payments were previously applied to offset prior claim overpayments.
- Some claimants were paid weekly benefit payments that exceeded the maximum benefit amount for the claims.
- Some claimants were paid inaccurate benefit payments because the RA System did not allow identified data errors that would alter the benefit amounts to be corrected until after the incorrect benefits were processed and paid.

- An RA System functionality defect related to employer chargeability processing issues where some claimants were erroneously determined ineligible for claim benefits by the RA System and the claimants were charged overpayments for all prior paid claim benefits.
- RA System functionality defects related to appeal decisions that incorrectly updated the status of the related claims which may result in erroneous claim benefit payments and employer charges. In one logged defect, a claim issue was updated to a status of not applicable instead of the adjudicated status of ineligible when the claim appeal issue was dismissed. A status of not applicable results in an eligible determination for payment purposes.
- RA System functionality defects that resulted in some employers being charged for more than the maximum charge amount or charged for benefit payments made in error.

In response to our audit inquiry, Department management stated that defects had been logged and were being addressed for the issues noted above.

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

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

Finding 14: Date Calculations

As part of the adjudication process, the Department may request additional documentation from claimants and employers (fact-finding documents). State law[10] and Department procedures define the time periods within which such documents must be submitted to the Department. Various dates in the RA System are automatically calculated and used in various processes including benefit eligibility determination, employer chargeability, and benefit payments.

As similarly noted in our report No. 2015-107 (finding No. 18), our audit procedures disclosed that, because of program code errors, the RA System did not always accurately calculate dates. Specifically, we noted that:

- An RA System fact-finding due date only provided a 24-hour response time instead of 48 hours.
- An RA System fact-finding due date was prior to the distributed date of the fact-finding document.
- An RA System claim issue was auto-adjudicated as ineligible before the fact-finding due date.

[10] Section 443.151(3)(a) and (5)(a), Florida Statutes.

In response to our audit inquiry, Department management stated that defects had been logged and were being addressed for the issues noted above. Nevertheless, without accurate due dates for fact-finding documents, data integrity may be compromised and determination decisions may be issued based on incorrect data.

Recommendation: We recommend that Department management continue efforts to identify and correct RA System program code errors to ensure that calculated dates are accurate.

Finding 15: Data Fixes

During the period July 2015 through February 2016, 3,127 data fixes were made to correct RA System data as compared to the 10,878 data fixes we noted in our report No. 2015-107 (finding No. 19) for a similar time interval. Data fixes use program scripts that update the RA System database directly without going through the input and processing controls of the RA System that help to ensure the integrity of RA System data.

Our audit procedures disclosed that data fixes were needed because of errors in the RA System that prevented Department users from inputting and processing data corrections through RA System application processes. A data fix could include one or multiple records depending on the type of correction or change needed. Although procedures were in place for Department staff review and approval of data fixes, the corrections to the data were not subject to the same edits as data input and processed through the RA System. Additionally, although the data fixes were logged in online history audit trails, the data fixes were not logged in the same manner as they would have been had the data been input and processed through regular RA System application processing.

Notwithstanding the decrease in the number of data fixes and procedures in place for the review and approval of data fixes by Department staff, performing corrections and modifications to data outside the regular application controls of the RA System increases the risk that controls designed to ensure the integrity of data may be circumvented and, as a result, the integrity of the data may be compromised.

Recommendation: We recommend that Department management continue efforts to improve the functionality of the RA System to reduce the need to perform corrections and modifications (data fixes) outside the RA System application controls.

Finding 16: RA System Claim Logs

Claim logs are available on claimant profile screens and users can view the logs based on claimant, claim, or other search criteria for researching claim issues. In our report No. 2015-107 (finding No. 22), we noted that the RA System claim logs did not always record complete and accurate information.

Our audit follow-up procedures included inquiries with Department staff and review of RA System claim logs and the related defect tickets. Our procedures disclosed that there continued to be instances where some transactions were not recorded in the RA System claim logs or the information recorded in the RA System claim logs was not an accurate reflection of the transactions. As a result, claim issues may not be resolved or may be incorrectly resolved based on the incomplete or inaccurate information in the claim logs. Specifically, we found that:

- Some relevant transactions were not logged. For example, under certain circumstances, some claim issue modifications, such as claim issues added to or removed from the Hold Indefinite (HDID) Report, were not logged and, therefore, may hinder claim issue tracking.
- In some instances, the claim logs reflected inaccurate information, such as incorrectly attributing actions taken on a claim issue to a particular staff member or indicating the claim issue creation date as the adjudication date.

In response to our audit inquiry, Department management stated that the root cause for the instances noted above has not been identified; however, a defect has been logged. Additionally, Department management stated that instances identified applicable to individual claims are being addressed through data fixes until the defect ticket applicable to the root cause is resolved.

Recommendation: We recommend that Department management continue efforts to identify and resolve the cause of inaccurate RA System claim logs.

Finding 17: Security Control Documentation and Procedures

AEIT rules[11] required that agency information owners be responsible for authorizing access to the information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management and the complete and accurate assignment of user access privileges. Effective security controls also include the establishment and ongoing review of security policies and procedures to manage and protect IT resources. As similarly noted in our report No. 2015-107 (finding No. 24), our audit procedures disclosed certain security controls related to security control documentation and procedures that need improvement. Specifically, we noted that:

- Access roles granted to the RA System users were not appropriately authorized and documented. The Department used authorization forms to document authorization of access roles granted to the RA System users. The authorization forms included the job position of the employee to indicate the access roles that should be granted to the user. However, the authorization forms were not sufficient to provide an adequate control for granting access roles to the RA System users. To corroborate our understanding, we selected and reviewed five authorization forms to determine whether the access roles granted to RA System users were appropriately authorized and documented. We found that, for the five authorization forms we reviewed, the access forms were not specific enough to identify the multiple access roles assigned to each user as the access role names did not match the job position titles and, in some cases, the job position title was not identified.
- Procedures for granting access roles to RA System users need improvement. The RA System had a predefined set of access roles for each business unit that the respective business unit security officer assigned to the business unit's users. Business unit supervisors relied on the

[11] AEIT Rule 71A-1.007(1), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records, property, administrative authority, and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. AST Rule 74-2.003(1), Florida Administrative Code, requires that each agency ensure that access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. AST Rule 74-2.003(5)(g)5., Florida Administrative Code, requires information system owners (ISOs) to define application security-related business requirements using role-based access controls and rule-based security policies where technology permits.

business unit security officers to assign the appropriate access roles to the users. The *Departmental Security Officer Quick Reference Guide* (*Security Guide*) provided the security officers with guidance for granting users RA System access roles. However, neither the *Security Guide* nor any other security procedures identified the appropriate access roles for each position within a specific business unit. Additionally, 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, as evidenced in Finding 19 of this report. Also, the *Security Guide* and other security procedures did not identify access role combinations that were incompatible and in violation of an appropriate separation of duties.

- Procedures for conducting Department security investigations of suspicious activities that may be indicative of identity theft or other fraud need to be developed and implemented. In February 2015, the Department began using the FIRRE System in conjunction with the RA System and its track data access function to investigate suspicious activities of RA System users (both internal and external). Department management developed three guides related to the FIRRE System: *FIRRE Procedure Quick Reference Guide*, *Verification Quick Reference Guide*, and *Investigator Quick Reference Guide*. However, as of February 9, 2016, Department management had not developed procedures for performing the investigations that addressed the individuals responsible for working with the FIRRE System and individuals responsible for working with the RA System track data access function, how to use the track data access function to research suspicious user or claimant events and what to do when evidence of fraudulent activity or patterns were found, or how to document the investigation. In response to our audit inquiry, Department management indicated that they are aware of a need to document these procedures and are in the process of establishing a formal written process.

Absent adequate security control documentation and appropriate security control procedures, management has limited assurance that Department staff will follow the intent of management regarding the appropriate RA System access role assignment and that any suspicious activities of RA System users will be thoroughly investigated.

Recommendation: We recommend that Department management enhance the access authorization forms used to authorize RA System access roles. In addition, we recommend that Department management enhance security 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. Security procedures should also be enhanced to provide guidance for assigning access roles to users in other business units. We also recommend that Department management continue efforts to develop procedures for performing security investigations of suspicious activities of RA System users.

Finding 18: Periodic Access Review

AEIT rules[12] required agency information owners to review access rights periodically based on risk, access account change activity, and error rate. 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.

As of March 22, 2016, the Department had not established or implemented appropriate procedures for the periodic review of user access accounts within the privileged access groups of the Department and

[12] AEIT Rule 71A-1.007(2), Florida Administrative Code. AST Rule 74-2.003(1)(a)6., Florida Administrative Code, required periodic reviews of access privileges based on system categorization or assessed risk.

RA System domains of the Department's network. A similar finding was noted in our report No. 2015-107 (finding No. 25).

Without periodic reviews of user access accounts within the privileged access groups, management's assurance that user access privileges are authorized and appropriate is limited.

Recommendation: We recommend that Department management establish and implement appropriate procedures for the periodic review of user access accounts within the privileged access groups of the Department and RA System domains of the Department's network to ensure that user access privileges are authorized and appropriate.

Finding 19: 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. 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 application and the Department domain disclosed, as similarly noted in our report No. 2015-107 (finding No. 26), that some access controls need improvement.

RA System Application Access

We reviewed RA System access privileges to determine the appropriateness of the access privileges granted for six users with the ability to update driver license or SSN information. We reviewed the access privileges for three users within the Adjudication unit, one user within the Benefits Payment Control unit, and two users within the Tallahassee Contact Center and noted that the two users in the Tallahassee Contact Center had been granted access privileges that gave the users the ability to perform functions that were unnecessary for their assigned job duties. Specifically, we found that:

- For both users, the "Claimant Authentication Summary" function provided a screen that allowed the users to update driver license information.
- For one of the two users, the "Fact-Finding" function allowed for the display of a screen with a "Fact-Finding Documents Received" section that lists documents, such as images of a claimant's driver license or SSN card. However, the screen also allowed documents to be deleted which was unnecessary for the user's assigned job duties.

The users within the Tallahassee Contact Center function as customer service representatives to help claimants understand their claims and any outstanding documentation requirements. They use the RA System to verify the identity of claimants prior to providing assistance and they validate the employment status of claimants. While it is appropriate for these employees to have read access to driver license numbers or SSNs to verify the identity of claimants, they should not have the ability to update or delete this information.

Department Domain Access

A service account is a special user account that an application or service uses to interact with the operating system. Services use the service accounts to log on and make changes to the operating system or configuration. Many service accounts have unnecessary administrator-equivalent privileges. Therefore, service account credentials should not be used for interactive (between a user and a

computer) log-on. As part of our audit procedures, we reviewed the 33 privileged access accounts within the administrator groups for the Department domain as of November 30, 2015, to determine the appropriateness of the access accounts. Our review disclosed that:

- For 17 service access accounts, the service accounts were not restricted from interactive log-on and, if the passwords were known, the privileged access accounts could be used to log on to the Department domain without individual accountability. In response to our audit inquiry, Department management indicated that, while there are several methods that could be used in combination to restrict the logon capabilities for the service access accounts, Department management had not developed plans to analyze how the service access accounts could be restricted.
- For the 17 service access accounts noted above, the accounts had administrative access privileges that were not required for service accounts and, in response to our audit inquiry, Department management indicated that they had not documented the risk and the reasons for granting administrative access privileges to the service access accounts.

Inappropriate or unnecessary access privileges to the RA System and the Department domain increases the risk of unauthorized modification, loss, or disclosure of Department data and IT resources and the inability to assign individual responsibility.

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

Finding 20: Shared Access Accounts

Effective access controls include a process for the unique identification of system users that allows management to affix responsibility for system activity to an individual.

Department Domain Access

As part of our audit procedures, we reviewed the 33 privileged access accounts within the administrator groups for the Department domain as of November 30, 2015, to determine the appropriateness of the access accounts. As similarly noted in our report No. 2015-107 (finding No. 26), we noted that two system administrators shared a user ID and password for authentication for a service access account used to manage the discovery and archiving of content held within two server environments. Individual accountability cannot be assigned for actions taken with a shared privileged access account.

RA System Database Access

Our audit procedures disclosed that, as of December 4, 2015, the four database administrators assigned to the RA System were using two database access accounts and corresponding passwords to perform database administration functions instead of using unique access accounts to provide for individual accountability. Department staff had not created separate user access accounts to be used for database administration for the RA System database.

The lack of individual accountability when accessing RA System data and related IT resources increases the risk of unauthorized modification, loss, or disclosure of RA System data and related IT resources and the sharing of user IDs and passwords may limit the Department's ability to assign responsibility for system activities.

Recommendation: To provide for individual accountability for system activities, we recommend that Department management limit account access privileges to the RA System and related IT resources.

Finding 21: Change Management Controls

Effective controls over program changes ensure that only authorized, tested, and approved program changes are implemented into the production environment. Further, effectiveness of change management controls is enhanced through controls that ensure the change management control process is followed when the program changes are implemented into the production environment.

Our audit procedures disclosed that, although the Department used a change management system for tracking the authorization, testing, approval, and implementation of 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. A similar finding was noted in our report No. 2015-107 (finding No. 30).

Absent effective change management controls to ensure that all program changes are authorized, tested, and approved, the risk is increased that erroneous or unauthorized program changes may be implemented into the production environment and not be timely detected.

Recommendation: We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to the RA System are implemented into the production environment.

Finding 22: Other Security Controls – User Authentication, Access Controls, 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 user authentication, access controls, 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 user authentication, access controls, 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. A similar finding was communicated to Department management in connection with our report No. 2015-107 (finding No. 29).

Recommendation: We recommend that Department management improve certain security controls related to user authentication, access controls, 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. 2015-107.

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 October 2015 through February 2016 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 2015 through February 2016 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. 2015-107.
- 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 system 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 system 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 system 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.
- Obtained an understanding of the RA System data and business process flows, including key sources of data input, key application transactions and processes, and key types of data output related to the application.
- Obtained an understanding of selected security management controls related to the RA System.
- Obtained an understanding of Department procedures for its account management processes for authorizing, creating, modifying, and revoking RA System access.
- Obtained an understanding of the RA System configuration management processes.
- Evaluated the effectiveness of RA System input, processing, and output control procedures to promote the completeness, accuracy, validity, and confidentiality of RA system data and IT resources.
- Examined various RA System defect tickets regarding timely distribution of claim notices, generation of claim issues, technical system errors, reports and interfaces, overpayments and charges, date calculations, and RA System claim logs to determine the status of corrective actions for prior audit findings related to input, processing, and output controls for the RA System.
- Evaluated the effectiveness of selected RA System security management processes for protecting confidential and exempt data.
- Examined selected access privilege controls and review procedures and evaluated the effectiveness of the controls and procedures for restricting access to sensitive IT resources related to the RA System.
- Evaluated the effectiveness of selected access privilege controls to ensure the appropriateness of privileged account access to the Department domain for 33 access accounts as of November 30, 2015. We also evaluated the effectiveness of selected access privilege controls to ensure the appropriateness, as of December 1, 2015, of privileged account access to the RA System production domain for 15 access accounts, the RA System test domain for 19 access accounts, and the RA System development domain for 29 access accounts all.
- Evaluated the effectiveness of selected access privilege controls and determined whether RA System database access privileges granted for the 12 active access accounts as of December 4, 2015, belonged to active employees.
- Examined selected RA System access privilege controls and review procedures and evaluated the effectiveness of the controls and procedures for restricting access to sensitive transactions and activities.

- Evaluated whether the RA System access privileges granted for 5 of 39 users as of April 11, 2016, were appropriately authorized and documented.
- Evaluated the appropriateness of RA System access privileges, as of January 12, 2016, granted for 14 of 138 users.
- Evaluated the appropriateness of RA System access privileges granted to driver license or SSN information for three users in the Adjudication unit as of March 3, 2016, one user in the Benefits Payment Control unit as of March 9, 2016, and two users in the Tallahassee Contact Center as of March 18, 2016.
- Evaluated the effectiveness of selected user identification and authentication controls over the RA System and IT resources.
- Evaluated the effectiveness of selected logging and monitoring controls over the RA System and related IT resources.
- Evaluated the effectiveness of selected configuration management controls related to the RA System.
- Evaluated the effectiveness of data correcting mechanisms applied to selected data conversion inaccuracies.
- 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

Rick Scott
GOVERNOR

FLORIDA DEPARTMENT of ECONOMIC OPPORTUNITY

Cissy Proctor
EXECUTIVE DIRECTOR

October 14, 2016

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 information technology operational audit of the Reemployment Assistance System. We thank you and your staff for the recommendations designed to enhance our continuing efforts to effectively serve the citizens of our State.

If you have additional questions or needs, please contact Jim Landsberg, Inspector General, at (850) 245-7141.

Sincerely,

Cissy Proctor

CP/tc

Enclosure

Florida Department of Economic Opportunity | Caldwell Building | 107 E. Madison Street | Tallahassee, FL 32399
866.FLA.2345 | 850.245.7105 | 850.921.3223 Fax
www.floridajobs.org | www.twitter.com/FLDEO | www.facebook.com/FLDEO

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

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

Finding No. 1: Application Design Documentation

Auditor Recommendation: We recommend that Department management maintain current RA System application design documentation to help management ensure that the RA System continues to align with management's business requirements.

Department of Economic Opportunity (DEO) Response: The Department's business unit continues to work with IT management to update use case documentation and complete data flow diagrams of the RA System. We are scheduled to have this project completed within the next four months.

Finding No. 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 claimant user IDs for the RA System, Department management take appropriate steps to establish another identifier for claimant user IDs.

Department of Economic Opportunity (DEO) Response: The Department implemented an enhancement on September 24, 2016 that allows claimants to log in with their Claimant ID or SSN. The enhancement to further disallow the use of SSNs entirely for login purposes is currently in the development stage. We expect to have this enhancement implemented in production by March 2017.

Finding No. 3: Passwords

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

Department of Economic Opportunity (DEO) Response: The Department is currently developing additional criteria to require claimants to use passwords with more complexity. Passwords would meet requirements to be defined as a complex password. This enhancement will be pursued with Finding No. 2 above related to claimants creating their own unique user IDs. We expect to have this enhancement implemented in production by March 2017.

Finding No. 4: Application Input Edits

Auditor Recommendation: We again recommend that Department management improve controls related to application input edits to ensure the accuracy of RA System data and to ensure compliance with ET Handbook 301.

Department of Economic Opportunity (DEO) Response: Department staff continues to manually enter the postmark date when scanning and indexing documents into the RA System. A fix was entered to have the postmark and received dates of documents corrected from defaulting to the current date. That fix, along with the enhancement to track the "life cycle" of a document when scanned and indexed into the RA System, would address these concerns. This fix is planned, but currently not completed.

The Department also implemented a change on July 23, 2016 regarding the "mandatory notes fields" issue, which requires staff to type at least four alpha characters to enter a note in the RA System.

Finding No. 5: Input Forms, Documents, and Messages

Auditor Recommendation: To help ensure the completeness, accuracy, and validity of the RA System input data, we 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.

Department of Economic Opportunity (DEO) Response: The Department resolved the issue regarding the error message received when entering accurate employment dates. Additional fixes were identified to correct the error messages noted in the finding.

The Department's IT Management currently has a developer assigned to address the standardized input forms. His primary task is to review and update missing or inaccurate fact-finding documentation. The review is being done for all three languages in which the documents are available (English, Spanish, and Creole). Each production deployment includes several of these corrections under one fix.

Finding No. 6: Timely Review and Processing of Received Documents

Auditor Recommendation: We recommend that Department management improve procedures for the document intake and indexing processes 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 to improve the accuracy of claim determinations, benefit payments, and employer charges.

Department of Economic Opportunity (DEO) Response: The enhancement referenced in Finding No. 4 will assist the Department with improving procedures for the document intake and indexing processes as it would track the "life cycle" of a document when scanned and indexed into the RA system.

Finding No. 7: Manual Overrides

Auditor Recommendation: We recommend that Department management continue to execute the newly implemented procedure for monitoring manual overrides applied to transactions in the RA System to ensure that the overrides are restricted to authorized personnel and are appropriate.

Department of Economic Opportunity (DEO) Response: The Department has implemented three levels of security for monitoring manual overrides. This includes: unit supervisors performing random reviews, the Internal Security Unit (ISU) reviewing the *Forced Override Report*, and the fraud unit (FIRRE)

performing reviews. In addition, we have made changes to restrict the amount of staff with override roles to those individuals whose job duties require the roles.

Finding No. 8: Monitoring of Claim Issues

Auditor Recommendation: To ensure that claim determinations are based on accurate data, we recommend that Department management improve monitoring procedures for relevant claim issues and claims.

Department of Economic Opportunity (DEO) Response: The Department continues to work on process improvements as it relates to work assignments. Adjudication Management's business process instructions are to require that the adjudicator review all issues and request assignment of all pending issues on the claim be handled by the same adjudicator. There is an enhancement in our pending inventory to allow for more efficient use of the system for assigning and handling issues by adjudication staff.

Finding No. 9: Timely Distribution of Claim Notices

Auditor Recommendation: We recommend that Department management continue their efforts to identify and correct RA System processes and improve monitoring procedures to help ensure that claim notices are timely distributed to claimants and employers.

Department of Economic Opportunity (DEO) Response: The Department continues to identify and correct sporadic reports received of issues remaining "in progress." A fix for this reported issue is scheduled to be deployed to production on November 19, 2016.

In the instance of certain employer claim notices not "distributed" the following business day, the fix has been identified and will be scheduled for a production build in the near future. Until then, the Department is identifying these notices daily and updating the status nightly in order for the notices to be distributed timely.

An enhancement is scheduled for production on October 29, 2016 that will provide a written notice of determination to claimants determined ineligible due to identity issues identified by the fraud unit (FIRRE).

Finding No. 10: 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.

Department of Economic Opportunity (DEO) Response: A fix for this issue is currently targeted for production deployment on December 3, 2016. The Department will continue to identify and correct the underlying issue until that time.

Finding No. 11: Technical System Errors

Auditor Recommendation: We recommend that Department management continue their efforts to identify and correct technical system errors in the RA System to ensure the completeness, accuracy, and integrity of RA System data.

Department of Economic Opportunity (DEO) Response: The Department continues to work diligently to resolve these issues as reported. A planned process change for the Adjudication unit is scheduled for production in early 2017.

Finding No. 12: Reports and Interfaces

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct defects related to reports and interfaces and implement reconciliation controls for all data exchange interfaces with the RA System to ensure accurate claim determinations and complete and accurate data transfers.

Department of Economic Opportunity (DEO) Response: The Department will continue working to implement reconciliation controls in relation to reports and interfaces.

Finding No. 13: Overpayments and Charges

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

Department of Economic Opportunity (DEO) Response: The Department will continue to identify and implement enhancements to the RA System's automated controls to improve the processing of data. An enhancement was put into production on July 23, 2016 that prevents certain inaccurate and erroneous payments and charges from processing. The functionality issue related to employer chargeability was corrected and deployed to production on March 26, 2016. The appeal issue referenced regarding the not applicable status was resolved in February 2016. In addition, the reference to some employers being charged more than their maximum benefit amount was addressed, and those charges were corrected as of June 2016.

Finding No. 14: Date Calculations

Auditor Recommendation: We recommend that Department management continue efforts to identify and correct RA System program code errors to ensure that calculated dates are accurate.

Department of Economic Opportunity (DEO) Response: The Department will continue to identify and correct the issues noted above. The example referenced in bullet one was actually a cosmetic (screen) error. The RA System was correctly giving the parties 48 hours to respond as the issues were not pushed

to an adjudicator to work until the fact-finding document was received or the 48-hour deadline had passed. For the other two examples referenced, the fix for those issues has been planned.

Finding No. 15: Data Fixes

Auditor Recommendation: We recommend that Department management continue efforts to improve the functionality of the RA System to reduce the need to perform corrections and modifications (data fixes) outside the RA System application controls.

Department of Economic Opportunity (DEO) Response: The Department continues to improve functionality to reduce the need for data fixes. As more time passes since the implementation of the new RA System, there will be less need for data fixes as they are mostly the result of conversion issues. Department staff requesting data fixes are responsible for logging the requests and validating the results in a testing environment prior to approving the data fix for deployment to production. Copies of the validation process are uploaded to our online application lifecycle management system.

Finding No. 16: RA System Claim Logs

Auditor Recommendation: We recommend that Department management continue efforts to identify and resolve the cause of inaccurate RA System claim logs.

Department of Economic Opportunity (DEO) Response: The Department continues to identify and resolve any reports of inaccurate claim logs. An enhancement has been scheduled to track certain claim processes by creating a claim log when these issues are handled. The Department has resolved the issue regarding claim logs not reflecting accurate information as of January 2016.

Finding No. 17: Security Control Documentation and Procedures

Auditor Recommendation: We recommend that Department management enhance the access authorization forms used to authorize RA System access roles. In addition, we recommend that Department management enhance security 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. Security procedures should also be enhanced to provide guidance for assigning access roles to users in other business units. We also recommend that Department management continue efforts to develop procedures for performing security investigations of suspicious activities of RA System users.

Department of Economic Opportunity (DEO) Response: The Department's Internal Security Unit (ISU) is reviewing the recommendations above and is in the process of enhancing access authorization forms. The ISU will work with management to identify roles that should not be combined in order to maintain appropriate separation of duties. Additionally, ISU will work with the FIRRE unit to develop procedures for performing security investigations within the RA System.

Finding No. 18: Periodic Access Review

Auditor Recommendation: We recommend that Department management establish and implement appropriate procedures for the periodic review of user access accounts within the privileged access groups of the Department and RA System domains of the Department's network to ensure that user access privileges are authorized and appropriate.

Department of Economic Opportunity (DEO) Response: The Department continues to work to ensure access privileges are authorized and appropriate through a semi-annual review of user accounts, as well as daily/weekly review of the RA System track data access functionality. The Internal Security Unit will enhance its semi-annual user access review procedures to provide additional guidance for reviewing user accounts.

Finding No. 19: Appropriateness of Access Privileges

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

Department of Economic Opportunity (DEO) Response: The Department continues to conduct periodic reviews of access privileges for the RA System and the Department domain. Reviews are conducted by the Internal Security Unit (ISU), Department security officers, and the fraud unit (FIRRE). In addition, only those users whose job duties require the ability to update or remove necessary information currently have this access.

The Department has also implemented a track data access review within the RA System. Unit supervisors and the ISU review users' transaction history within the RA System weekly. As to service access accounts, the restriction from interactive log-on, and the removal of administrative privileges, the Department will further evaluate potential changes based upon the auditor's recommendations.

Finding No. 20: Shared Access Accounts

Auditor Recommendation: To provide for individual accountability for system activities, we recommend that Department management limit account access privileges to the RA System and related IT resources.

Department of Economic Opportunity (DEO) Response: The Department has created individual user accounts for daily activities. Elevated account privileges are limited and are shared for system maintenance with only a small group of IT professionals. This access, like all access to the system, is tracked in the system logs and is reviewed on a weekly basis.

Finding No. 21: Change Management Controls

Auditor Recommendation: We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to the RA System are implemented into the production environment.

Department of Economic Opportunity (DEO) Response: The Department continues working to establish tighter controls for the change set management. Currently, the Department uses Microsoft's Team Foundation Server (TFS) to manage version control and tracking on the program. The code for the program branch in TFS is locked to prevent any future changes to the code before it is promoted and tested on multiple lower environments. After the testing process is completed and the change management team approves the build, the same code for the program branch in TFS is deployed to production.

Finding No. 22: Other Security Controls – User Authentication, Access Controls, and Logging and Monitoring

Auditor Recommendation: We recommend that Department management improve certain security controls related to user authentication, access controls, 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.

Department of Economic Opportunity (DEO) Response: The Department continues working to ensure that the current security measures are reviewed and tested on a weekly basis. The Department strives to improve security controls to ensure confidentiality, integrity, and availability of RA System data and related IT resources.