REPORT NO. 2013-107
FEBRUARY 2013

DEPARTMENT OF ECONOMIC OPPORTUNITY

REEMPLOYMENT ASSISTANCE PROGRAM

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE DEPARTMENT OF ECONOMIC OPPORTUNITY

Effective July 1, 2011, and allowing for a three-month transition period that ended October 1, 2011, Chapter 2011-142, Laws of Florida, transferred the Agency for Workforce Innovation (with the exception of the Office of Early Learning) to the newly created Department of Economic Opportunity. (The Office of Early Learning transferred to the Department of Education.) Cynthia Lorenzo served as Director of the Agency for Workforce Innovation through September 30, 2011.

The creation, powers, and duties of the Department of Economic Opportunity were established within Section 20.60, Florida Statutes (2011). 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:

Hunting Deutsch	From April 16, 2012
Cynthia Lorenzo	Acting, from February 1, 2012, to April 15, 2012
Doug Darling	From October 1, 2011, to January 31, 2012

The audit team leader was Wayne Revell, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CITP, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF ECONOMIC OPPORTUNITY

Reemployment Assistance Program

SUMMARY

The Department of Economic Opportunity (Department) is responsible for administering the State's Reemployment Assistance (RA) Program, inheriting responsibility for the Program from the Agency for Workforce Innovation effective October 1, 2011. The Unemployment Compensation (UC) System is the system used by the Department to determine eligibility and calculate benefit amounts for individuals seeking unemployment compensation.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to the UC System. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2012-028, relating to IT controls over the UC System.

The results of our audit are summarized below:

SECURITY CONTROLS

Finding No. 1: Some user access privileges relating to the UC System had been granted in excess of what was necessary for the performance of job responsibilities. In addition, Department documentation of supervisor authorization for some user access privileges did not explicitly describe the access privileges that had been granted to the users. Similar findings related to UC System access privileges were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Finding No. 2: The Department did not deactivate the access privileges of some former employees and contractors in a timely manner.

Finding No. 3: Contrary to the State of Florida, *General Records Schedule* requirements for the retention of access control records, the Department did not retain complete Appeals or Benefit Overpayment Screening System (BOSS) access control records.

Finding No. 4: The Department's review of Appeals application access privileges was not sufficiently comprehensive. Similar findings related to reviews of the UC System and related IT resource access privileges were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Finding No. 5: Certain Department security controls were deficient in the areas of security event logging and telecommuting, and needed improvement in the area of user authentication. Similar findings were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Finding No. 6: The Department's *Florida Unemployment Compensation Program Operational Security Plan* contained outdated and inaccurate information related to the UC System security environment. Additionally, there was no evidence of a periodic review of the *Plan* by Department management to ensure its ongoing effectiveness. A similar finding was noted in our report No. 2012-028.

APPLICATION CONTROLS

Finding No. 7: As similarly noted in prior audits of the RA Program, most recently our report No. 2012-028, the UC System needed improvement with regard to editing of data and calculations of certain percentages and amounts to provide increased assurance of the validity of data within the System.

BACKGROUND

The UC System is composed of several interacting subsystems, including the UC Claims and Benefits Subsystem, Appeals, and the Benefit Overpayment Screening System (BOSS). The UC Claims and Benefits Subsystem includes an interface with the debit card system, Electronic Payment Processing Information Control Card (EPPICard). The UC Claims and Benefits Subsystem processes new claims by determining monetary eligibility for benefit payments. It

also determines employers' chargeability for benefits and facilitates the payment of claimant benefits. EPPICard is used to provide benefits to claimants through an electronic debit card program. Benefit payment information is communicated between the UC Claims and Benefits Subsystem and EPPICard through a debit card interface.

When the Department issues a UC benefit determination, an adversely affected claimant or employer may file an appeal regarding eligibility, qualification, experience rate charges, child support deductions, overpayment, or fraud. Appeals is used by the Office of Appeals to track and record actions associated with the appeals process, including the resolution of disputed unemployment compensation claims and tax liability protests. BOSS is an online system used to issue overpayment determinations and agreements, track repayments, and initiate and track recovery efforts.

Chapter 2012-30, Laws of Florida, effective July 1, 2012, renamed the UI Program the Reemployment Assistance (RA) Program.

The Department has undertaken an RA system modernization project, called Project Connect, intended to improve the claims, benefits, and appeals processes. Project Connect is planned to replace the current collection of reemployment assistance systems, some of which are more than 35 years old. According to Department management, in developing Project Connect, the Department is focused not just on new technology but also reengineering processes for improved service to claimants and employers. The project scope addresses all RA functions: initial claims and continued claims, wage determination, adjudication, appeals, benefit payment control, and program integrity. The Department plans for Project Connect, like the current system, to interface with various other State and Federal systems for the data necessary to carry out the RA Program. The planned implementation date of Project Connect is October 28, 2013.

The RA Program is included within the scope of our Statewide audit of Federal awards administered by the State of Florida and the results of that audit, for the fiscal year ended June 30, 2012, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Security Controls

Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. Agency for Enterprise Technology (AEIT)[1] Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized.

Our audit disclosed that some access privileges were granted in excess of what was necessary for the performance of job responsibilities. Specifically, seven IT operations employees had been granted complete domain administrator privileges but only needed a subset of the privileges to perform their job responsibilities. The domain administrator

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

privileges allowed elevated access capabilities over numerous servers within the network domain, including UC servers, and also provided these IT operations employees the capability to modify or delete IT resources residing on servers within the domain, including UC IT resources, outside of the controls of the application or database. A similar finding was noted in prior audits of the RA Program, most recently our report No. 2012-028. In addition, one employee was granted unnecessary update access privileges within Appeals.

The critical nature of the UC System and the presence of confidential information within the UC System data files indicated a need for the Department to further restrict domain administrator privileges within the Department network domain and Appeals access privileges. Absent further restrictions of domain administrator and Appeals access privileges, the risk of unauthorized disclosure, modification, or destruction of UC System data and IT resources was increased.

According to the *Reemployment Assistance Security Manual*, supervisors must submit authorization forms for Department employees and contractors documenting mainframe system access privileges. However, the authorization form did not explicitly document specific access privileges granted to users. Although the authorization forms were available for the 5 debit card interface users included in our audit testing and the 18 Appeals users and 7 BOSS users included in our samples, the forms only documented that the mainframe access had been authorized. No additional documentation was available to demonstrate that access to the debit card interface, Appeals, and BOSS was appropriately authorized. A similar finding was noted in our report No. 2012-028.

Recommendation: The Department should further restrict access privileges to only what is necessary for the performance of job responsibilities. As appropriate, the Department should consider establishing more granular definitions of roles and privileges to enable the assignment of only the necessary subsets of domain administrator privileges to IT operations staff. In addition, the Department should maintain appropriate documentation of supervisor authorization of all specific levels of access privileges that have been granted to employees.

Finding No. 2: Timely Deactivation of Access Privileges

AEIT Rule 71A-1.007(6), Florida Administrative Code, provides that access authorization shall be promptly removed when the user's employment or contractual services is terminated or access to the information is no longer required. Prompt action is necessary to ensure that a former employee, contractor, or others do not misuse the former employee's or contractor's access privileges.

We reviewed the logical access privileges for 491 Department employees and 526 contractors who terminated employment or contractual services during the period October 1, 2011, through June 30, 2012. We determined that 23 former Department employees and 2 former contractors retained their Appeals access privileges after their dates of termination. As of the date of our testing, August 7, 2012, the access privileges had remained active for periods ranging from 40 to 310 days after termination. Additionally, we determined that 1 former Department employee's UC Claims and Benefits Subsystem access privileges had been deactivated as of the date of our testing, but his access privileges had remained active for 31 days after his date of termination. The Department was unable, upon audit inquiry, to determine whether the Appeals access privileges of the 23 former employees and 2 former contractors were used after their dates of termination. Although the UC Claims and Benefits Subsystem access privileges of the 1 former employee remained active after termination, the access privileges were not used after the date of termination. Nevertheless, without timely deactivation of former employee or contractor access privileges, the risk is increased that the access privileges could be misused by the former employees, contractors, or others.

Recommendation: The Department should enhance its practices to ensure that the Appeals and UC Claims and Benefits access privilege of all former employees and contractors are deactivated in a timely manner.

Finding No. 3: Access Controls Records Retention

The State of Florida, *General Records Schedule GS-1-SL for State and Local Government Agencies (General Records Schedule*), revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the *General Records Schedule* requirements, the Department did not retain complete Appeals or BOSS access control records. Specifically, the Department did not retain logs that would provide the dates when user access privileges were removed or the access privileges that had been granted to former Appeals or BOSS users.

Without the adequate retention of access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements.

Recommendation: The Department should retain complete Appeals and BOSS access control records as required by the *General Records Schedule*.

Finding No. 4: Periodic Review of Access Privileges

Periodic review of user access privileges helps ensure that user access privileges remain appropriate. Users of the UC System, including Appeals, included both Department employees and contractors.

The Department's periodic review of Appeals application access privileges was not sufficiently comprehensive, as it was limited to only a sample of Appeals users. As demonstrated by the inappropriate access privileges disclosed in Finding Nos. 1 and 2, the lack of comprehensive periodic reviews of access privileges increased the risk that inappropriate access privileges may not be timely detected or deactivated that could result in unauthorized disclosure, modification, or destruction of UC data and IT resources. Similar findings regarding the periodic review of access privileges were noted in our report No. 2012-028.

Recommendation: The Department should conduct comprehensive periodic reviews of Appeals application access privileges.

Finding No. 5: Security Controls – Security Event Logging, Telecommuting, and User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls that were deficient in the areas of security event logging and telecommuting, and needed improvement in the area of user authentication. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Similar findings were communicated to Department management in connection with prior audits of the RA Program, most recently our report No. 2012-028. Without adequate security controls in the areas of security event logging, telecommuting, and user authentication, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls in the areas of security event logging, telecommuting, and user authentication to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 6: UC Operational Security Plan

Effective security management includes the development of security plans to provide an overview of the security requirements for a system and a description of the security controls in place or planned for meeting those requirements. Security plans are to be evaluated and adjusted periodically to ensure that the plans are kept up to date. The *Florida Unemployment Compensation Program Operational Security Plan (Plan)* was approved in July 2006. The *Plan* documents implemented management, operational, and technical security measures for the RA Program and its IT systems. The *Plan* also identifies, among other things, the security roles and responsibilities of persons and organizations that support the operation of the RA Program or utilize its resources. Furthermore, the *Plan* also provides security-related information to help to facilitate the establishment of agreements between the Department and other State organizations that provide infrastructure, development, and operational support to the RA Program.

We noted that the *Plan* contained outdated information including numerous references to systems that no longer exist and a reference to an office that no longer exists. In addition, documents referenced in the *Plan* did not always reflect the most current version of those documents. Furthermore, there was no evidence of a periodic review of the *Plan* by Department management to ensure its ongoing effectiveness. This finding was also noted in our report No. 2012-028. In the absence of a current security plan, the risk is increased that management's IT security objectives will not be effectively communicated or achieved.

Recommendation: The Department should update the *Florida Unemployment Compensation Program Operational Security Plan* to reflect the current system environment and periodically review the *Plan* to ensure its ongoing effectiveness.

Application Controls

Finding No. 7: Programmed Edits

Application controls include programmed edits that evaluate the accuracy, completeness, and validity of input data. As described in the following paragraphs, the UC System needed improvement with regard to editing of data and calculation of certain percentages and amounts. Similar findings were noted in prior audits of the UI Program, most recently our report No. 2012-028.

Certain Appeals data could be erroneously updated or changed using the system's Case Examine function. Specifically, the Cost Center, Adjudication Hub, and Zip Code fields accepted invalid data (e.g., all nines). The lack of data validity edits of the aforementioned fields in Appeals increased the risk of inaccurate and invalid data being accepted into the system and may jeopardize the integrity and reliability of the data.

We also noted instances where the Wage Determination Component of the UC Claims and Benefits Subsystem failed to check the validity of an amount input in one field and did not calculate an additional amount stored in another field. One transaction type allowed user input of the state's maximum benefit amount (MBA). In Florida, the MBA is $6,325. However, the Subsystem allowed the user to input an amount that exceeded the MBA. Under these

conditions, the risk is increased that an excessive dollar amount will be accepted in the Subsystem and relied upon by other states.

The Combined Wage Claim unit determines Florida's UC liability. Wages used in the determination of this liability are automatically provided by the UC Claims and Benefits Subsystem. However, the Combined Wage Claim unit associates must manually calculate the total percentage and maximum chargeable amount related to the liability. The Department's ability to ensure the accuracy of the UC liability would be enhanced if the Subsystem automatically calculated these percentages and amounts. Using manually-calculated instead of system-calculated percentages and amounts increased the risk of incorrect percentages and amounts being used by the Subsystem.

Recommendation: The Department should, where practicable, implement additional edits and system calculations to prevent the entry of invalid data and minimize the risk of calculation errors.

PRIOR AUDIT FOLLOW-UP

The Department had partially corrected two of the findings included in our report No. 2012-028. Corrective actions were not taken for three of the five prior audit findings as described in the findings above.

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 July 2012 through October 2012 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to the UC System 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. An additional objective was to determine whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2012-028.

The scope of our audit focused on evaluating selected IT controls applicable to the UC System. The audit included selected general IT controls over systems modification and logical access to programs and data. The audit also included selected application IT controls and selected user controls relevant to the UC System and the interface with the EPPICard System. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from October 1, 2011, through June 30, 2012, and selected Department actions through October 5, 2012. We also examined the operation of certain relevant IT controls as of July 1, 2011, through September 30, 2011, during which the Agency for Workforce Innovation was responsible for the administration of the UI Program.

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 controls considered.

As described in more detail below, for the IT system and controls included within the scope of the 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 our 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 vendors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the UC System, including the system purpose, goals, and compliance requirements; computing platforms and related hardware; basic data and business flows including the data exchanges with EPPICard; program change management; IT and user organization structure and management, and the Department's security program.
- Obtained an understanding of the logical access controls for the UC System, including user account administration.
- Obtained an understanding of the UC System application and user controls.
- Observed and evaluated key processes and procedures related to the security controls for the UC System, including the Department security program, user account administration procedures, access authorization, appropriateness of user access, timely disabling of access privileges, periodic review of user access privileges, separation of duties, monitoring of appropriateness of security accesses, and documentation of UC system changes.
- Observed and evaluated the effectiveness of key application controls, including programmed edits and data reconciliation.
- Tested the effectiveness of procedures for the review and deactivation of access privileges related to the UC System. Specifically, we identified and tested 491 employees and 526 contractors who terminated employment or contractual services during the period October 1, 2011, through June 30, 2012, to determine if UC Claims and Benefits Subsystem, Appeals, and BOSS access privileges, if assigned, were timely deactivated.
- Evaluated on a sample basis procedures for authorizing, testing, approving, and implementing program changes to the UC Claims and Benefits Subsystem. Specifically, we sampled 10 of 53 program change requests for evidence of authorization, testing, and approval for implementation.
- Tested the effectiveness of procedures for authorizing, testing, approving, and implementing program changes to BOSS. Specifically, we identified and tested the two program changes to BOSS that were submitted and implemented during the period October 1, 2011, through June 30, 2012.

- Evaluated the effectiveness of administrative procedures for account administration of the UC System interface with EPPICard. Specifically, for the five users with administrator access privileges to EPPICard interface, as applicable, we determined whether their access privileges had been authorized, were appropriate for their assigned job duties, and enforced an appropriate separation of duties.
- Evaluated on a sample basis the appropriateness of access privileges for Appeals users. Specifically, we sampled 18 of 173 Appeals users to determine whether their access privileges had been authorized and were appropriate for their assigned job duties.
- Evaluated on a sample basis the appropriateness of access privileges for BOSS. Specifically, we sampled 7 of 62 BOSS users to determine whether their access privileges had been authorized and were appropriate for their assigned job duties.
- Tested the effectiveness of mainframe security password settings to evaluate the effectiveness of the settings in adequately protecting IT resources.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated February 8, 2013, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

Rick Scott
GOVERNOR

FLORIDA DEPARTMENT of ECONOMIC OPPORTUNITY

Jesse Panuccio
EXECUTIVE DIRECTOR

February 8, 2013

Mr. David W. Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, we have prepared the enclosed response to the preliminary and tentative audit findings and recommendations which may be included in your report on Information Technology Operational Audit of the Department of Economic Opportunity's Reemployment Assistance Program for the fiscal year ended June 30, 2012.

We thank you and your staff for the recommendations designed to enhance our on-going efforts to efficiently and effectively serve the citizens of our state.

If you have any questions or require additional information, please contact Mr. Joseph K. Maleszewski, Inspector General at (850) 245-7141.

Sincerely,

Jesse Panuccio

JP/cam

Enclosure

Florida Department of Economic Opportunity The Caldwell Building 107 E. Madison Street Tallahassee, FL 32399-4120
866.FLA.2345 850.245.7105 850.921.3223 Fax www.FloridaJobs.org www.twitter.com/FLDEO www.facebook.com/FLDEO

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Economic Opportunity
Reemployment Assistance Information Technology Audit
July 1, 2011 through June 30, 2012
Revised Response to Preliminary and Tentative Findings

Finding No. 1: Appropriateness of Access Privileges

Some user access privileges relating to the Unemployment Compensation (UC) System had been granted in excess of what was necessary for the performance of job responsibilities. In addition, the Florida Department of Economic Opportunity (Department) documentation of supervisor authorization for some user access privileges did not explicitly describe the access privileges that had been granted to the users. Similar findings related to UC System access privileges were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Auditor Recommendation: The Department should further restrict access privileges to only what is necessary for the performance of job responsibilities. As appropriate, the Department should consider establishing more granular definitions of roles and privileges to enable the assignment of only the necessary subsets of domain administrator privileges to IT operations staff. In addition, the Department should maintain appropriate documentation of supervisor authorization of all specific levels of access privileges that have been granted to employees.

Department Response: Please note that Finding No. 1 focused on two separate groups for user access privileges:

1) Domain Administrator Access; and,
2) Mainframe System Access.

Domain Administrator Access: The Department's Office of Information Systems and Support Services (IT) accepts membership within the domain administrator group for the staff identified as a requirement to perform essential job functions. Furthermore, the passing of a Level II background check is required for all staff to perform these assigned job functions.

There were attempts to remove the staff from the domain administrator group, but this process disrupted the ability of each to manage granted permissions to the domain file share server. Since these permissions are different across this server, the only permissions having global access are those for the domain administrator group. These permissions are operationally required to setup new file share permissions and update permissions due to changes requested by the business units on a daily basis. Removing these staff from the domain administrator group negates the ability to log on and troubleshoot issues, review system logs, take needed corrective action, and ultimately manage servers they are responsible for maintaining.

The Department's Office of Information Systems and Support Services utilizes groups to provide access control, offering a check and balance effect where no single person has access to do something others cannot see. We have also purchased software that will

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Economic Opportunity
Reemployment Assistance Information Technology Audit
July 1, 2011 through June 30, 2012
Revised Response to Preliminary and Tentative Findings

allow for the granular selection of roles and privileges for staff. This software will also improve the ability to manage groups and control staff access. Until implementation of the new software, we will continue to use the domain administrator group for staff to complete essential day-to-day tasks. We expect to implement the new software by October 2013.

Mainframe System Access: The recommendation for Finding No. 1 states, "…the Department should maintain appropriate documentation of supervisor authorization of all specific levels of access privileges that have been granted to employees." The Department is currently reviewing the process by which business units request access to systems and applications. This includes system access authorization forms that document specific access privileges granted to users and the process for obtaining proper authorization. This core process is currently paper-based, which has led to lost and/or missing forms managed by the business units. IT is working with each unit to create an electronic form to centralize this access control process so all future requests are housed in a database repository for ease of management and historical audit control. We plan to implement this process by June 30, 2013.

Finding No. 2: Timely Deactivation of Access Privileges

The Department did not deactivate the access privileges of some former employees and contractors in a timely manner.

Auditor Recommendation: The Department should enhance its practices to ensure that the Appeals and UC Claims and Benefits access privilege of all former employees and contractors are deactivated in a timely manner.

Department Response: The Department concurs with this finding. Training is provided to Resource Access Control Facility security officers when they are designated as security officers. Written guidance is also included in *Internal User Guide for Resource Access Control Facility (RACF) Security Officers*, which requires access to be terminated on the last day of the individual's employment or last day they are in the position. Managers have been reminded to ensure all supervisors restrict access to the minimum required to perform the duties assigned and to ensure security agreement forms are completed properly and access is terminated in a timely fashion when no longer required. Contract managers were also reminded of the Department's requirements.

Finding No. 3: Access Controls Records Retention

Contrary to the State of Florida, *General Records Schedule* requirements for the retention of access control records, the Department did not retain complete Appeals or Benefit Overpayment Screening System (BOSS) access control records.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Economic Opportunity
Reemployment Assistance Information Technology Audit
July 1, 2011 through June 30, 2012
Revised Response to Preliminary and Tentative Findings

Auditor Recommendation: The Department should retain complete Appeals and BOSS access control records as required by the *General Records Schedule*.

Department Response: The Department concurs with this finding. When the BOSS system was developed, it was never designed to incorporate the security protocols cited by the Auditor General. To comply with the *General Records Schedule*, BOSS would require programming modifications. The Department will address the finding with respect to both the overpayment and appeals processes with the implementation of the RA Claims and Benefits Information System (Project Connect), which is scheduled to be deployed during the FY 2013-14.

Finding No. 4: Periodic Review of Access Privileges

The Department's review of Appeals application access privileges was not sufficiently comprehensive. Similar findings related to reviews of the UC System and related IT resource access privileges were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Auditor Recommendation: The Department should conduct comprehensive periodic reviews of Appeals application access privileges.

Department Response: The Department concurs with this finding. The Department's Internal Security Unit for the Division of Workforce Services will conduct more comprehensive periodic review of access privileges of the Appeals application.

Finding No. 5: Security Controls – Security Event Logging, Telecommuting, and User Authentication

Certain Department security controls were deficient in the areas of security event logging and telecommuting, and needed improvements in the area of user authentication. Similar findings were noted in prior audits of the RA Program, most recently our report No. 2012-028.

Auditor Recommendation: The Department should implement appropriate security controls in the areas of security event logging, telecommuting, and user authentication to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Department Response: The Department concurs with this finding. A management decision was made to address enhanced security controls and security event logging through the implementation of Project Connect, when deployed during FY 2013-14. In

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Florida Department of Economic Opportunity
Reemployment Assistance Information Technology Audit
July 1, 2011 through June 30, 2012
Revised Response to Preliminary and Tentative Findings

regard to telecommuting, the Department of Management Services' (DMS) Division of Human Resource Management administers the Telecommuting Program, which is authorized pursuant to s. 110.171, Florida Statutes. The Department is working with DMS to implement DMS' Telecommuting Security Assessment and Roadmap as soon as it becomes available. DMS does not have an estimated time of completion for the assessment and roadmap at this time.

Finding No. 6: UC Operational Security Plan

The Department's Florida Unemployment Compensation Program Operational Security Plan (Plan) contained outdated and inaccurate information related to the UC System security environment. Additionally, there was no evidence of a periodic review of the Plan by Department management to ensure its ongoing effectiveness. A similar finding was noted in our report No. 2012-028.

Auditor Recommendation: The Department should update this Plan to reflect the current system environment and periodically review it to ensure its ongoing effectiveness.

Department Response: The Department concurs with this finding. A final draft RA Legacy System Security Plan (SSP) was completed on January 24, 2013, and was provided to the Workforce Services Internal Security Unit Administrator and the Department's Information Security Manager for final review and editorial comments prior to submitting the plan for approval consideration and execution.

Finding No. 7: Programmed Edits

As similarly noted in prior audits of the RA Program, most recently our report No. 2012-028, the UC System needed improvement with regard to editing of data and calculations of certain percentage and amounts to provide increased assurance of the validity of data within the System.

Auditor Recommendation: The Department should, where practicable, implement additional edits and system calculations to prevent the entry of invalid data and minimize the risk of calculation errors.

Department Response: As has been previously indicated in prior year findings, it is the Department's intention to address this concern with implementation of the RA Claims and Benefits Information System during FY 2013-14.