REPORT NO. 2012-028
NOVEMBER 2011

AGENCY FOR WORKFORCE INNOVATION

UNEMPLOYMENT INSURANCE PROGRAM

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DIRECTOR OF THE AGENCY FOR WORKFORCE INNOVATION

Pursuant to Section 20.50, Florida Statutes, the Agency for Workforce Innovation is created within the Department of Management Services (DMS) and is a separate budget entity, not subject to control, supervision, or direction by DMS in any manner. The Director of the Agency for Workforce Innovation is appointed by the Governor and is the agency head for all purposes. Cynthia Lorenzo served as Director during the period of our audit.

Chapter 2011-142, Laws of Florida, provides that no later than October 1, 2011, with the exception of the Office of Early Learning, the Agency for Workforce Innovation would transition to the newly created Department of Economic Opportunity. The Office of Early Learning would transfer to the Department of Education. This bill was signed into law on June 14, 2011, by the Governor and became law effective July 1, 2011. The creation, powers, and duties of the Department of Economic Opportunity are established within Section 20.60, Florida Statutes (2011). Doug Darling was appointed Executive Director of the newly created Department of Economic Opportunity.

The audit team leader was Art Wahl, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, 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.

AGENCY FOR WORKFORCE INNOVATION

Unemployment Insurance Program

SUMMARY

The Agency for Workforce Innovation (Agency) was responsible for administering the State's Unemployment Insurance (UI) Program during the period of our audit. The Unemployment Compensation (UC) System was the system used by the Agency 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. 2011-021, relating to Agency IT controls over the UC System.

The results of our audit are summarized below:

SECURITY CONTROLS

Finding No. 1: As similarly noted in prior audits of the Agency, most recently our report No. 2011-021, 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, Agency documentation of supervisor authorization for some user access privileges did not explicitly describe the access privileges that had been granted to the users.

Finding No. 2: The Agency's review of UC System and related IT resource access privileges needed improvement. In addition, Agency procedures for the periodic review of access privileges for the UC System and related IT resources existed only in draft form. A similar finding was noted in our report No. 2011-021.

Finding No. 3: Certain Agency security controls were deficient in the area of telecommuting and needing improvement in the area of user authentication. Similar findings were noted in prior audits of the Agency, most recently our report No. 2011-021.

Finding No. 4: The Agency'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 Agency management. A similar finding was noted in our report No. 2011-021.

APPLICATION CONTROLS

Finding No. 5: As similarly noted in prior audits of the Agency, most recently our report No. 2011-021, 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. The ability to provide benefits to claimants through an electronic debit card program was implemented in February 2011 utilizing EPPICard. Benefit payment information is communicated between the UC Claims and Benefit Subsystem and EPPICard through a debit card interface.

When the Agency 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.

The UI 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, 2011, 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 needed in the performance of assigned job responsibilities and document the access privileges that have been authorized. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

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 who had been granted domain administrator privileges did not need domain administrator privileges to perform their job responsibilities. The domain administrator privileges allowed elevated access capabilities over numerous servers within the network domain, including servers that contained UC data and programs, 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. A similar finding was noted in prior audits of the Agency, most recently our report No. 2011-021. In addition, two employees were granted unnecessary update access privileges within the UC Claims and Benefits Subsystem for the debit card interface.

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

According to the *Unemployment Compensation Security Manual*, supervisors must submit authorization forms for Agency 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 five debit card interface users included in our tests, 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 was appropriately authorized.

Recommendation: Management should ensure that the security structure does not inappropriately give access privileges to users who do not require access to accomplish their job responsibilities. In addition, management should maintain appropriate documentation of supervisor authorization of all specific levels of access privileges that have been granted to employees.

Finding No. 2: Periodic Review of Access

Periodic review of user access privileges helps ensure that user access privileges remain appropriate. Written procedures help provide guidance and direction to employees responsible for performing such reviews by allowing for better communication and consistent application of management-intended controls.

Users of the UC System included both Agency employees and contractors. According to Agency security staff, the UC security officers were responsible for ensuring that user access to the UC System was appropriate.

The Agency's review of access privileges for the UC System and related IT resources needed improvement. Specifically, the Agency had not reviewed network or database access privileges on a periodic basis. In addition, the Agency's review of UC System access privileges did not include specific access privileges granted to the UC Claims and Benefits Subsystem, including the debit card interface. The Agency had not reviewed the Appeals Subsystem application access privileges and Agency reviews of the BOSS Subsystem application privileges consisted only of determining whether the privileges of users who were no longer defined to the Agency's e-mail system had been disabled.

The Agency had developed but not yet approved procedures that would require the periodic review of access privileges. As demonstrated by the inappropriate access privileges disclosed in Finding No. 1, the lack of periodic reviews of access privileges increased the risk that inappropriate access privileges may not be timely detected or disabled 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. 2011-021.

Recommendation: Management should approve and follow written procedures that describe management's expectations for the periodic review of access privileges for the UC System and related IT resources.

Finding No. 3: Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Agency security controls that were deficient in the area of 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 Agency data and IT resources. However, we have notified appropriate Agency management of the specific issues. Similar findings were noted in prior audits of the Agency, most recently our report No. 2011-021. Without adequate security controls in the areas of telecommuting and user authentication, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Agency data and IT resources may be subject to improper disclosure, modification, or destruction.

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

Finding No. 4: 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* was approved in July 2006. The *Plan* documents implemented management, operational, and technical security measures for the UI 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 UI Program or utilize its resources. Furthermore, the *Plan* also provides security-related information to help to facilitate the establishment of agreements between the Agency and other State organizations that provide infrastructure, development, and operational support to the UI 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*. A similar finding was noted in our report No. 2011-021. 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: Management 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. 5: 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 Agency, most recently our report No. 2011-021.

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 $7,150. 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 Agency'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: Management 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

Except as discussed in the preceding paragraphs, the Agency had taken corrective actions for findings applicable to the Agency included in our report No. 2011-021. Findings in our report No. 2011-021 applicable to the Southwood Shared Resource Center will be presented in a separate report.

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 during the period April 2011 through August 2011 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, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine the extent to which the Agency corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2011-021 that were applicable to the scope of this audit.

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 modifications 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 EPPICard. Our audit included examinations of various Agency records and transactions (as well as events and conditions) occurring from July 2010 through June 2011.

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; physical and environmental safeguards including disaster recovery; IT and user organization structure and management, and the Agency'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 Agency 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, selected server room physical controls, and documentation of UC system changes.

- Tested the effectiveness of procedures for the review and disabling of access privileges related to the UC System. Specifically, we identified and tested 19 former employees with UC System access privileges who terminated employment between July 1, 2010, and May 9, 2011.
- Observed and evaluated the effectiveness of UC System and Agency network password settings in adequately protecting IT resources.
- Evaluated on a sample basis the effectiveness of Agency procedures for performing background checks on IT contractors. Specifically, we sampled 27 contractors with start dates between July 1, 2010, through June 17, 2011.
- Evaluated on a sample basis procedures for authorizing, testing, approving, and implementing program changes to the UC System. Specifically, we sampled 27 program change requests for evidence of authorization, 17 changes for evidence of testing, and 28 changes for evidence of approval for implementation.
- Observed and evaluated the effectiveness of key application controls, including access violation reports, programmed edits, data reconciliation, and data monitoring.
- Evaluated on a sample basis the appropriateness of access privileges for the UC System. Specifically, we sampled 25 users of the UC system to determine whether they had been granted two access group profiles that provided the ability to enter claims, change addresses, and enter claim payments.
- Tested the effectiveness of logical access controls over domain administration. Specifically, we identified and tested 12 employees with domain administration access privileges to determine whether their access privileges were appropriate for their assigned duties.
- Evaluated the effectiveness of administrative procedures for account administration for the UC System interface with EPPICard. Specifically, for the seven 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.

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 November 10, 2011, the Executive Director of the Department of Economic Opportunity, provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

Rick Scott
GOVERNOR

FLORIDA DEPARTMENT of ECONOMIC OPPORTUNITY

Doug Darling
EXECUTIVE DIRECTOR

November 10, 2011

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 attached response to the preliminary and tentative findings and recommendations which may be included in your report on the Information Technology Audit of the Unemployment Insurance Program as administered by the Agency for Workforce Innovation, for the period July 1, 2010 through June 30, 2011.

Thank you for providing us the opportunity to respond to your preliminary findings. We hope that this response satisfies your requirements. If you have questions or require additional information, please contact James F. Mathews, Inspector General at (850) 245-7141.

Sincerely,

for Doug Darling
Executive Director

DD\ js

Enclosure

The Caldwell Building 107 E. Madison Street Tallahassee, Florida 32399-4120
850.245.7105 TTY/TDD 1-800-955-8771 Voice 1-800-955-8770 *FloridaJobs.org*

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Economic Opportunity (DEO)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2010 through June 30, 2011
Response to Preliminary and Tentative Findings

Finding No. 1: Appropriateness of Access Privileges

As similarly noted in prior audits of the Agency, most recently our report No. 2011-021, 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, Agency documentation of supervisor authorization for some user access privileges did not explicitly describe the access privileges that had been granted to the users.

Auditor Recommendation: Management should ensure that the security structure does not inappropriately give access privileges to users who do not require access to accomplish their job responsibilities. In addition, management should maintain appropriate documentation of supervisor authorization of all specific levels of access privileges that have been granted to employees.

DEO Response: The Department concurs with this finding. AWI/DEO reduced the number of Domain Administrators from twenty-one to twelve, a 45% reduction. A review was conducted by the Agency Infrastructure Manager. An additional seven staff with current Domain Administrator privileges will have further access restrictions enacted. These restrictions should be in place by December 2011. To further mitigate risk, all IT staff has undergone Level II background screenings.

On October 20, 2011, the Internal Security Unit (ISU) confirmed the five UC benefits employees with access to the debit card interface required the access for the performance of their duties. A draft document to formally establish the UC Program's procedure has been developed and should be approved and implemented prior to the end of November 2011. When implemented, an internal review/audit process to monitor compliance will be initiated.

Finding No. 2: Periodic Review of Access

The Agency's review of UC System and related IT resource access privileges needed improvement. In addition, Agency procedures for the periodic review of access privileges for the UC System and related IT resources existed only in draft form. A similar finding was noted in our report No. 2011-021.

Auditor Recommendation: Management should approve and follow written procedures that describe management's expectations for the periodic review of access privileges for the UC System and related IT resources.

DEO Response: The Internal Security Unit (ISU), in coordination with security officers, conducts semi-annual, documented reviews of access privileges and will include non-mainframe applications and associated databases in future reviews. The ISU will work

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Economic Opportunity (DEO)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2010 through June 30, 2011
Response to Preliminary and Tentative Findings

with Appeals, Benefit Payment Control, and the Special Payments Unit (for the debit cards) to assist in establishing written procedures for requesting and managing access to their respective subsystems. The ISU will then establish written monitoring procedures to ensure compliance. In addition, the ISU will review all applications to ensure the business owners have established written procedures to control access privileges and establish monitoring procedures to support compliance by December 31, 2011.

Network access is currently being monitored as part of daily operations. Periodic reviews of network access will formally be conducted twice a year, in January and July. IT Operations will conduct the first formal review in January 2012.

Finding No. 3: Security Controls

Certain Agency security controls were deficient in the area of telecommuting and needing improvement in the area of user authentication. Similar findings were noted in prior audits of the Agency, most recently our report No. 2011-021. Details of this finding are confidential in nature and are not disclosed in the audit report.

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

DEO Response: AWI/DEO management has implemented appropriate security controls in the areas of telecommuting and will implement additional user authentication to ensure the continued confidentiality, integrity, and availability of Department data and IT resources as recommended by the OAG.

Finding No. 4: UC Operational Security Plan

The Agency'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 Agency management. A similar finding was noted in our report No. 2011-021.

Auditor Recommendation: Management 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

DEO Response: In 2010, a UC Supplemental Budget Request was approved by the United States Department of Labor (USDOL) to obtain the vendor services necessary to update the UC Operational Security Plan. Direct Order (DO) A4B203, Contract C0556 was issued September 16, 2011 to Integrated Computer Solutions to assist UC with this

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Economic Opportunity (DEO)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2010 through June 30, 2011
Response to Preliminary and Tentative Findings

project. Due to the extensive amount of work required and the timeframe allowed by USDOL to use these funds, the revised plan and other requirements included in the contract are scheduled to be completed September 30, 2012.

Finding No. 5: Programmed Edits

As similarly noted in prior audits of the Agency, most recently our report No. 2011-021, 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.

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

DEO Response: Although no errors were noted in the audit findings, UC will implement, where practicable, additional edits and system calculations to prevent the entry of invalid data. Changes that can be identified will be implemented in the new UC system, *Connect*, which is scheduled for implementation in December 2012.