REPORT NO. 2011-021
OCTOBER 2010

AGENCY FOR WORKFORCE INNOVATION
SOUTHWOOD SHARED RESOURCE CENTER

UNEMPLOYMENT INSURANCE PROGRAM

Information Technology Operational Audit

For the Period
July 1, 2009, Through June 30, 2010

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 audit period.

EXECUTIVE DIRECTOR OF THE SOUTHWOOD SHARED RESOURCE CENTER

Pursuant to Section 282.205, Florida Statutes, the Southwood Shared Resource Center (SSRC) is established within DMS and is a separate budget entity not subject to control, supervision, or direction by DMS in any manner. SSRC is headed by a board of trustees, the members of which are appointed, pursuant to Section 282.203(2)(a), Florida Statutes, by the agency head or chief executive officer of the representative customer entities of SSRC. Pursuant to Section 282.203(3)(a), Florida Statutes, the board of trustees is responsible for employing the Executive Director of SSRC. John Wade served as Executive Director during the audit period.

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, 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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

AGENCY FOR WORKFORCE INNOVATION
SOUTHWOOD SHARED RESOURCE CENTER

Unemployment Insurance Program

SUMMARY

The Agency for Workforce Innovation (Agency) is responsible for administering the State's Unemployment Insurance (UI) Program. The Unemployment Compensation (UC) System is the system used by the Agency to determine eligibility and calculate benefit amounts for individuals seeking unemployment compensation. The Southwood Shared Resource Center (SSRC) provides support services for the Agency's computer operations and mainframe applications, including the UC System.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to the UC System during the period July 1, 2009, through June 30, 2010. We also determined the status of corrective actions regarding prior audit findings disclosed in audit report No. 2010-011, relating to Agency and SSRC IT controls over the UC System.

The results of our audit are summarized below:

Security Controls

Finding No. 1: **Various access controls relating to the UC System needed improvement. Similar issues were noted in our report No. 2010-011.**

Finding No. 2: **The Agency had not developed written procedures for disabling the access of former employees for non-mainframe UC subsystems, the network, or the database. A similar issue was noted in our report No. 2010-011. Additionally, the Agency did not timely disable the UC System access privileges of certain former employees.**

Finding No. 3: **The Agency did not have written procedures for periodic reviews of non-mainframe UC subsystem, network, or database access privileges.**

Finding No. 4: **The Agency had not timely performed background checks and fingerprinting of some contractors having sensitive IT responsibilities and elevated IT access privileges. A similar issue was noted in our report No. 2010-011.**

Finding No. 5: **Certain Agency security controls were deficient in the areas of telecommuting and protecting confidential and sensitive information. Additionally, certain Agency and SSRC security controls relating to user authentication needed improvement. These issues were also noted in our report No. 2010-011.**

Finding No. 6: **The Agency's Operational Security Plan for the Florida Unemployment Compensation Program 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.**

Other General Controls

Finding No. 7: **The Agency did not log or review program changes to the UC System production environment.**

Application Controls

Finding No. 8: **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.**

Additional Matter

Finding No. 9: The Agency had not executed a current service-level agreement with SSRC for support services provided for the UC 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 processes new claims by determining monetary eligibility for benefit payments. It also determines employers' chargeability for benefits and facilitates the payment of claimant benefits.

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.

Section 443.1317(1)(a), Florida Statutes, provides that the Agency has ultimate authority over the administration of the UI Program. The Agency contracted with ISOCORP to provide application development and support for the UC System. SSRC is responsible for supporting the UC System's data center operations.

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, 2010, 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. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Our audit disclosed instances where access privileges were granted in excess of what was necessary for the performance of job duties and were inconsistent with an appropriate separation of incompatible duties. Specifically:

- One access profile (SUPER) within Appeals allowed users update capability after a case is closed. Three users had been assigned the SUPER profile. However, one of the users did not need the access that this profile provided to perform his job duties, as also noted in our report No. 2010-011. The access privileges were unnecessary for the performance of the user's assigned job responsibilities and increased the risk of unauthorized disclosure, modification, or destruction of UC data. In response to audit inquiry, Agency staff indicated that they have deactivated the user's access.
- Twenty-two IT operations staff had been granted domain administrator privileges that allowed elevated access capabilities over numerous servers within the domain, including servers that contained UC data and programs. The domain administrator privileges provided the IT operations staff the capability to modify or delete IT resources residing on servers within the domain, including UC IT resources. A similar issue was also noted in our report No. 2010-011. In response to audit inquiry, Agency management indicated that, until more resources become available, the Agency will continue to monitor domain administrator access privileges

as part of its annual user access review and that the latest review was conducted in May 2010. However, as discussed further in Finding No. 3, the May 2010 review was not documented. Agency management also stated that additional compensating controls had been implemented, including background screening for IT staff. Management further stated that they were in the process of developing an IT Operations Manual that, when completed, would address domain administrator access privileges. Nevertheless, the critical nature of the UC System and the presence of confidential information within UC System data files indicated a need for the Agency to restrict domain administrator privileges within the Agency domain. Absent further restrictions of domain administrator privileges, the risk of unauthorized disclosure, modification, or destruction of UC System data and IT resources was increased.

- Twenty-nine network system analysts had been granted access to PC-Duo, as also noted in our report No. 2010-011. PC-Duo is a remote control software product for networked and remote users that enables network analysts to provide user support. PC-Duo had been implemented without the option that requires the user to grant permission for the network analyst to assume control of the user's computer. In response to audit inquiry, Agency management indicated that they were evaluating other software products to address remote user support and that they would continue to evaluate and manage the risk associated with the use of remote control software to determine appropriate control settings. Agency management also stated that additional compensating controls had been implemented to reduce the security-related risk, including background screening for IT staff, and that they were in the process of developing an IT Operations Manual that, when completed, would address remote access of workstations and servers and policy enforcement of acceptable use of IT resources. Nevertheless, under these conditions, the risk was increased that unauthorized activities could be performed using a local computer without the authorized user's knowledge.

- As also noted in our prior reports on the UI Program, most recently our report No. 2010-011, some programmers and a systems staff member, including contractors, had UC Claims and Benefits access privileges that were not required to perform their job duties. Specifically, 10 of 24 individuals previously noted in our prior reports, who had been granted access privileges to UC Claims and Benefits production data files, continued to have inappropriate application level access to the production UC System. The 10 individuals included Agency employees and contractors as follows: 9 programmers and 1 systems staff member (a production support analyst). Monitoring or reviewing of the access privileges for the above-mentioned individuals had not been performed by the Agency or SSRC. Under these conditions, the risk was increased that UC Claims and Benefits programs and data could be compromised without detection. In response to audit inquiry, SSRC staff indicated that the inappropriate access has now been removed.

- Of a sample of 21 UC System end users, 1 Agency employee had access privileges that were not needed to perform her job duties, increasing the risk that the access privileges could be misused. In response to audit inquiry, Agency staff removed the inappropriate access.

Our audit also disclosed that the Agency lacked an access exception form for one UC System end user to document management justification of a sensitive combination of UC System access privileges. The UC Security Manual provides that access exception forms are to be completed by UC managers providing sufficient justification for granting user access to a combination of transactions or transaction groups that results in the ability to bypass access controls intended to promote a proper separation of duties. These forms were to be maintained by the Agency's Internal Security Unit (ISU). Of the 21 UC System end users included in our sample described above, 11 had been granted a combination of access privileges that required the Agency to complete an access exception form to document justification for their level of access. However, an access exception form was not available for 1 of the 11 users. Without appropriate documentation of approved user access privileges, management's ability to monitor the appropriateness of access privileges may be limited. In response to audit inquiry, an access exception form for the user was completed by the appropriate UC manager.

As also noted in our prior reports on the UI Program, most recently our report No. 2010-011, access violation reports for the Agency's Highway Safety and Motor Vehicle (HSMV) cross-match application were not produced; therefore, the Agency did not monitor for unauthorized attempts to access the application. The HSMV cross-match application

was implemented in an effort to eliminate improper benefit payments to claimants whose identities were in question. Repeated unsuccessful access attempts could be an indicator of someone trying to compromise the security of the system and its data. Without a periodic review of access violations, such attempts to compromise the security of cross-match data may not be timely detected or appropriately acted upon by management.

Recommendation: The Agency and SSRC should strengthen system access privileges to ensure that an appropriate separation of duties is enforced. The Agency should also ensure that the security structure does not inappropriately give access privileges to users who do not require access to accomplish their job responsibilities. Additionally, the Agency should periodically review UC Claims and Benefits user access privileges and ensure that the appropriate documentation is maintained for users with sensitive combinations of access privileges. Furthermore, the Agency should periodically review HSMV cross-match application access violations.

Finding No. 2: Timely Disabling of Access Privileges

Effective access controls include provisions for the timely disabling of former employee access privileges to ensure that the access privileges are not misused by the former employee or others. The Agency had not developed written procedures for disabling the access of former employees for non-mainframe UC subsystems, the network, or the database. A similar issue was noted in our report No. 2010-011. In response to audit inquiry, Agency management stated that they were in the process of developing procedures to address this issue. Without written procedures for disabling access privileges, there was an increased risk that access privileges may not be timely disabled in a consistent manner pursuant to management's expectations.

We compared the mainframe UC access privileges of active users as of March 31, 2010, to a list of 249 employee terminations that occurred during the period July 1, 2009, through March 31, 2010, to determine whether the accounts of former employees had been timely disabled. Our test disclosed that the access privileges of 4 of the 249 former employees included in our test remained active from 4 to 74 days after termination. In response to audit inquiry, Agency management provided evidence that the access privileges had not been used to access the UC System after termination. Nevertheless, these conditions increased the risk that the access privileges could be misused by the former employees or others.

Recommendation: The Agency should develop and follow written procedures for timely disabling the access privileges of former employees for all levels of access to UC data and IT resources.

Finding No. 3: 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. However, no written Agency procedures existed that required the UC security officers to perform periodic reviews of non-mainframe UC subsystem, network, or database access privileges or described management's expectations for how the reviews were to be performed, including how often they were to be performed, and what actions UC security officers should take when discrepancies in access privileges are found.

Furthermore, the Agency had not formally reviewed UC application level (other than mainframe applications), network, or database access privileges on a periodic basis. In response to audit inquiry, Agency staff indicated that the last review of UC user access privileges was performed in May 2010 at the direction of the Agency's Information Security Manager, but no documentation of the review was maintained by the Agency.

As demonstrated by the inappropriate access privileges disclosed in Finding Nos. 1 and 2, the lack of periodic reviews of access privileges increased the risk that inappropriate access privileges will not be timely detected or disabled that could result in unauthorized disclosure, modification, or destruction of UC data and IT resources.

Recommendation: The Agency should develop and implement written procedures describing management's expectations for periodic reviews of all UC System access privileges.

Finding No. 4: Positions of Special Trust

Section 110.1127(1), Florida Statutes, states that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations as a condition of employment and continued employment. The security background investigations are to include, but not be limited to, fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation.

DMS Rule 60DD-2.001(2)(a)75., Florida Administrative Code, defines sensitive locations as physical locations such as a data center, financial institution, network operations center, or any location where critical, confidential, or exempt information resources can be accessed, processed, stored, managed, and maintained. DMS Rule 60DD-2.001(2)(a)80., Florida Administrative Code, defines special trust or position of trust as a position in which an individual can view or alter confidential information or is depended upon for continuity of information resource imperative to the operations of the agency and its mission.

Background checks included in the recruitment process are an integral component of managing IT resources. Our audit disclosed that background checks (including fingerprinting) were not performed for some UC contractors in a timely manner. In response to audit inquiry, Agency management indicated that they had improved their practices for background screening for contractors in January 2010. However, background checks for 8 of 14 contractors who began work after the new practices were implemented were performed between 1 and 99 days after the contractor began work at the Agency. Without timely background checks, including fingerprinting, the risk was increased that a person with an inappropriate background could be contracted for one of these positions. A similar issue regarding positions of special trust was noted in our report No. 2010-011.

Recommendation: The Agency should conduct timely background checks for its contractors who work in positions of special trust.

Finding No. 5: 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 areas of telecommuting and protecting

confidential and sensitive information. Our audit further disclosed certain Agency and SSRC security controls relating to user authentication that needed improvement. 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 and SSRC management of the specific issues. These issues were also noted in connection with our report No. 2010-011. Without adequate security controls in the areas of telecommuting, protecting confidential and sensitive information, 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: The Agency and SSRC should implement appropriate security controls in the areas of telecommuting, protecting confidential and sensitive information, and user authentication to ensure the continued confidentiality, integrity, and availability of Agency 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 they are kept up to date.

The Operational Security Plan for the Florida Unemployment Compensation Program was updated 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 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 existed. 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. 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 Agency should update the Operational Security Plan for the Florida Unemployment Compensation Program to reflect the current system environment and periodically review the Plan to ensure its ongoing effectiveness.

Other General Controls

Finding No. 7: Program Change Controls

Effective program change controls are intended to ensure that all program changes are properly authorized, tested, and approved for implementation. Our audit disclosed that changes to the UC System production environment (i.e., production programs) were not logged or reviewed to ensure that unauthorized changes had not been made. Under these conditions, the risk was increased that unauthorized or erroneous programs could be moved into the production environment without timely detection, jeopardizing the ongoing integrity of the UC System.

Recommendation: To ensure that changes to the UC System are made in a consistent manner pursuant to management's expectations, the Agency should log and review all changes to the production environment to detect the movement of any unauthorized or erroneous programs, should it occur.

Application Controls

Finding No. 8: Programmed Edits

Application controls include programmed edits that evaluate the accuracy, completeness, and validity of input data. As also noted in our report No. 2010-011, 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, jeopardizing the integrity and reliability of the data. In response to audit inquiry, Agency staff indicated that they were in the process of addressing these issues.

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

Additional Matter

Finding No. 9: Service-Level Agreement

A service-level agreement is a negotiated agreement between two parties where one is the customer and the other is the service provider. Service-level agreements are necessary to define IT services provided by service providers to State agencies and other governmental entities and to ensure that services provided by the service providers support the business objectives of the customer entities. Service-level agreements define the roles and responsibilities of each party, including security management practices, service renewal provisions, and termination requirements. Service-level agreements also set forth the billing methodology and the costs of the services to be paid by the customer entities.

Section 282.203(1)(g), Florida Statutes, provides that each primary data center shall enter into a service-level agreement with each customer entity to provide services as defined and approved by the data center Board of

Trustees in compliance with rules of the Agency for Enterprise Information Technology. Section 282.203(1)(g)3., Florida Statutes, states that the failure to execute a service-level agreement within 60 days after service commencement shall, in the case of an existing customer entity, result in a continuation of the terms of the service-level agreement from the prior fiscal year, including any amendments that were formally proposed to the customer entity by the primary data center within the three months before service commencement, and a revised cost-of-service estimate. If a new customer entity fails to execute an agreement within 60 days after service commencement, the data center may cease services. Proviso language to Specific Appropriation Item 2206 of Chapter 2010-152, Laws of Florida, provides that by September 1, 2010, the Agency shall execute a service level agreement, pursuant to Section 282.203(1)(g), Florida Statutes, to specify the services and levels of services it is to receive from SSRC.

SSRC provides support services for the Agency's computer operations and mainframe applications, including the UC System. Although the Agency executed a service-level agreement with the Department of Management Services (DMS) on May 5, 2010, for mainframe-managed services, the Agency had not executed a service-level agreement with SSRC for many of its other services and was relying on a prior service-level agreement between the Agency and DMS to detail the related responsibilities.[1] The absence of a current signed agreement with SSRC increased the risk that Agency service requirements, including the security and the availability of the equipment and the data residing therein, will not be sufficiently met.

Recommendation: The Agency should execute a current service-level agreement with SSRC that defines the specific requirements related to the support services for the Agency's computer operations and mainframe applications.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Agency had taken corrective actions for findings included in our report No. 2010-011.

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 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

[1] Effective July 1, 2008, SSRC assumed the responsibility for providing support services for the Agency's computer operations and mainframe applications, including the UC System. These services were formerly the responsibility of DMS.

was in the process of correcting, deficiencies disclosed in our report No. 2010-011 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 during the period July 1, 2009, through June 30, 2010.

In conducting our audit, we:

- Interviewed Agency personnel.
- Obtained an understanding of the UC System, including the purpose and goals of the System, and the basic data and business processing flows through the System.
- Obtained an understanding of UC System application controls, including input, processing, output, and user controls.
- Obtained an understanding of general IT controls related to the UC System.
- Observed, tested, and evaluated key processes and procedures related to the appropriateness of selected application controls, including separation of duties, application edits, and transaction logging within the system.
- Observed, tested, and evaluated key processes and procedures related to the appropriateness of UC System user account administration procedures.
- Observed and evaluated key processes and procedures related to the Agency security plan and program, including risk assessments, security policies and procedures, and security awareness training.
- Observed, tested, and evaluated key processes and procedures related to logical access controls over UC System IT resources, including adequacy of review and removal of access privileges, adequacy of review of access to UC System computer resources, and the adequacy of password controls related to the UC System.
- Observed, tested, and evaluated key processes and procedures related to the Agency systems modification controls related to the UC System.
- Determined whether the Agency and SSRC had executed a service-level agreement.

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

MANAGEMENTS' RESPONSES

In letters dated October 15, 2010, the Director of the Agency for Workforce Innovation and the Executive Director of the Southwood Shared Resource Center, respectively, provided responses to our preliminary and tentative findings. These letters are included at the end of this report as EXHIBIT A

THIS PAGE INTENTIONALLY LEFT BLANK.

EXHIBIT A
MANAGEMENTS' RESPONSES

Charlie Crist
Governor
Cynthia R. Lorenzo
Director

October 15, 2010

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, 2009 through June 30, 2010.

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,

Cynthia R. Lorenzo
Director

CRL/js

Enclosure

Agency for Workforce Innovation
The Caldwell Building, Suite 100•107 East Madison Street•Tallahassee, Florida•32399-4120
Telephone (850) 245-7105•Fax (850) 921-3223•TTY/TDD 1-800-955-8771-Voice1-800-955-8770
www.floridajobs.org

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

Finding No. 1: Appropriateness of Access Privileges

Various access controls relating to the UC System needed improvement. Similar issues were noted in Auditor General Report No. 2010-011.

Auditor Recommendation: The Agency and Southwood Shared Resource Center (SSRC) should strengthen system access privileges to ensure that an appropriate separation of duties is enforced. The Agency should also ensure that the security structure does not inappropriately give access privileges to users who do not require access to accomplish their job responsibilities. Additionally, the Agency should periodically review UC Claims and Benefits user access privileges and ensure that the appropriate documentation is maintained for users with sensitive combinations of access privileges. Furthermore, the Agency should periodically review Highway Safety and Motor Vehicle (HSMV) cross-match application access violations.

The audit findings specifically stated:

Bullet #1 - One access profile (SUPER) within Appeals allowed users update capability after a case is closed. Three users had been assigned the SUPER profile. However, one of the users did not need the access that this profile provided to perform his job duties, as also noted in Report No. 2010-011. The access privileges were unnecessary for the performance of the user's assigned job responsibilities and increased the risk of unauthorized disclosure, modification, or destruction of UC data. In response to audit inquiry, Agency staff indicated that they have deactivated the user's access.

AWI Response: The Agency will continue to remind managers and reinforce written procedures and practices for security officers to ensure data access privileges are periodically reviewed and that authorized individuals are provided access to only the UC data that is necessary in the performance of assigned job duties and responsibilities.

Bullet #2 - Twenty-two IT operations staff had been granted domain administrator privileges that allowed elevated access capabilities over numerous servers within the domain, including servers that contained UC data and programs. The domain administrator privileges provided the IT operations staff the capability to modify or delete IT resources residing on servers within the domain, including UC IT resources. A similar issue was also noted in Report No. 2010-011. In response to audit inquiry, Agency management indicated that, until more resources become available, the Agency will continue to monitor domain administrator access privileges as part of its annual user access review and that the latest review was conducted in May 2010. However, as discussed further in Finding No. 3, the May 2010 review was not documented. Agency management

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

also stated that additional compensating controls had been implemented, including background screening for IT staff. Management further stated that they were in the process of developing an IT Operations Manual that, when completed, would address domain administrator access privileges. Nevertheless, the critical nature of the UC System and the presence of confidential information within UC System data files indicated a need for the Agency to restrict domain administrator privileges within the Agency domain. Absent further restrictions of domain administrator privileges, the risk of unauthorized disclosure, modification, or destruction of UC System data and IT resources was increased.

> **AWI Response:** AWI has determined that domain administrator privileges were appropriately granted. Nevertheless, in July 2010, AWI sought and was awarded a United States Department of Labor grant to address this audit finding. AWI intends to evaluate mitigation strategies and implement a software-based solution by April 2011.

Bullet #3 - Twenty-nine network system analysts had been granted access to PC-Duo, as also noted in Report No. 2010-011. PC-Duo is a remote control software product for networked and remote users that enables network analysts to provide user support. PC-Duo had been implemented without the option that requires the user to grant permission for the network analyst to assume control of the user's computer. In response to audit inquiry, Agency management indicated that they were evaluating other software products to address remote user support and that they would continue to evaluate and manage the risk associated with the use of remote control software to determine appropriate control settings. Agency management also stated that additional compensating controls had been implemented to reduce the security-related risk, including background screening for IT staff, and that they were in the process of developing an IT Operations Manual that, when completed, would address remote access of workstations and servers and policy enforcement of acceptable use of IT resources. Nevertheless, under these conditions, the risk was increased that unauthorized activities could be performed using a local computer without the authorized user's knowledge.

> **AWI Response:** AWI will utilize the PC-Duo option that requires the user to grant permission for the network analyst to assume control of the user's computer. The Agency intends to implement this option by January 2011.

Bullet #4 - As also noted in prior reports on the UI Program, most recently Report No. 2010-011, some programmers and a systems staff member, including contractors, had UC Claims and Benefits access privileges that were not required to perform their job duties. Specifically, 10 of 24 individuals previously noted in our prior reports, who had been granted access privileges to UC Claims and

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

Benefits production data files, continued to have inappropriate application level access to the production UC System. The 10 individuals included Agency employees and contractors as follows: 9 programmers and 1 systems staff member (a production support analyst). Monitoring or reviewing of the access privileges for the above-mentioned individuals had not been performed by the Agency or SSRC. Under these conditions, the risk was increased that UC Claims and Benefits programs and data could be compromised without detection. In response to audit inquiry, SSRC staff indicated that the inappropriate access has now been removed.

> **AWI Response:** The SSRC staff has reported that the access for the referenced individuals has now been removed. AWI considers this finding closed.

Bullet #5 – Of a sample of 21 UC System end users, 1 Agency employee had access privileges that were not needed to perform her job duties, increasing the risk that the access privileges could be misused. In response to audit inquiry, Agency staff removed the inappropriate access.

The audit also disclosed that the Agency lacked an access exception form for one UC System end user to document management justification of a sensitive combination of UC System access privileges. The UC Security Manual provides that access exception forms are to be completed by UC managers providing sufficient justification for granting user access to a combination of transactions or transaction groups that result in the ability to bypass access controls intended to promote a proper separation of duties. These forms were to be maintained by the Agency's Internal Security Unit (ISU). Of the 21 UC System end users included in our sample described above, 11 had been granted a combination of access privileges that required the Agency to complete an access exception form to document justification for their level of access. However, an access exception form was not available for 1 of the 11 users. Without appropriate documentation of approved user access privileges, management's ability to monitor the appropriateness of access privileges may be limited. In response to audit inquiry, an access exception form for the user was completed by the appropriate UC manager.

> **AWI Response:** The Agency will continue to remind managers and reinforce written procedures and practices for security officers to ensure data access privileges are periodically reviewed and that authorized individuals are provided access to only the UC data that is necessary in the performance of assigned job duties and responsibilities.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

As also noted in prior reports on the Unemployment Insurance Program, most recently Report No. 2010-011, access violation reports for the Agency's HSMV (Highway Safety and Motor Vehicles) cross-match application were not produced; therefore, the Agency did not monitor for unauthorized attempts to access the application. The HSMV cross-match application was implemented in an effort to eliminate improper benefit payments to claimants whose identities were in question. Repeated unsuccessful access attempts could be an indicator of someone trying to compromise the security of the system and its data. Without a periodic review of access violations, such attempts to compromise the security of cross-match data may not be timely detected or appropriately acted upon by management.

AWI Response: While the Agency has not experienced any known security breaches related to the HSMV cross-match application, a work request has been submitted to Agency IT staff to develop a report documenting unauthorized attempts to access the data supplied to the Agency by the Department of Highway Safety and Motor Vehicles. This report should be available by July 2011.

Finding No. 2: Timely Disabling of Access Privileges

The Agency had not developed written procedures for disabling the access of former employees for non-mainframe UC subsystems, the network, or the database. A similar issue was noted in Report No. 2010-011. Additionally, the Agency did not timely disable the UC System access privileges of certain former employees.

Auditor Recommendation: The Agency should develop and follow written procedures for timely disabling the access privileges of former employees for all levels of access to UC data and IT resources.

AWI Response: AWI is continuing to improve upon and develop the necessary written procedures for termination of access for non-mainframe UC systems. The Agency is currently developing an automated process which will include an annual compliance and audit calendar -- that will include periodic reviews of access for all information systems. AWI intends to complete this project and implement the compliance process by April 2011.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

Finding No. 3: Periodic Review of Access

The Agency did not have written procedures for periodic reviews of non-mainframe UC subsystem, network, or database access privileges.

Auditor Recommendation: The Agency should develop and implement written procedures describing management's expectations for periodic reviews of all UC System access privileges.

AWI Response: AWI is continuing to improve upon and to develop the necessary written procedures for conducting periodic review of all information systems. The Agency is currently developing an automated process which will include an annual compliance and audit calendar that will include periodic reviews of access for all information systems. AWI intends to complete this project and implement the compliance process by April 2011.

Finding No. 4: Positions of Special Trust

The Agency had not timely performed background checks and fingerprinting of some contractors having sensitive IT responsibilities and elevated IT access privileges. A similar issue was noted in Report No. 2010-011.

Auditor Recommendation: The Agency should conduct timely background checks for its contractors who work in positions of special trust.

AWI Response: All background checks have been completed for the contractors mentioned in the audit finding. AWI will continue to monitor and manage the background screening process in order to identify areas for improvement, as recommended by the Auditor General.

Finding No. 5: Security Controls

Certain Agency security controls were deficient in the areas of telecommuting and protecting confidential and sensitive information. Additionally, certain Agency and SSRC (Southwood Shared Resource Center) security controls relating to user authentication needed improvement. These issues were also noted in Report No. 2010-011. Details of this finding are confidential in nature and are not disclosed in the audit report.

Auditor Recommendation: The Agency and SSRC should implement appropriate security controls in the areas of telecommuting, protecting confidential and sensitive

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

information, and user authentication to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

AWI Response: The Agency has taken steps to implement the appropriate security controls as recommended by the Auditor General to protect the confidentiality, integrity, and availability of Agency data and IT resources. All necessary steps to correct the deficiencies noted should be complete by June 2011.

Finding No. 6: UC Operational Security Plan

The Agency's Operational Security Plan for the Florida Unemployment Compensation Program 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.

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

AWI Response: The Agency will review the Operational Security Plan for Florida Unemployment Compensation Program to reflect the current system environment and develop an on-going plan for ensuring its effectiveness through periodic reviews. The Agency has received a Supplemental Budget Request (SBR) from the United States Department of Labor (USDOL) to hire a vendor to assist in performing a review of the Operational Security Plan. It is anticipated that the review and update will be completed by December 2011.

Finding No. 7: Program Change Controls

The Agency did not log or review program changes to the UC System production environment.

Auditor Recommendation: To ensure that changes to the UC System are made in a consistent manner pursuant to management's expectations, the Agency should log and review all changes to the production environment to detect the movement of any unauthorized or erroneous programs, should it occur.

AWI Response: AWI intends to improve on its change control process by developing a logging and review process of production changes to the mainframe. The process will include A) a weekly system generated log of production changes, B) a review of those changes compared against approved changes of the UC-IT Change Advisory Board

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

(CAB), C) recognition of the review through inclusion in the weekly CAB meeting's agenda, and D) recording of the review and its discussion in the CAB's meeting minutes. AWI has identified an appropriate logging report and intends to integrate the report(s) with a monitoring process by April 2011.

Finding No. 8: Programmed Edits

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

AWI Response: In connection with the issue relating to the programmed edits involving the Appeals data, a work request has been submitted to address the program edits. This request is scheduled for completion in June 2011.

In connection with the Wage Determination Component of the UC Claims and Benefits Subsystem, combined wage claims involve the transfer of wages earned in one state for use in another state to establish benefit eligibility under the state law of the paying state. The Federal government developed model programming for all states to use within their automated systems for electronic submission of data. Wage data and billing information is transferred among states over the Interstate Connection (ICON) system as prescribed by the United States Department of Labor. The ICON system does not have edits to determine if the state is correctly entering amounts as each state has different weekly benefit amounts and maximum available credits. Any edits added to the ICON system must be approved by the USDOL vendor that maintains the system. This issue will be examined in connection with the development of the new UC Claims and Benefits Information System.

Finding No. 9: Service-Level Agreement

The Agency had not executed a current service-level agreement with SSRC for support services provided for the UC System.

Auditor Recommendation: The Agency should execute a current service-level agreement with SSRC that defines the specific requirements related to the support services for the Agency's computer operations and mainframe applications.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit
July 1, 2009 through June 30, 2010
Response to Preliminary and Tentative Findings

AWI Response: AWI entered into four Service Level Agreements (SLAs) with the SSRC (Southwood Shared Resource Center) for utilized services on September 7, 2010. Those SLAs were 1) Co-Location Services, 2) Managed Disk; 3) Mainframe Services, and 4) Open Systems. AWI intends to finish the SLA signatory process by completing the final SLA (Shared Transitional Services) in December 2010.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

State of Florida
Southwood Shared Resource Center
2585 Shumard Oak Boulevard
Tallahassee, Florida 32399-0950
Phone: 850.413.9300
Fax: 850.921.8343
http://ssrc.myflorida.com

Governor
Charlie Crist

Executive Director
John Wade

October 15, 2010

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

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report, *Agency for Workforce Innovation and the Southwood Shared Resource Center - Unemployment Insurance Program.* Our response corresponds with the order of your preliminary and tentative findings and recommendations.

Finding No. 1 – Appropriateness of Access Privileges

Certain Agency and SSRC security controls relating to user authentication needed improvement.

Recommendation

The Agency and SSRC should strengthen system access privileges to ensure that an appropriate separation of duties is enforced.

Response

The SSRC will create a process to review all system access privileges with the Agency on a quarterly basis. The process will be created and implemented by 4/1/2011.

Finding No. 5 – Security Controls

Certain Agency security controls were deficient in the areas of telecommuting and protecting confidential and sensitive information. Additionally, certain Agency and SSRC security controls relating to user authentication needed improvement. These issues were also noted in our report No. 2010-011.

Recommendation

The Agency and SSRC should implement appropriate security controls in the areas of telecommuting, protecting confidential and sensitive information, and user authentication to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

A Certified Tier III Facility

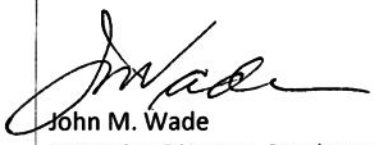
EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Response

The SSRC will work with AWI to develop and implement a solution to correct the identified security issues by 4/1/2011.

If further information is needed concerning our response, please contact Cathy Kreiensieck, Chief of Enterprise Planning & Management, Southwood Shared Resource Center at 413-9309.

Sincerely,



John M. Wade
Executive Director, Southwood Shared Resource Center

CC: David Faulkenberry, Chairman of the SSRC Board
John Davis, Audit Director, DMS