

Rick Scott
Governor
Cynthia R. Lorenzo
Director
James F. Mathews
Inspector General

April 20, 2011

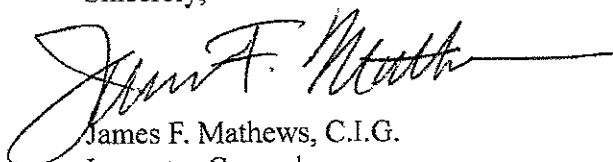
Ms. Cynthia Lorenzo, Director
Agency for Workforce Innovation
Suite 212, Caldwell Building
107 East Madison Street
Tallahassee, Florida 32399-4120

Dear Director Lorenzo:

As required by Section 20.055(5)(h), Florida Statutes, we have prepared the attached status of corrective actions, as of April 20, 2011, taken by the Agency for Workforce Innovation for findings and recommendations contained in Auditor General Audit Report No. 2011-021, *Agency for Workforce Innovation, Southwood Shared Resource Center, Unemployment Insurance Program, Information Technology Operational Audit*, issued on October 20, 2010. This audit focused on evaluating the effectiveness of selected information technology controls applicable to the UC System during the period July 1, 2009, through June 30, 2010.

In accordance with Section 20.055(5)(h), Florida Statutes, I am also copying the Joint Legislative Auditing Committee. If you have any questions, please call me at (850) 245-7141.

Sincerely,


James F. Mathews, C.I.G.
Inspector General

JFM/js

cc: Joint Legislative Auditing Committee
Tom Clendenning

RECEIVED
APR 20 2011

Office of Inspector General

MSC #130, Caldwell Building • 107 East Madison Street • Tallahassee • Florida 32399-4126
Phone 850-245-7135 • Fax 850-245-7144 • TTY/TDD 1-800-955-8771-Voice 1-800-955-8770

www.floridajobs.org

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

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit 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.

6-Month Status: The Agency continues 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

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

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 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: In July 2010, AWI 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.

6-Month Status: AWI has made significant progress towards addressing this audit finding and a fully enacted solution will be completed this month (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,

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

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 setting by January 2011.

6-Month Status: As noted above, 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. AWI has made significant progress towards addressing this audit finding and a fully enacted solution will be completed this month (April 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 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: SSRC staff indicated that the inappropriate access has now been removed. AWI considers this finding closed.

6-Month Status: As noted, the inappropriate access has now been removed and 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.

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

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.

6-Month Status: As noted, 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.

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 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.

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.

6-Month Status: As noted, 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.

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit 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 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: 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.

6-Month Status: The Agency has created and implemented a violation attempts SAR (Sysout Archival and Retrieval) report that documents unauthorized attempts to access the data supplied to the Agency by the Department of Highway Safety and Motor Vehicles.

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. This process should be complete by the end of April 2011.

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

6-Month Status: AWI is currently promulgating procedures as part of the Agency's IT Operations Manual that will require periodic review and the timely disabling of access privileges. AWI intends to complete this process by June 2011.

Finding No. 3: Periodic Review of Access

The Agency did not have written procedures for periodic reviews of non-mainframe UC subsystems, 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. AWI 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.

6-Month Status: AWI is currently promulgating procedures as part of the Agency's IT Operations Manual that will require periodic review and the timely disabling of access privileges. AWI intends to complete this process by June 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: AWI will continue to monitor and manage the background screening process in order to identify areas for improvement, as recommended by the OAG.

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

6-Month Status: 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 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 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.

6-Month Status: As noted above, 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.

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

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

environment and develop an on-going plan for ensuring its effectiveness through periodic reviews.

6-Month Status: 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 and subsequent update of the Operational Security Plan. This process is scheduled for completion 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 (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.

6-Month Status: As noted above, AWI has identified an appropriate logging report and has successfully integrated it into the UC-IT Change Advisory Board's procedures related to logging and reviewing of changes each week to help in detecting the movement of any unauthorized or erroneous programs.

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.

Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings

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: Where practicable the Agency will implement additional edits with respect to claims filed under the Interstate Arrangement for Combining Employment and Wages. 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) 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. Since all states use the same transaction via the ICON system, it may not be possible to create edits to the degree to which the auditor recommends.

6-Month Status: As noted above, since all states use the same transaction via the ICON system, it may not be possible to create edits to the degree to which the auditor recommends; however, this issue is being examined in connection with the development of the new UC Claims and Benefits Information System. The development of the new system is under contract and is scheduled for completion by December 2012. The contractor has been notified that these edits should be included as part of the new 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.

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

**Agency for Workforce Innovation (AWI)
Auditor General Audit -
Unemployment Compensation (UC) Information Technology (IT)
Audit No. 2011-021, dated October 20, 2010
July 1, 2009 through June 30, 2010
6-Month Status of Audit Findings**

SLA signatory process by completing the final SLA (Shared Transitional Services) in December 2010.

6-Month Status: AWI finished the SLA signatory process by completing the final SLA (Shared Transitional Services) in October 2010.