Charlie Crist
Governor
Cynthia R. Lorenzo
Director
James F. Mathews
Inspector General

March 8, 2010

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)(g), Florida Statutes, we have prepared the attached status of corrective actions, as of March 8, 2010, taken by the Agency for Workforce Innovation for findings and recommendations relating to the Agency contained in Auditor General Audit Report No. 2010-011, *Agency for Workforce Innovation, Southwood Shared Resource Center, Unemployment Insurance Program, Information Technology Operational Audit,* issued on September 8, 2009. This report covered Information Technology issues within the Agency for Workforce Innovation for the period July 1, 2008, through June 30, 2009 and selected actions from July 2007.

In accordance with Section 20.055(5)(g), 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

Attachment

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-Voice1-800-955-8770
www.floridajobs.org

Agency for Workforce Innovation (AWI)
Six Month Status Report – Auditor General Report No. 2010-011
Information Technology (IT) Operational Audit

Finding No. 1: Access Controls - Appeals and BOSS (Benefit Overpayment Screening System)

Our audit disclosed instances where access privileges were granted in excess of what was necessary for the performance of job duties and may not have enforced an appropriate separation of incompatible duties. Under these conditions, the risk of unauthorized disclosure, modification or destruction of data and IT resources is increased.

Auditor Recommendation: The Agency should strengthen system access privileges to ensure that an appropriate separation of duties is enforced. The Agency also should develop a formal access authorization process, including written evidence of access requests and authorizations and periodic review of user access privileges. Additionally, the Agency should develop procedures for removing access privileges for all Agency maintained applications to ensure that user accounts of former employees are removed or revoked in a timely manner. Furthermore, the Agency should ensure that the security architecture does not inappropriately give access privileges to users who do not require access to accomplish their job responsibilities.

The audit findings specifically stated:

Bullet #1 (original finding) - One access profile (SUPER) within Appeals allowed users update capability after a case is closed. Five users had been assigned the SUPER profile. However, three of the users did not need the access that this profile provided to perform their job duties. In response to audit inquiry, access for two of the users was deactivated by the Agency and access for the third user was changed to read only.

Bullet #2 (original finding) - One access profile (SYSMNT) within Appeals allowed administrator-level privileges. Six users had been assigned the profile. Two of the users did not need this access to perform their job duties. In response to audit inquiry, the Agency deactivated the access privileges of the two users.

Original AWI Response (Bullets #1 and #2): When the Office of Appeals converted the Appeals Intranet Application from PowerBuilder, development staff who previously needed access to the PowerBuilder application were inadvertently transferred to the new system with super authority. When this was brought to the attention of the Agency during the audit, the access was immediately removed. These findings are considered corrected.

Status as of March 2010: These findings are considered corrected.

Bullet #3 (original finding) - Two of 13 users having access to BOSS were programmers who had been granted administrator access to the production environment. This access allowed the programmers to perform system maintenance such as adding users, creating documents, and updating table codes, contrary to an appropriate separation of duties. Also, the Agency had no access forms on file to document authorizations for this access.

> **Original AWI Response:** Both programmers have had their access levels changed and no longer have administrator access to the production environment. In April 2010, AWI plans to initiate an annual review of access control lists for all AWI managed systems. AWI has developed procedures for removing or revoking access to Agency maintained applications.
>
> **Status as of March 2010:** This finding is considered corrected.

Bullet #4 (original finding) - Twenty-one IT operations staff had been granted domain administrator access that allowed administrative access over all Unemployment Compensation (UC) application servers within the domain. In response to audit inquiry, Agency staff indicated that they were in the process of separating duties based upon job functions in an effort to reduce the number of users with domain administrator access.

> **Original AWI Response:** As resources become available, we will continue our process of separating duties based upon job functions to reduce the number of users with domain administrative access to an appropriate level.
>
> **Status as of March 2010:** Until more resources become available, AWI will monitor domain administrator access as part of its annual User Access review. This finding is considered corrected.

Our audit also disclosed additional access controls related to Appeals and BOSS that needed improvement. Specifically:

Bullet #5 (original finding) - The Office of Appeals did not have a formal process for granting access to Appeals. Requests for read only access for external users to the application were documented by e-mail requests; however, copies of e-mails were not retained by the Agency. The lack of access documentation, including evidence of appropriate approval of requested access privileges, may limit management's ability to ensure the appropriateness of the access privileges to be granted.

Bullet #6 (original finding) - The Agency had not developed policies and procedures for removing the access of former employees. Without written procedures for removing access privileges, there is an increased risk that access privileges may not be timely deleted in a consistent manner pursuant to management's expectations.

Original AWI Response (Bullets #5 and #6): The Agency is developing a written policy for granting access to the appeals system and is working with IT to integrate the removal of access for employees leaving the agency into the termination process for all IT applications. Users within the Office of Appeals have always been required to complete an *Add RACF* (Resource Access Control Facility) *Operator Form* (ISU-27) to request system access. This must be signed by the employee and the supervisor and copies are retained by the Appeals RACF Security Officer.

It is also the policy of the Office of Appeals to require employees within the Office of Appeals who are leaving to complete a *Delete Operator Access Form* (ISU-30) and have it signed by their supervisor. These are also retained by the Appeals RACF Security Officer.

It is only external users with Read Only access who are allowed to obtain access to the appeals application when the individual's supervisor requests access via e-mail to the Appeals RACF Security Officer. When the requestor is outside the Office of Appeals the Appeals Process Manager must also approve access to the appeals application. These e-mails were not retained once the individual was added to the system.

It is now the policy of the Office of Appeals for the RACF Security Officer to maintain copies of the e-mail requests. The RACF Security Officer has also requested to be added to the distribution list for notification of any employee who leaves the employ of the agency. For each termination the RACF Security Officer will eliminate any employee access to the appeals application. Please note that when IT removes network authority for any AWI employee there is no ability to access the appeals application even where direct access to the appeals application has not been removed within the application.

Status as of March 2010: It is now the policy of the Office of Appeals for the RACF Security Officer to maintain copies of the e-mail requests.

The Agency is developing a written policy for granting access to the appeals system and is working with IT to integrate the removal of access for employees leaving the agency into the termination process for all IT

applications. It is anticipated that this finding will be corrected by April 1, 2010.

Bullet #7 (original finding) - Contrary to the Appeals Application Project document that specified what established profiles should allow, a certain profile (CSEPOST) allowed users to change the appeal date within the application. Three of 10 Appeals users included in our sample had been granted this profile. The risk is increased that the unintentionally granted access capability provided by this profile would allow the appeal date to be changed; thereby circumventing time frames established for processing appeals.

Original AWI Response: Only employees within the Clerk's Office or with administrator access should have the ability to change an appeal date. Access outside the Appeals Clerk's Office has been removed. The Agency has revised the Appeals Application Project document to accurately reflect what the profile allows. This finding is considered corrected.

Status as of March 2010: This finding is considered corrected.

Bullet #8 (original finding) - Five of 13 users included in our sample within the Office of Appeals and Benefit Payment Control (BPC) had been granted administrator access privileges to their local computer. Local administrator privileges grant users the ability to add and remove software on their local computer without the knowledge or approval of network administrators. Under these conditions, the risk is increased that a user will install unauthorized or malicious software, jeopardizing the confidentiality, integrity, and availability of Agency data and IT resources.

Original AWI Response: AWI has initiated an agency-wide review of desktop administrative privileges. Each unit was asked to respond and validate the need for desktop administrative privileges. Upon completion of this project, the entire agency will have undergone an administrative privileges review. This project is scheduled for completion in October 2009.

Status as of March 2010: The users listed in the audit finding have either had their local personal computer (pc) administrative privileges removed or the business unit provided justification for their continued use of those privileges. All business units were also notified who in their respective units currently had local pc administrative privileges. Based on the business unit's response, we removed these rights accordingly. If they wished for these rights to remain active, the business unit provided a

written justification for each instance. This finding is considered corrected.

Bullet #9 - Two of nine BPC users included in our sample had been granted access to UC transactions that would allow payments of unemployment claims and the ability to change addresses for claimants, contrary to an appropriate separation of duties.

Original AWI Response: In addition to the RACF security officer and the backup security officer, currently only four individuals in Benefit Payment Control (BPC) have the ability to allow payments and change addresses. Written exception requests for these four employees were approved and submitted to the Internal Security Unit as is required by policy. Two of the four exceptions are managers who frequently assist with the work in all areas of the section, one is temporarily assisting another section part-time and has an exception that will expire in December 2009 and the fourth employee's work duties necessitate access to both functions. This finding is considered corrected.

Status as of March 2010: This finding is considered corrected.

Bullet #10 (original finding) - Twenty-nine network system analysts had been granted access to PC-Duo. 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. Under these conditions, the risk is increased that unauthorized activities could be performed using a local computer without the authorized user's knowledge.

Original AWI Response: AWI is migrating away from using PC-Duo and will be implementing the Microsoft System Control Center. At the time of implementation, AWI will evaluate the risk associated with this finding to determine appropriate control settings. This finding has a corrective action date of January 2010.

Status as of March 2010: AWI has migrated away from using PC-Duo and evaluated the Microsoft System Control Center as an alternative. AWI will continue to evaluate and manage the risk associated with this finding to determine appropriate control settings. This finding is considered corrected.

Finding No. 2: Security Controls (Confidential Finding) - (original finding)

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 Southwood Shared Resource Center (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 staff of the specific issues. Without adequate security controls, 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.

Auditor Recommendation: The Agency and SSRC should implement appropriate security controls to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

Original AWI Response: The Agency, in coordination with SSRC, has reviewed and addressed the appropriate security controls identified in the finding.

Status as of March 2010: This finding is considered corrected.

Finding No. 3: Appeals – Input Data Edits - (original finding)

Application controls include programmed edits that evaluate the accuracy, completeness and validity of input data. Our audit disclosed that 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 increases the risk of inaccurate and invalid data being accepted into the system, jeopardizing the integrity and reliability of the data.

Auditor Recommendation: The Agency should, where practicable, implement additional edits to prevent the entry of invalid data.

Original AWI Response:

The Office of Appeals has added these edits to the list of requested enhancements to the Appeals Application and will work with IT to develop edits to prevent the entry of invalid data. Only the zip code field has a current impact on the processing of cases and the UC Program is currently working to implement address validation software which would alert the office to incorrect mailing addresses.

If an invalid cost center is entered, the transmittal process identifies it as an exception because the computer would be unable to assign the case to an appeals office. The cost center would then be corrected and the case assigned. The adjudication hub codes are not used, but were put in for possible future use when and if the claims and appeals applications communicate to a greater degree. Currently, that field is disregarded. There is a low risk that inaccurate or invalid data would jeopardize the desired outcomes.

Status as of March 2010: The anticipated completion date for this finding is April 2010.

Finding No. 4: Positions of Trust and Related Background Checks - (original finding)

AWI Policy No. 1.08, Positions of Special Trust, provides that Level 2 background checks are to be performed for contractors. In response to audit inquiry, Agency management indicated that all IT contractors were considered to be working in positions of special trust. As similarly noted in our report No. 2009-070, our audit disclosed that, contrary to Agency policy, Level 2 background screening, including Federal background records checks and fingerprinting, had not been conducted on 14 of 36 IT contractors engaged by the Agency as of May 1, 2009. Without performing Level 2 background screening of contractors in these positions, the risk is increased that a person with an inappropriate background could be contracted for one of these positions.

Auditor Recommendation: The Agency should comply with its policy for performing Level 2 background screening, including fingerprinting, for its contractors who work in positions of special trust.

Original AWI Response:

The background checks for the 36 IT contractors in question have been completed. AWI continues to perform Level 2 background checks on all IT contractors who meet the requirements of AWI Policy 1.08. The state mandated process includes a gap of time between when the IT contractor physically arrives to begin the process and the time when the Florida Department of Law Enforcement provides the completed background check documentation. AWI continues to seek methods to reduce this time gap and accompanying risk. This finding has a corrective action date of December 2009.

Status as of March 2010: This finding is considered corrected.

Finding No. 5: Access Controls – UC Claims and Benefits and Highway Safety and Motor Vehicles (HSMV) Cross-Match Application - (original finding)

Effective IT management includes establishing controls over access to programs and data and separation of duties to provide reasonable assurance that unauthorized or erroneous disclosure, modification, or destruction of information will be prevented or timely detected. Periodically comparing authorizations to actual access privileges and access activity helps to ensure that the access that was authorized is the access that has actually been granted. Appropriate access controls also include provisions for user access rights to data to be in line with defined and documented business needs and job requirements. Furthermore, once unauthorized or unusual access activity is identified, it is to be reviewed and apparent or suspected violations are to be investigated.

As also noted in our report No. 2009-070, some programmers, systems staff, and an operator, including contractors, had been granted access privileges that were not required to perform their job duties. Specifically, of the 54 individuals who had been granted access privileges to UC Claims and Benefits production data files, 24 had inappropriate access to the production applications. The 24 individuals included employees from the Agency, Florida Department of Revenue (FDOR), SSRC, and contractors as follows: 19 programmers, 4 systems staff, and 1 operator. Monitoring or reviewing of the access privileges for the above-mentioned individuals had not been performed. 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, as of June 2, 2009, the inappropriate update authority in the production environment had been removed.

In addition, as also noted in audit report No. 2009-070, 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. Without a periodic review of access violations, repeated attempts to compromise the security of cross-match data may not be timely detected or appropriately acted upon by management.

Auditor Recommendation: The Agency and SSRC should strengthen system access privileges to ensure an appropriate separation of duties. In addition, the Agency and SSRC should monitor and review the ongoing appropriateness of access privileges to promote the integrity of the UC System and data. The Agency should also periodically review UC Claims and Benefits user access privileges and HSMV cross-match application access violations.

Original AWI Response:

> **Paragraphs #1 and #2** - In response to audit inquiry, SSRC staff indicated that, as of June 2, 2009, the inappropriate update authority in the production environment had been removed. AWI has requested documented confirmation of

the new security settings from SSRC and is conducting limited testing of access permissions.

Paragraph #3 - The Agency has not created access violation reports for the HSMV cross match because authorization to access the cross match are monitored. Without authority to access the information, access is denied. Only employees provided access to the cross match can access the data and their access is monitored. Because of the low risk that this data could be compromised and in consideration of the record workloads the unemployment compensation program has been working under for over the last year, there are no immediate plans to create access violation reports. However, the Agency is beginning the process of gathering requirements for the new Unemployment Compensation Claims and Benefits Information System. Consideration will be given to creating such reports for the new system.

Status as of March 2010: These findings are considered corrected.