REPORT NO. 2010-011
SEPTEMBER 2009

AGENCY FOR WORKFORCE INNOVATION
SOUTHWOOD SHARED RESOURCE CENTER
UNEMPLOYMENT INSURANCE PROGRAM

Information Technology Operational Audit

For the Period
July 1, 2008, Through June 30, 2009,
and Selected Actions From July 2007

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. During the audit period, the following individuals served as Director:

Director	Dates of Service
Monesia T. Brown	January 2, 2007, through February 2, 2009
Cynthia Lorenzo	Interim Director from February 2, 2009, through June 9, 2009; Director from June 10, 2009

EXECUTIVE DIRECTOR OF THE SOUTHWOOD SHARED RESOURCE CENTER

Pursuant to Sections 282.205(1) and (3), Florida Statutes, effective July 1, 2008, the Southwood Shared Resource Center (SSRC) is established within DMS and is a separate budget entity not subject to control, supervision, or direction of DMS in any manner. The 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 the SSRC. Pursuant to Section 282.203(3)(a), Florida Statutes, the board of trustees is responsible for employing the Executive Director of the SSRC. John Wade was employed as Executive Director on November 24, 2008.

The audit team leaders were Wayne Revell, CISA, and Lynley Trent, CPA, 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.

Within the Agency, the Appeals application (Appeals) is used by the Office of Appeals to manage unemployment benefit appeals cases. The Benefit Overpayment Screening System (BOSS) is used by the Benefit Payment Control (BPC) section to manage payments of unemployment benefits to help ensure the integrity of the UI Program.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to Appeals and BOSS during the period July 1, 2008, through June 30, 2009. Our audit also focused on determining the status of corrective actions regarding prior audit findings disclosed in audit report No. 2009-070, relating to Agency and SSRC IT controls over the UC System. Additionally, our audit focused on Agency activities related to the issuance of UC appeals decisions and the establishment of UC benefit overpayment determinations and redeterminations during the period July 2007 through January 2009.

The results of our audit are summarized below:

Appeals and BOSS

Finding No. 1: **Various access controls relating to Appeals and BOSS needed improvement.**

Finding No. 2: **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.**

Finding No. 3: **Editing of input data in Appeals needed improvement to provide increased assurance of the validity of data within the system.**

Follow-Up on Prior Audit Findings

Finding No. 4: **As also noted in our audit report No. 2009-070, Federal background checks were not performed for some IT contractors.**

Finding No. 5: **The Agency did not ensure the appropriateness of some UC Claims and Benefits access privileges and did not monitor for unauthorized attempts to access the Highway Safety and Motor Vehicle (HSMV) cross-match application. These issues were also disclosed in our audit report No. 2009-070.**

BACKGROUND

The UC System is composed of several interacting subsystems, including the UC Claims and Benefits subsystem, Appeals, and 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.

Pursuant to Section 443.151, Florida Statutes, 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 an application system 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 used by the BPC section to assist staff with determining and generating unemployment compensation overpayment determinations. 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. The SSRC is responsible for supporting the UC System's data center operations. The UI Program is included in the audit of the Federal Awards Programs for the State of Florida for the 2008-09 fiscal year.

FINDINGS AND RECOMMENDATIONS

Appeals and BOSS

Finding No. 1: Access Controls - Appeals and BOSS

Effective IT management includes establishing controls over access to programs and data that enforce an appropriate separation of incompatible duties and provide reasonable assurance that unauthorized or erroneous disclosure, modification, or destruction of information will be prevented or timely detected.

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. Specifically:

- 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.
- 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.
- 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.
- Twenty-one IT operations staff had been granted domain administrator access that allowed administrative access over all 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.

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

- 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.
- 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.
- 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.
- Five of 13 users included in our sample within the Office of Appeals and 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.
- 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.
- 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.

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.

Finding No. 2: 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 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.

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

Finding No. 3: Appeals – Input Data Edits

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.

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

Prior Audit Follow-Up

The Agency had taken corrective actions for the findings included in our report No. 2009-070, except as disclosed in the following paragraphs.

Finding No. 4: Positions of Trust and Related Background Checks

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 (FBI).

DMS Rule 60DD-2.001(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(80), Florida Administrative Code, defines special trust and 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.

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.

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.

Finding No. 5: Access Controls – UC Claims and Benefits and HSMV Cross-Match Application

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, DOR, the 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.

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.

Follow-Up to Management's Response:

In her response to this finding, the Director stated that the Agency had not created access violation reports because authorizations to access the cross match application are monitored and, without authority to access information, access is denied. The point of our finding is that monitoring of unsuccessful or invalid access attempts would strengthen access controls over HSMV cross-match data. Repeated unsuccessful access attempts could be an indicator of someone trying to compromise the security of the system and its data; thus, the creation and monitoring of access violation reports provide a means to timely detect and appropriately respond to such attempts.

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 Appeals and BOSS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- Determine the extent to which the Agency and SSRC corrected, or were in the process of correcting, deficiencies disclosed in audit report No. 2009-070 that are applicable to the UC System.
- Evaluate the effectiveness of established internal controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.
- Evaluate management's performance in achieving compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

The scope of our audit focused on evaluating selected IT controls applicable to Appeals and BOSS and evaluating the Agency's and SSRC's corrective actions regarding IT control deficiencies applicable to the UC System disclosed in the prior audit during the period July 1, 2008, through June 30, 2009. Our audit scope also included examinations of various records and transactions (as well as events and conditions) occurring during the period July 2007 through January 2009.

In conducting our audit, we:

- Interviewed Agency and SSRC personnel.
- Obtained an understanding of Appeals and BOSS, including the processing hardware, software, and user environments; purpose and goals; and the basic data flow though the applications.
- Obtained an understanding of the Appeals and BOSS application controls, including input, processing, output, and user controls.
- Obtained an understanding of general IT controls related to Appeals and BOSS.
- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of selected input, processing, and output control procedures, including the adequacy of Appeals and BOSS

controls to prevent or detect unauthorized or erroneous payments to UC claimants through the use of appropriate access roles.

- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of user application access capabilities, including proper separation of duties for Appeals and BOSS.
- Observed, documented, and evaluated key processes and procedures related to physical and environmental safeguards protecting Appeals and BOSS.
- Observed, documented, tested, and evaluated key processes and procedures related to the Agency and SSRC change control processes for making modifications to Appeals and BOSS.
- Observed, documented, tested, and evaluated key processes and procedures related to the Agency and SSRC security programs, including procedures for security administration, adequacy of review and removal of access privileges, adequacy of review of access to Appeals and BOSS, and the adequacy of password controls related to Appeals and BOSS.
- Obtained an understanding of internal controls and tested key processes and procedures related to the processing of UC appeals and the establishment and recording of UC benefit overpayment determinations and redeterminations in BOSS. Applicable audit procedures included:
  - Evaluating internal controls over the UC appeals process.
  - Testing 30 UC appeals cases, selected from Appeals to determine whether the cases were properly processed, tracked, and adequately supported in compliance with applicable laws, rules, and guidelines.
  - Testing nine applicable appeals decisions to determine whether UC overpayment determinations were properly established in BOSS or redeterminations were properly adjusted in BOSS.
  - Evaluating internal controls over the process of detecting, investigating, and establishing UC benefit overpayment cases.
  - Testing 28 cases established in BOSS to determine whether possible overpayments were properly investigated, documented, and processed in compliance with applicable laws, rules, and guidelines.
  - Testing 29 applicable UC appeals cases and 20 applicable UC benefit overpayment cases to determine whether the applicable records were adjusted in the UC Claims and Benefit System and in compliance with applicable laws, rules, and guidelines.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENTS' RESPONSES

In letters dated August 28, 2009, and August 5, 2009, 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.

EXHIBIT A
MANAGEMENTS' RESPONSES

Charlie Crist
Governor
Cynthia R. Lorenzo
Director

August 28, 2009

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, 2008 through June 30, 2009 and selected actions from July 2007.

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, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

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** - 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** - 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.
>
> > **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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

Bullet #3 - 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.

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.

Bullet #4 - Twenty-one IT operations staff had been granted domain administrator access that allowed administrative access over all 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.

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.

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

Bullet #5 - 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 - 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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

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.

Bullet #7 - 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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

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.

Bullet #8 - 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.

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.

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.

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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

Bullet #10 - 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.

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.

Finding No. 2: Security Controls (Confidential 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.

AWI Response:

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

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

Finding No. 3: Appeals – Input Data Edits

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.

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.

Finding No. 4: Positions of Trust and Related Background Checks

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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

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.

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.

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

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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Agency for Workforce Innovation (AWI)
Unemployment Compensation (UC) Information Technology (IT) Audit,
July 1, 2008 through June 30, 2009 and Selected Actions From July 2007
Response to Preliminary and Tentative Findings

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.

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.

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

August 5, 2009

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, *Unemployment Insurance Program, Agency for Workforce Innovation and the Southwood Shared Resource Center.* Our response corresponds with the order of your preliminary and tentative findings and recommendations.

Finding No. 2 - Security Controls

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

Recommendation

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

Response

The SSRC has implemented the appropriate controls to correct the identified security issues.

Finding No. 5 – Access Controls

The Agency did not ensure the appropriateness of some UC Claims and Benefits access privileges and did not monitor for unauthorized attempts to access the Highway Safety and Motor Vehicle (HSMV) cross-match application. These issues were also disclosed in our audit report No. 2009-070.

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.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES

Response

The SSRC has reviewed the report pertaining to employee access and will continue to work with AWI to strengthen the current policy on access privileges to ensure the appropriate segregation of duties.

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 Wade
Executive Director, Southwood Shared Resource Center

CC: Nelson Hill, Chairman of the SSRC Board
John Davis, Audit Director, DMS

A Certified Tier III Facility