REPORT NO. 2012-138
MARCH 2012

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

INTEGRATED BENEFIT RECOVERY SYSTEM (IBRS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

Pursuant to Section 20.19(2)(a), Florida Statutes, the Secretary of the Department of Children and Family Services is appointed by the Governor, subject to confirmation by the Senate. During the period of our audit, the following individuals served as Secretary:

David E. Wilkins	From January 24, 2011
George H. Sheldon	From October 17, 2008, to March 3, 2011

The audit team leader was Bill Tuck, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

Integrated Benefit Recovery System (IBRS)

SUMMARY

Section 414.41, Florida Statutes, provides that, whenever it becomes apparent that any person or provider has received any public assistance to which she or he is not entitled, through either simple mistake or fraud on the part of the Department of Children and Family Services (Department) or on the part of the recipient or participant, the Department shall take all necessary steps to recover the overpayment. The Department established, operates, and maintains the Integrated Benefit Recovery System (IBRS) in its efforts to recover improperly issued public assistance benefits based on the benefit recovery claim referrals received from the Florida Online Recipient Integrated Data Access (FLORIDA) System. IBRS assists in the identification, investigation, determination, and collection of benefit overpayments.

Our audit focused on evaluating selected information technology (IT) controls applicable to IBRS. The results of our audit are summarized below:

Finding No. 1: Benefit recovery claim referrals could be canceled in IBRS without supervisor approval and the cancellations were not timely monitored.

Finding No. 2: IBRS access privilege authorization documentation for some users was incomplete or missing.

Finding No. 3: The Department did not timely deactivate the IBRS access privileges of some former employees.

Finding No. 4: The access privileges of some contractors and a Department employee were inappropriate for their job responsibilities and did not enforce an appropriate separation of duties.

Finding No. 5: Certain security controls related to user authentication needed improvement.

BACKGROUND

The Department of Children and Family Services (Department) was created pursuant to Section 20.19, Florida Statutes, with a stated mission to work in partnership with local communities to ensure the safety, well-being, and self-sufficiency of the people served. Also, Section 409.031, Florida Statutes, designates the Department as the State agency responsible for the administration of social service funds under Title XX of the Social Security Act.

According to Department of Children and Family Services Rule 65A-1.203, Florida Administrative Code, the Economic Self-Sufficiency (ESS) Program Office is the entity within the Department responsible for public assistance eligibility determination. Public assistance programs include Temporary Assistance for Needy Families, Refugee Assistance, Supplemental Nutrition Assistance, and Medical Assistance Programs. The ESS Program Office utilizes the FLORIDA System to assist in eligibility determination and benefit issuance for public assistance programs.

The Department uses IBRS in its efforts to collect and recover overpaid benefits and benefits paid to ineligible clients. IBRS was developed as part of the Department's initiative to produce a newly retooled and modernized Web-based public assistance service delivery system, the Automated Community Connection to Economic Self-Sufficiency (ACCESS). IBRS gathers and processes benefit recovery information and directly interfaces with the FLORIDA System. IBRS is housed and operated in the Northwood Shared Resource Center (NSRC).

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Benefit Recovery Claim Referral Cancellations

IT controls in the business process environment can be manual or automated. Automated controls are system based, such as edits and validations, and can be used to control the correctness or accuracy of data. Manual controls are procedures that require human intervention, such as the approval of a transaction, and are typically used to assure the reasonableness or propriety of transactions.

Benefit recovery claim referrals are created in the FLORIDA System by public assistance case workers. The referrals migrate via system interface to IBRS where the benefit recovery process is initiated. Benefit recovery claim cases remain active in IBRS until closed, canceled, written-off, or voided. Voided benefit recovery claims require the approval of a supervisor. Write-offs are processed by the Benefit Recovery Financial Management unit and are normally performed because of death, bankruptcies, identity thefts, claims for less than $25 with no activity in the last three years, or claims with no activity in the last ten years. The reduction of a benefit recovery claim to $0 prompts IBRS to systematically close the claim. Benefit recovery claim referrals from the FLORIDA System can be canceled by any IBRS case worker or supervisor who has access privileges to the referrals.

Our audit disclosed that benefit recovery claim referrals could be canceled in IBRS without supervisor approval. They were subject to monitoring by Quality Management staff only on an annual basis. Although reports were available that would allow Central Office or local supervisors to monitor cancellations on an ongoing basis, the lack of supervisory approval and timely monitoring of cancellations increases the risk that a benefit recovery claim referral may be erroneously or maliciously canceled without timely detection.

Recommendation: The Department should ensure that benefit recovery claim referral cancellations are approved by a supervisor and timely monitored for appropriateness on an ongoing basis.

Finding No. 2: Documentation of IBRS User Account Access Privileges

Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. Agency for Enterprise Information Technology Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. According to the *Benefit Recovery Collections Resource Guide, a FLORIDA Individual Security Information Form* (access authorization form) must be completed and sent to the security officer when requesting IBRS access privileges.

For a sample of 25 of the 624 IBRS user accounts, we requested the corresponding access authorization forms to determine the level of access that had been authorized by management. For 15 of the 25 user accounts included in our sample, Department staff could not provide the access authorization forms. Department staff provided us with access authorization forms for the remaining 10 user accounts in the sample; however, one or more of the required authorization signatures was missing from nine of the ten forms and three of the ten forms lacked security profile information required for the access authorization form.

In response to audit inquiry, Department staff indicated that access authorization forms for some of the user accounts in our sample could not be located as a seven-year retention cycle was in place for selected documentation and the missing access authorization forms may have been destroyed as part of this data retention practice. Without

appropriately documented access authorization forms for IBRS user accounts, management's ability to ensure that user access privileges do not exceed what is necessary for the accomplishment of assigned job responsibilities may be limited.

Recommendation: The Department should ensure that access authorization forms are appropriately completed and maintained for all user accounts.

Finding No. 3: Timely Deactivation of Access Privileges

Effective logical access controls include provisions for the timely deactivation of former employee access privileges when employment terminations occur. Prompt action is necessary to ensure that the former employee or others do not misuse the former employee's access privileges. According to the Department's *Children and Families* (*CF) Operating Procedure No. 60-70, Chapter 1*, supervisors are responsible for notifying the appropriate security manager or officer to delete access to assigned data systems within 24 hours of the employee's termination.

We reviewed logical access privileges for IBRS for the 988 Department employees who had terminated employment during the period of July 1, 2010, through June 30, 2011. Our review disclosed that the access privileges of some former employees had not been timely deactivated, increasing the risk of inappropriate activity within IBRS. Specifically, IBRS access privileges for 14 of the 988 former employees remained active beyond the next business day for various time periods up to 35 days after termination. The access privileges for 1 former employee were not deactivated for 83 days after termination. Additionally, the access privileges of another former employee were still active as of the date of our review. Upon audit inquiry, the Department deactivated the access privileges of this former employee on September 30, 2011, which was 273 days after termination.

Our review further disclosed that 1 former employee's user account and access privileges were used to access IBRS after the employee's termination from employment. The employee's termination date was April 1, 2011, but her access privileges were not deactivated until April 6, 2011, and log information provided by the Department indicated that her account was used to access and view IBRS on April 4, 2011. Our review of the logs indicated that no updates were made by the user account in IBRS. However, available IBRS log information was not sufficient to demonstrate what was viewed in IBRS with the user account. As of January 23, 2012, the Department was in the process of determining which clients' information had been accessed.

Recommendation: The Department should ensure that the access privileges of former employees are deactivated in a timely manner to minimize the risk of compromising IBRS data and IT resources.

Finding No. 4: Appropriateness of Access Privileges

Effective access controls include measures that limit contractor and employee access privileges to only what is necessary in the performance of assigned job responsibilities and restrict contractors and employees from performing incompatible functions or functions outside of their areas of responsibility. For example, application programmers should typically not require or be granted access to production libraries or data or have administrative access privileges on database and application servers.

Our review of the Department's file permissions for selected folders and files on the IBRS production application and database servers and the IBRS development application server disclosed that five contractors in the ACCESS

Applications Unit who had application programming duties were granted inappropriate access permissions to IBRS programs and data. Specifically:

- Four contractors had modify, read and execute, list folder contents, read, and write permissions to folders on the server in which the IBRS production application programs resided.
- Two contractors, including one of the four contractors described above with access permissions to the production application program folders, had modify, read and execute, list folder contents, read, and write permissions to a folder on the server in which IBRS programs resided for acceptance testing purposes.
- One of the contractors described above with excessive permissions to the production application programs also had modify, read and execute, list folder contents, read, and write permissions to the folder on the server in which the IBRS production data resided.

Additionally, during our review of the appropriateness of administrator-level access to the IBRS servers, we identified a Department employee with application programming responsibilities as a member of an administrative group on the IBRS database server and the IBRS application server. This employee previously worked as a database analyst for the Department and may have required administrator-level access privileges at that time. However, in her current position as an application programmer, she no longer required administrator-level access privileges on the IBRS servers.

Allowing application programmers elevated access to production application programs, development application programs in the acceptance region, and production data, together with administrator-level access to the database and application servers did not enforce an appropriate separation of duties and increased the risk of unauthorized disclosure, modification, or destruction of IBRS data and IT resources.

Recommendation: The Department should review the folder and file permissions of contractors and employees for all paths of access to IBRS programs and data and adjust the permissions to ensure that access permissions are commensurate with assigned job responsibilities. The Department should also review all administrator-level access privileges to the IBRS database and application servers and make adjustments to ensure that access privileges to the servers are appropriate.

Finding No. 5: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to user authentication for IBRS to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit during the period June 2011 through October 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to IBRS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected IT controls applicable to the IBRS. The audit included selected general IT controls over logical access to programs and data and application change management. The audit also included selected IBRS application and user controls relevant to IBRS. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from July 2010 through October 2011 and selected Department actions through January 2012.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of IBRS, including the purpose or goals of the application and related compliance requirements; the application data and business processing flows; the IT and user organizational structure and management hierarchy related to the logical security of IBRS; the computing platforms and related software; the access paths by which IBRS IT resources can be viewed, modified, or deleted; the user account administration processes for authorizing, creating, modifying, and revoking IBRS application and IT resources user accounts; and the application change management process.
- Evaluated on a sample basis the appropriateness of user access privileges for IBRS application users. Specifically, we sampled the access privileges for 25 of 624 IBRS user accounts to evaluate and determine if the access was authorized on documented forms, was appropriate for the users' job responsibilities, and enforced an appropriate separation of duties.
- Tested the appropriateness of administrator logical access privileges to system resources related to IBRS. Specifically, we evaluated the appropriateness of access privileges granted to the IBRS development application, production application, and database servers and the appropriateness of elevated (administrator group) access privileges granted to the IBRS production database and the IBRS production application server.
- Tested IBRS access privileges to determine if Northwood Shared Resource Center (NSRC) Department IT staff were appropriately restricted from updating IBRS data through the IBRS application.
- Reviewed the effectiveness of Department procedures for timely deactivating the IBRS user access privileges of former Department employees.
- Reviewed the effectiveness of procedures for timely deactivating IBRS server and database access privileges of former Department contractors and employees. Specifically, we determined whether all Department users identified with access privileges to the IBRS servers or database were currently employees or contractors and

had not terminated employment, terminated the contracts, or been reassigned to other duties that did not require the access privileges.

- Reviewed the adequacy of RACF password controls for IBRS, including parameter settings for revocation of inactive accounts, revocation of unsuccessful logon attempts, password complexity, password change interval, password history, and system time-out.
- Reviewed on a sample basis 10 of 28 IBRS application change requests that occurred between July 1, 2010, and June 30, 2011, to determine whether IBRS application changes were adequately authorized, documented, tested, approved for production, and implemented.
- Reviewed selected application and user controls related to IBRS for the recovery of benefits, including the timeliness of the benefit recovery, and the follow-up and resolution of benefit recovery cases.
- We did not test network and barrier controls for the Department related to IBRS because these controls are the responsibility of NSRC and will be addressed in a future audit of NSRC.
- We did not test password controls for the IBRS database because these controls are the responsibility of NSRC and will be addressed in a future audit of NSRC.

AUTHORITY

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

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated March 8, 2012, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

State of Florida
Department of Children and Families

Rick Scott
Governor

David E. Wilkins
Secretary

March 8, 2012

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

Dear Mr. Martin:

Thank you for your February 9 letter accompanying the preliminary findings and recommendations of your report to be prepared on the Information Technology Operational Audit of the Department of Children and Family Services, Integrated Benefit Recovery System (IBRS).

The Department generally concurs with the findings of your report. Enclosed is the Department's response to the specific recommendations you provided.

If you or your staff have additional questions, please contact Mr. Matthew Dempsey at (850) 717-4781, or Don Sherman at (850) 487-8970.

Sincerely,

David E. Wilkins
Secretary

Enclosure

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Information Technology Operational Audit of the
FLORIDA DEPARTMENT OF CHILDREN AND FAMILY SERVICES
INTEGRATED BENEFIT RECOVERY SYSTEM (IBRS)

Finding No. 1: Benefit Recovery Claim Referral Cancellations

Recommendation: The Department should ensure that benefit recovery claim referral cancellations are approved by a supervisor and timely monitored for appropriateness on an ongoing basis.

Department Response: Monthly, the Benefit Recovery supervisor will monitor the cancelled referrals listed on the Referral Monitoring (IBRS502) report in IBRS for accuracy.

Finding No. 2: Documentation of IBRS User Account Access Privileges

Recommendation: The Department should ensure that access authorization forms are appropriately completed and maintained for all user accounts.

Department Response: The Department concurs with this finding and information is being distributed to re-emphasize the retention policy for maintaining user access documentation.

Finding No. 3: Timely Deactivation of Access Privileges

Recommendation: The Department should ensure that the access privileges of former employees are deactivated in a timely manner to minimize the risk of compromising IBRS data and IT resources.

Department Response: The Department concurs with this finding and information is being distributed to re-emphasize the importance of timely deactivating terminated employees.

Finding No 4: Appropriateness of Access Privileges

Recommendation: The Department should review the folder and file permissions of contractors and employees for all paths of access to IBRS programs and data and adjust the permissions to ensure that access permissions are commensurate with assigned job responsibilities. The Department should also review all administrator-level access privileges to the IBRS database and application servers and make adjustments to ensure that access privileges to the servers are appropriate.

Department Response: The Department concurs with this finding and action has been taken to remove inappropriate access and enforce rules related to the separation of duties.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 5: Security Controls – User Authentication

Recommendation: The Department should implement appropriate security controls related to user authentication for IBRS to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Department Response: The Department concurs with this finding.