REPORT NO. 2010-130
MARCH 2010

DEPARTMENT OF REVENUE

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM, CHILD SUPPORT ENFORCEMENT (CSE) COMPONENT AND CHILD SUPPORT ENFORCEMENT AUTOMATED MANAGEMENT SYSTEM (CAMS)

Information Technology Operational Audit

For the Period
July 1, 2008, Through June 30, 2009,
and Selected Actions Through December 15, 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE DEPARTMENT OF REVENUE

Pursuant to Section 20.21(1), Florida Statutes, the head of the Department of Revenue is the Governor and Cabinet (Attorney General, Chief Financial Officer, and Commissioner of Agriculture). Pursuant to Section 20.05(1)(g), Florida Statutes, the Governor and Cabinet is responsible for appointing the Executive Director of the Department of Revenue. Lisa Echeverri served as Executive Director during the audit period.

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

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF REVENUE

Florida Online Recipient Integrated Data Access (FLORIDA) System,
Child Support Enforcement (CSE) Component
and
Child Support Enforcement Automated Management System (CAMS)

SUMMARY

Pursuant to Section 409.2557(1), Florida Statutes, the Department of Revenue (Department) is designated as the State agency responsible for the administration of Florida's Child Support Enforcement (CSE) Program under Title IV-D of the Federal Social Security Act. Pursuant to Title 45, Section 302.85(a), Code of Federal Regulations, states are required to have in effect a computerized child support enforcement system. The Florida Online Recipient Integrated Data Access (FLORIDA) System, operated and maintained by the Department of Children and Family Services, was the Title IV-D system that automated case management. To meet Federally required changes resulting from the Family Support Act of 1988 and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, the Department developed the Child Support Enforcement Automated Management System (CAMS) to enhance case management and ultimately replace the FLORIDA System CSE Component. CAMS is a phased development project. Phase I enhanced case enforcement through the use of automated enforcement tools. CAMS interfaces with the FLORIDA System CSE Component to maintain the synchronization of data between the two systems.

Our audit focused on evaluating selected information technology (IT) controls applicable to the FLORIDA System CSE Component and CAMS for the period July 1, 2008, through June 30, 2009, and selected actions through December 15, 2009. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2008-020 that were applicable to the scope of this audit.

The results of our audit are summarized below:

Security Controls

Finding No. 1: Documentation of authorization for FLORIDA System CSE Component and CAMS access privileges for some users was missing, incomplete, or inaccurate. Similar issues regarding CAMS were disclosed in our report No. 2008-020.

Finding No. 2: The access privileges of some FLORIDA System CSE Component and CAMS users were not appropriate for their job responsibilities. Similar issues regarding CAMS access privileges were disclosed in our report No. 2008-020.

Finding No. 3: Some access privileges in the FLORIDA System CSE Component and CAMS did not enforce an appropriate separation of incompatible duties. Similar issues regarding CAMS access privileges were disclosed in our report No. 2008-020.

Finding No. 4: The Department did not timely remove FLORIDA System CSE Component and CAMS access privileges of some former employees and contractors. Similar issues regarding the removal of CAMS access privileges were disclosed in our report No. 2008-020.

Finding No. 5: The Department did not periodically review the appropriateness of CAMS user access privileges.

Finding No. 6: The Department could not provide documentation of its evaluation of network vulnerability scans or subsequent actions to mitigate vulnerabilities. Similar issues regarding CAMS were disclosed in connection with our report No. 2008-020.

Finding No. 7: **Certain Department security controls related to user authentication needed improvement. Similar issues were disclosed in connection with our report No. 2008-020.**

Application Controls

Finding No. 8: **Because of limitations in CAMS access control functionality, many CAMS users inappropriately had the ability to perform enforcement override transactions on cases. Additionally, the Department did not monitor enforcement override transactions to ensure that such users had not performed unauthorized overrides.**

Finding No. 9: **The Department had not resolved some issues with address information in CAMS that were previously noted in our report No. 2008-020.**

Finding No. 10: **The Department did not have written procedures for supervisor monitoring and follow-up of unprocessed CAMS tasks.**

BACKGROUND

The Department has administered the Child Support Enforcement (CSE) program since 1994. The objective of the CSE program is to obtain financial and medical support for children when both parents do not assume full responsibility for supporting their children. The purpose of the program is to ensure that, to the greatest extent possible, children are provided for from the resources of the responsible parents. Participation in the program is mandatory for the parents of children receiving public assistance (PA) and voluntary for others. In PA cases, child support payments collected by the CSE program are used to reimburse the State for amounts paid for PA on behalf of the child.

The CSE Program Office administers the CSE program in five regions throughout the State. The Program Office performs specific functions to assist the regions in locating noncustodial parents, establishing paternity, establishing and modifying obligations for financial and medical support, and enforcing and collecting these obligations. The Department of Children and Family Services (DCFS) maintains the FLORIDA System that is comprised of two components, PA and CSE. The PA Component is used by the DCFS Economic Self-Sufficiency Program Office in PA program eligibility determination and benefit issuance. DCFS refers PA applicants to the Department to begin CSE efforts when necessary.

In October 2003, the Department began the CAMS initiative using a phased development approach to replace the FLORIDA System CSE Component as the application system supporting Florida's CSE program. CAMS will interface with the FLORIDA System until the CSE Component is phased out and replaced by CAMS. The Department elected to use SAP Public Services, Inc., software to develop CAMS. Case compliance enforcement and locate (location of noncustodial parents or guardians) functionality was selected for CAMS Phase I development and was implemented in 2006. Since implementation, new cases are created in the FLORIDA System and updated to CAMS by a nightly update. Case creation, case maintenance, payment processing, fund distribution, and additional case enforcement functionality will be automated in CAMS during the development of CAMS Phase II, which is scheduled for release in 2012.

FINDINGS AND RECOMMENDATIONS

Security Controls

Finding No. 1: Documentation of User Access Authorizations

Effective security controls include logical (electronic) access controls that restrict legitimate and appropriate users to the specific IT resources needed and prevent others from accessing the resources. Access controls include, among other things, the use of access authorization forms to document the access privileges that have been authorized by management for system users to be granted.

FLORIDA System CSE Component. According to the Department's Security Operational Procedure 016, FLORIDA System user account administration (creating, changing, or revoking user access privileges to the FLORIDA System CSE Component) is shared between regional and headquarters security officers. Regional security officers manage the FLORIDA System access privileges of employees within their assigned districts. The headquarters security officer manages security profiles and also performs user account management for headquarters staff and region staff with selected high risk profiles. According to the Security Operational Procedure 016, access authorization forms must be completed and submitted to security officers to add, change, or revoke FLORIDA System CSE Component user access privileges. Required information on these forms includes first and last name, action required, user identification code (ID), security profile name, and security level. Additionally, selected high risk profiles require the completion of an additional profile specific form. Our audit disclosed instances where, as discussed in the following paragraphs, the Department had not appropriately documented authorizations of user access privileges granted to some employees, contrary to the Security Operational Procedure 016.

For a sample of 30 FLORIDA System CSE Component user accounts including both employees and contractors, we requested the corresponding access authorization forms to determine the level of access that had been authorized by management. For 1 of the 30 user accounts included in our sample, Department staff could not provide the authorization forms.

For the remaining 29 user accounts in our sample, we inspected the authorization forms that Department staff provided to us. For 5 of the 29 user accounts, the authorization forms were missing required information. Specifically, 2 lacked the security profile, 2 lacked the required approval signature of the Payment Processing Fund and Distribution Process (PPFDP) Manager, and l lacked both the security profile and the approval signature of the PPFDP Manager.

CAMS. According to CAMS security procedures, user account administration (creating, changing, or revoking user access privileges to CAMS) is performed by CAMS security administration staff. CAMS end-user access requests are documented on CSE CAMS Access and Training Request Forms (CS AT-30). Access requests for systems staff are documented on a CAMS User Request Form for Production Systems. As similarly noted in our report No. 2008-020, the Department had not appropriately documented authorizations of user access privileges granted to some employees and contractors.

For a sample of 40 CAMS end users and systems staff users, including both employees and contractors, we requested the corresponding access authorization forms to determine the level of access that had been authorized by management. For 4 of the 40 end users and systems staff users included in our sample, Department staff could not provide the authorization forms.

For the remaining 36 end users and systems staff users in our sample, we inspected the authorization forms that Department staff provided to us. For 8 of the 36 users, the authorization forms were missing required information. Specifically, none of the 8 access request forms specified the access level requested. Without appropriately documented user access authorization forms, management's ability to ensure that user access privileges granted to employees or contractors did not exceed what is necessary for the accomplishment of assigned job duties is limited.

Recommendation: The Department should ensure that access authorization forms for the FLORIDA System CSE Component and CAMS are appropriately completed and maintained.

Finding No. 2: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job responsibilities. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Our audit disclosed that some FLORIDA System CSE Component and CAMS users, including both employees and contractors, had update access privileges that were not necessary for their job responsibilities. These conditions increase the risk of errors, fraud, misuse, or other unauthorized modification of Department data. Similar issues regarding CAMS user access privileges were noted in our report No. 2008-020. Specifically:

- The FLORIDA System CSE Component update access privileges for 8 of 30 users included in our sample were not necessary for their job responsibilities. In response to audit inquiry, Department staff indicated that they subsequently removed the unnecessary update access privileges of the 8 users.
- The CAMS update access privileges for 16 of 18 end-users included in our sample were not necessary for their job responsibilities.
- The CAMS system-level update access privileges for 6 of 22 IT staff included in our sample were not necessary for their job responsibilities. This issue was also noted in our report No. 2008-020 for 3 of the 6 IT staff.
- Of the 22 CAMS IT staff included in our sample, 16 also had end-user access privileges to CAMS for production troubleshooting and problem resolution that allowed the IT staff to make updates to production data in CAMS. According to Department staff, the job responsibilities of the 16 IT staff did not require the ability to make data changes in production. However, the 16 IT staff had been given the end-user update privileges because, at the time the privileges were established, the ability did not exist to grant view-only privileges. Although the Department had a signed acceptance of risk form for the update access granted to the 16 IT staff, the Department did not monitor the use of the access privileges by the IT staff, contrary to the representations in the Department's acceptance of risk form, to ensure that these users were not making unauthorized data changes in production. As of July 1, 2009, the Department had not developed access monitoring reports for this purpose.

Two profiles existed within the FLORIDA System CSE Component that were intended for users who required inquiry only access to the system. However, our audit disclosed that the two profiles also allowed selected update ability to case data. In response to audit inquiry, Department staff indicated that both of the profiles had been modified as of December 15, 2009, to allow inquiry only access.

Recommendation: The Department should limit access privileges to the FLORIDA System CSE Component and CAMS resources to only what is needed to perform job responsibilities. Additionally, update access privileges assigned to system staff for production CAMS should be monitored as required by the Department's acceptance of risk forms.

Finding No. 3: Separation of Duties

An important aspect of IT security management includes establishing IT access privileges that enforce an appropriate separation of incompatible duties. Separating incompatible duties diminishes the risk that errors or fraud will go undetected because the activities of one group or individual will serve as a check on the activities of the other group or individual.

Our audit disclosed that the access privileges of some users within the FLORIDA System CSE Component and CAMS and in both systems combined allowed the performance of system functions that were contrary to an appropriate separation of duties. These conditions, described in the following paragraphs, increase the risk that erroneous or fraudulent transactions could be processed without timely detection.

One of the 30 users included in our sample and previously discussed in Finding No. 2 was a contractor providing legal services who had update access privileges in the FLORIDA System CSE Component that allowed her to update case management data. According to Department guidelines, such update access privileges should be restricted from contractors providing legal services. In response to audit inquiry, Department staff indicated that the contractor was a former employee whose employee-level access privileges had not been removed.

One of the 22 IT staff included in our sample and previously discussed in Finding No. 2 had a combination of assigned access privileges that allowed the ability to both change CAMS production source code and perform updates to production CAMS data as an end user. This combination of access privileges was contrary to an appropriate separation of duties. A similar issue was noted in our report No. 2008-020.

Within the FLORIDA System CSE Component, specific finance screens allow the user to create or assign payments. Our audit disclosed that some users, contrary to an appropriate separation of duties, could create or assign a payment in the FLORIDA System CSE Component and update addresses for the custodial family in CAMS.

Specifically, we examined, on a sample basis, the access privileges of 70 users who had access privileges in either the CSE Component or CAMs. From our sample, we determined that 45 of the 70 users had access privileges in both systems. Of the 45 users who had been granted update access privileges to the CSE Component finance screens used to create or assign payments, 7 also had the capability in CAMS to change custodial family addresses.

In addition, a Department security profile guide was incomplete, limiting the ability of security administration staff to prevent the establishment of an incompatible combination of CSE Component and CAMS access privileges. It was the Department's practice for CSE Component security administration staff, prior to granting access to profiles that allow a user to create or assign payments, to communicate with CAMS security administration staff regarding the user's access in CAMS to ensure that a combination of incompatible access privileges was not created. CSE Component security administration staff relied on a security profile guide to prevent granting access privileges in the FLORIDA System CSE Component that were incompatible with the user's established access privileges in CAMS. However, our audit disclosed that the guide did not identify six CSE Component profiles that provided the ability to create or assign a payment. Consequently, security administrators may not have been alerted to avoid assigning users any of the six CSE Component profiles and CAMS access privileges that allowed the ability to update custodial family addresses, contrary to an appropriate separation of duties.

Of the six CSE Component profiles, Department staff stated in response to audit inquiry that:

- Two profiles were assigned to IT staff responsible for resolving production issues in CAMS. As of May 31, 2009, eight IT staff had been assigned the profiles. Department staff changed the two profiles on October 29, 2009, to remove the ability to assign payments in the CSE Component.

- The remaining four profiles should have been identified in the security profile guide as incompatible with address update privileges in CAMS. Department staff, under the direction of the Information Security Assurance Committee (ISAC), was in the process of identifying the number of users who had been assigned the four profiles. For these users, Department staff planned to modify user access privileges and profiles as appropriate to resolve any incompatible duties that are identified.

Recommendation: The Department should enhance the effectiveness of FLORIDA System CSE Component access controls to ensure that contractors do not possess access privileges reserved for Department staff. Additionally, the Department should ensure that CAMS systems staff are not assigned access privileges that allow them to perform incompatible functions. The Department should also ensure that users with access privileges to both systems cannot create or assign payments and also update custodial family addresses in CAMS. Additionally, the Department should ensure that the FLORIDA System CSE Component documentation is updated to accurately reflect which access profiles are incompatible with the ability in CAMS to update addresses.

Finding No. 4: Timely Removal of Access Privileges

Effective logical access controls include provisions for the timely removal of former employee and contractor access privileges when employment or contract terminations occur. Prompt action is necessary to ensure that access privileges are not misused by the former employee, contractor, or others. According to the Department's Information Security Policy, DOR-SEC-004, a user's access privileges are to be revoked immediately upon termination of employment or when the user transfers to a position where access to the IT resource is no longer required.

Upon audit request, the Department provided us with a list of all 348 employees who terminated employment during the period July 1, 2008, through June 24, 2009. Additionally, the Department provided us with a list of 116 contractors who terminated contractual services during the period July 1, 2008, through June 30, 2009. Our comparison of these lists to users with access privileges to the FLORIDA System CSE Component and CAMS disclosed that the access privileges of some former employees and contractors were not timely removed, increasing the risk of inappropriate activity within the FLORIDA System CSE Component and CAMS. Similar issues regarding CAMS access privileges were noted in our report No. 2008-020.

Specifically, the FLORIDA System CSE Component access privileges of 26 former employees and 39 former contractors remained active for periods ranging from 2 to 333 days after termination. Additionally, for CAMS, the access privileges of 20 former employees and 32 former contractors remained active for periods ranging from 3 to 289 days after termination. According to Department staff, none of these access privileges were used to access the system after termination.

Recommendation: The Department should ensure that the access privileges of former employees and contractors are removed in a timely manner in order to minimize the risk of compromising CSE program data and IT resources.

Finding No. 5: Periodic Review of CAMS Access

Periodic review of user access privileges help ensure that user access privileges remain appropriate. Written policies and procedures help provide guidance and direction to employees responsible for performing such reviews by allowing for better communication and consistent application of management intended controls.

The Department did not review CAMS access privileges on a periodic basis. According to CAMS security administration staff, Departmental system owners were responsible for ensuring that the access granted to users was appropriate for their system. However, no written Departmentwide policies or procedures existed that required a periodic review of access privileges by system owners.

As time permitted, CAMS security administration staff produced and reviewed various access reports to determine whether access was still required. In response to audit inquiry, Department staff indicated that the last reviews of CAMS user access privileges were performed in May 2009 and July 2008 by security administration staff. During the review in May 2009, security administration staff revoked 96 inactive user IDs. The dates the user IDs and associated access privileges were last used ranged from July 18, 2006, to December 31, 2008. Additionally, production access roles for 65 former CAMS Phase I contractors were removed in May 2009 to ensure when CAMS Phase II development began that access to CAMS production was not inadvertently given to the former contractors if they were rehired and given network access.

The lack of a periodic review of access privileges increases the risk that excessive or inappropriate access privileges will not be timely detected or removed, as demonstrated by the excessive or unnecessary IT resource access privileges previously described in Finding Nos. 2, 3, and 4 of this report. Under such conditions, the risk is increased of unauthorized disclosure, modification, and destruction of CAMS data and IT resources.

Recommendation: The Department should establish written policies and procedures for the periodic review of CAMS access privileges by system owners.

Finding No. 6: Vulnerability Scanning

Risk management, the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, is an important component of a successful IT security program. Identifying IT system vulnerabilities is a major step in the risk assessment process. Automated vulnerability scanning tools can be used to scan a group of host computers or a network for known vulnerabilities. Vulnerability scanning helps identify outdated software versions, missing patches, and unsecure configurations. Vulnerability scanning often produces false positives (false indications of vulnerabilities); therefore, manual review is necessary to accurately interpret scanning results. National Institute of Standards and Technology (NIST) guidelines recommend the generation of a report that summarizes the results of scanning and analysis, including identification of critical vulnerabilities and mitigating actions that will be taken. Use of vulnerability scanning tools helps ensure that system software is updated and secured in a timely manner.

The Department did not perform vulnerability scanning on a regular basis throughout the audit period, as similarly noted in connection with our report No. 2008-020. According to Department security staff, the Department began using scanning software in March 2009. Network scans were being performed once a week on 15 servers at a time. The results of scanning were sent to network staff for evaluation and mitigation. In response to audit inquiry, Department staff indicated that results of scanning evaluation and mitigation activities were not available. According to Department staff, they were still in the process of determining how to document the results of such activities.

Without documented results of vulnerability scanning evaluation and planned mitigation actions, there is an increased risk that vulnerabilities may not be mitigated leaving systems susceptible to attack.

Recommendation: The Department should continue its efforts to implement a process for documenting the results of vulnerability scanning evaluation and mitigation.

Finding No. 7: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. As similarly noted in our report No. 2008-020, our audit disclosed certain Department security controls related to user authentication controls that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management 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 Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of data and IT resources.

Application Controls

Finding No. 8: Enforcement Overrides

Effective application security controls include restricting end-user access privileges to only those necessary to perform their responsibilities. According to the CSE Policy and Procedures Manual, Section 7420 Enforcement Overrides, authorized CAMS users have the ability to manually override any or all enforcement activities on a case when appropriate. It is the CSE Program's policy to lawfully pursue support obligation collections in accordance with Federal and State laws and regulations. Only authorized staff are to use the enforcement override procedures when the case circumstances require it. Authorized users, including CSE Trainers, supervisors, designated Revenue Specialist IIs, and Revenue Specialist IIIs, have the authority to set or remove enforcement overrides.

Our audit disclosed that CAMS did not provide the ability to assign view-only access privileges to enforcement override screens. Consequently, all users with access to these screens, including some who only required the ability to view overrides to perform their job responsibilities, had the ability to both view overrides and perform enforcement override transactions (setting and removing overrides).

As of November 6, 2009, 756 users had access to enforcement override screens. In response to audit inquiry, Department staff stated that, of the 756 users, 481 needed update capability based on their role assignments. When CAMS was implemented in 2006, specific roles were identified by the Department as needing update capability and other roles were determined to need view-only capability. However, Department staff further stated that they had not reviewed the appropriateness of the role assignments since the roles were initially established.

CSE staff utilized CAMS case reports to monitor the status of cases with overrides in place to identify overrides that could be removed, to track the number of cases with overrides, and to assess whether such overrides were consistent with Program Office policy. However, the monitoring activities did not include a determination of whether users who should only be viewing overrides had performed any override transactions. Without adequate controls to ensure that only authorized and appropriate users are performing override transactions, the risk is increased that unauthorized overrides of enforcement activities could occur.

Recommendation: The Department should enhance CAMS functionality to provide the capability to assign view-only access privileges for the enforcement override screens. Upon implementation of the enhancements, the Department should restrict the ability to perform enforcement override transactions to authorized and appropriate users. Until such functionality can be established in CAMS, the Department should closely monitor the system activities of users with access to the override screens to ensure that only authorized users are performing override transactions.

Finding No. 9: Ongoing Address Issues

IT controls are intended to promote the integrity of data stored within an information system and exchanged between systems. CAMS utilized mailing software that corrected and standardized address components to increase mailing efficiency and cost effectiveness. Additionally, the mailing software functioned to maintain a consistent address format within the system and apply the format to data received from various external sources and the FLORIDA System CSE Component. The mailing software was also used to facilitate communication between CAMS and the FLORIDA System CSE Component by parsing (separating) the address information into discrete components, such as street, city, and postal code.

Address data was communicated between the FLORIDA System CSE Component and CAMS through conversion and transaction records. Conversion records originated in the FLORIDA System CSE Component and represented the address data known when a child support case was established. Transaction records or change records originated in CAMS and were transmitted to the FLORIDA System CSE Component. Transaction records included additions, updates, or inactivations to the original address data. Transaction records were derived from three sources:

- Manual entries made in CAMS as a result of a change of address after the case was loaded into CAMS. After a case was converted to CAMS, all member address changes were made in CAMS rather than in the FLORIDA System CSE Component.
- Change of address records entered into CAMS from external interfaces (e.g., updates provided by the Department of Highway Safety and Motor Vehicles).
- Change records submitted by the State Disbursement Unit (SDU)[1] through the FLORIDA System CSE Component.

The Department had made improvements in identifying and correcting certain address issues noted in our report No. 2008-020. However, in response to audit inquiry, Department staff acknowledged that other address issues noted in the prior audit had not been resolved. Specifically:

- The Department's use of the mailing software to correct and standardize address data loaded into the two systems could result in address mismatches between the two systems in some instances. Additionally, in some instances, correct addresses stored in CAMS could be replaced by undeliverable or incorrect address information.
- Transaction records were not always communicated to the FLORIDA System CSE Component. When a communication failure existed on the mailing software server, transaction records sent from CAMS did not update the FLORIDA System CSE Component. The communication failure was not automatically detected and reported. These communication outages created a delay in CSE activities because updates to addresses were delayed in being recorded in the FLORIDA System CSE Component. In response to audit inquiry, Department staff indicated that the communication error was corrected in October 2009.

[1] Pursuant to Section 61.1826(1), Florida Statutes, the Department contracted with the Florida Association of Court Clerks to establish and operate an SDU for the collection and disbursement of child support payments.

- Address change records from the SDU could result in nonstandard data being communicated and stored in both systems in some instances. Additionally, for residential addresses that the SDU reported as no longer active, no mechanism existed to provide an end date for the inactive residential addresses in the FLORIDA System CSE Component.
- External interface sources could replace some correct address information with undeliverable or invalid address information.

Incorrect address information increases the risk that child support payments will not be delivered to the custodial parents in a timely manner. It also increases the risk that notices of noncompliance, as well as notices of enforcement actions, will not reach noncustodial parents.

Recommendation: The Department should continue its efforts to identify and correct address issues with the CAMS application in order to promote the integrity of the data in CAMS and the FLORIDA System CSE Component and the effective and efficient operation of the CSE program.

Finding No. 10: Caseworker Task Monitoring Procedures

Procedures for monitoring the results of system processing help ensure that data is processed through the system completely and accurately. During data processing, transactions may not be processed completely or accurately as a result of errors or inconsistencies in data, system interruptions, communication failures, or other events. A monitoring capability helps ensure that these instances are identified and processing continues.

Although compliance and enforcement activities were automated in CAMS, caseworker tasks such as update depository number or perform manual locate were generated when manual intervention was required to continue processing. CAMS assigned the caseworker tasks to workgroups. Caseworkers could view all unprocessed tasks assigned to their workgroup upon logging in to CAMS. CAMS Task and Activity Statistics reports were available for the CSE supervisors to monitor unprocessed CAMS tasks. Although the Department had an informal process in place for the monitoring of tasks in CAMS using these reports, the Department did not have written procedures for supervisor monitoring and follow-up of unprocessed tasks to ensure that tasks were completed in a timely manner. Without written procedures for the monitoring of outstanding CAMS tasks, the risk is increased that tasks will not be completed or followed up on, resulting in enforcement activities not being performed in a timely manner pursuant to management's expectations.

Recommendation: The Department should document the procedures for monitoring tasks in CAMS to ensure that unprocessed tasks are completed in a timely manner consistent with management's expectations.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings applicable to the scope of this audit included in our report No. 2008-020.

OBJECTIVES, SCOPE, AND METHODOLOGY

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

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

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to the FLORIDA System CSE Component and CAMS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine the extent to which the Department corrected, or were in the process of correcting, deficiencies disclosed in our report No. 2008-020 that are applicable to the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System CSE Component and CAMS during the period July 1, 2008, through June 30, 2009, and selected actions through December 15, 2009.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the CSE program including the purpose, goals, and compliance requirements; basic data and business processing flows; IT organizational structure and management; and the interaction of the FLORIDA System CSE Component and CAMS.
- Obtained an understanding of the FLORIDA System CSE Component and CAMS including the computing platforms and related software.
- Obtained an understanding of the logical access controls for the FLORIDA System CSE Component and CAMS including user account administration for each system.
- Obtained an understanding of the CAMS application controls, including input, processing, output, and user controls.
- Observed and evaluated key processes and procedures related to the Department's risk assessments.
- Observed, tested, and evaluated key processes and procedures related to the security controls for the FLORIDA System CSE Component and CAMS, including user account administration procedures, access authorization, appropriateness of user access, timely removal of access privileges, and periodic review of user access privileges.
- Observed, tested, and evaluated key processes and procedures related to Department network and barrier controls, including password controls, network account administration, and vulnerability assessments.
- Observed, tested, and evaluated key processes and procedures related to the CAMS input, processing, and user controls, exception reporting, and follow-up procedures as they related to the enforcement of financial and medical support orders.
- Observed and evaluated key processes and procedures related to locate and address verification processing, including the synchronization of data between CAMS and the FLORIDA System CSE Component.

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 4, 2010, the Executive Director 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

FLORIDA
DEPARTMENT OF REVENUE

Executive Director
Lisa Echeverri

Child Support Enforcement
Ann Coffin
Director

General Tax Administration
Jim Evers
Director

Property Tax Oversight
James McAdams
Director

Information Services
Tony Powell
Director

March 4, 2010

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

Dear Mr. Martin:

As required by section 11.45(4)(d), Florida Statutes, attached is the Department's response to the preliminary and tentative findings and recommendations of your Information Technology Audit of the Department of Revenue Florida Online Recipient Integrated Data Access (FLORIDA) System, Child Support Enforcement (CSE) Component and Child Support Enforcement Automated Management System (CAMS), for the period July 1, 2008, through June 30, 2009, and selected actions through December 15, 2009.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Teresa Wood, Director of Auditing, at 487-0701.

Sincerely,

Lisa Echeverri

LE/lh

Attachment

cc: Sharon Doredant
Teresa Wood

Tallahassee,
Florida
32399-0100
www.myflorida.com/dor

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response to Preliminary and Tentative Audit Findings
Child Support Enforcement, FLORIDA and CAMS
Information Technology Audit
For the Period July 2008 through June 2009

Finding No. 1: Documentation of authorization for FLORIDA System CSE Component and CAMS access privileges for some users was missing, incomplete, or inaccurate.

Recommendation: The Department should ensure that access authorization forms for the FLORIDA System CSE Component and CAMS are appropriately completed and maintained.

Response: We concur. The Department will be providing training to staff regarding the accurate completion and retention of FLORIDA security user access request forms. We will review Department files to ensure there is documentation that authorizes security access for each active CAMS and FLORIDA user by June 2010.

Finding No. 2: The access privileges of some FLORIDA System CSE Component and CAMS users were not appropriate for their job responsibilities.

Recommendation: The Department should limit access privileges to the FLORIDA System CSE Component and CAMS resources to only what is needed to perform job responsibilities. Additionally, update access privileges assigned to system staff for production CAMS should be monitored as required by the Department's acceptance of risk forms.

Response: The Department agrees.

Update capability is provided to security roles when the system does not allow for a view-only version (example: Enforcement Override). In addition, role-based security design uses a risk-based approach which allows security roles to be assigned to groups of users instead of being user-specific. This approach better allows security roles to be assessed for both conflicts of duties and least privilege. A security role may provide users with more capability than required to do their normal job, but should not include any conflicts of duties. While it is the Department's intent to reduce the number of security roles, we intend to review all CAMS Phase I role assignments as part of the development of the CAMS II roles definition which will be implemented in February 2012 to assure the appropriateness of access privileges.

The Department will also implement an annual review of system staff with FLORIDA and CAMS access to ensure current profiles are appropriate to job duties. The Department will monitor update access privileges assigned to system staff on a quarterly basis. Anticipated implementation of DOR FLORIDA and CAMS Security procedures and first annual review is December 2010.

1

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: Some access privileges in the FLORIDA System CSE Component and CAMS did not enforce an appropriate separation of incompatible duties.

Recommendation: The Department should enhance the effectiveness of FLORIDA System CSE Component access controls to ensure that contractors do not possess access privileges reserved for Department staff. Additionally, the Department should ensure that CAMS systems staff are not assigned access privileges that allow them to perform incompatible functions. The Department should also ensure that users with access privileges to both systems cannot create or assign payments and also update custodial family addresses in CAMS. Additionally, the Department should ensure that the FLORIDA System CSE Component documentation is updated to accurately reflect which access profiles are incompatible with the ability in CAMS to update addresses.

Response: We concur. The Department reviewed access privileges of FLORIDA users that have the ability to create or assign payments, then made CAMS or FLORIDA role changes for those who were found to have segregation of duties issues. CAMS and FLORIDA security administrators now have a documented process in place to verify access privileges between the two systems so we can avoid conflicts for future user access requests. When the Phase II of CAMS is implemented, the potential for this problem will not exist since all functionality will be in CAMS.

We will implement a process to allow for "firefighter/super user" access for temporary use. This process will allow us to remove normally excessive access privileges from a user, but allow a user who has been previously authorized to log on to a firefighter/super user role to perform a specific task then log out. All activity while using this special access will be documented and is available for review. This will be implemented with Phase II of CAMS, scheduled for statewide implementation in February 2012.

Finding No. 4: The Department did not timely remove FLORIDA System CSE Component and CAMS access privileges of some former employees and contractors.

Recommendation: The Department should ensure that the access privileges of former employees and contractors are removed in a timely manner in order to minimize the risk of compromising CSE program data and IT resources.

Response: We concur. The Department has made significant improvement in this area by automating the employee separation notification process. This new process was implemented in April 2009. Using the on-line separation process automatically deactivates system access for separated employees. Monthly reviews of personnel actions are done to catch unreported separations. Department program directors receive reports of any untimely employee separation notifications and work with supervisors to ensure timely use of the on-line separation process. Because 100% compliance depends on each supervisor initiating separation notifications timely, we will focus on supervisor awareness through supervisor training and regular Child Support Program communications.

Building on the same solution for employees leaving the agency we are now looking to improve the timeliness of security access changes for internal employee reassignments

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

and for contractors by expanding the automated notification and system access deactivation process to include these types of changes as well. This should be completed by June 2010.

Finding No. 5: The Department did not periodically review the appropriateness of CAMS user access privileges.

Recommendation: The Department should establish written policies and procedures for the periodic review of CAMS access privileges by system owners.

Response: We concur. The Department will develop a process to allow managers and security role owners to review the access privileges of their staff so that managers can periodically look up and verify the access privileges for their staff. We will accomplish this by implementing a transaction similar to one developed in SUNTAX that allows managers to review the security roles and last login date for their staff. We will also create procedures to require managers to do this review annually. The target date for completion is September 2010.

Finding No. 6: The Department could not provide documentation of its evaluation of network vulnerability scans or subsequent actions to mitigate vulnerabilities. Similar issues regarding CAMS were disclosed in connection with our report No. 2008-020.

Recommendation: The Department should continue its efforts to implement a process for documenting the results of vulnerability scanning evaluation and mitigation.

Response: We concur. The Information Services Program uses the Nessus scanning software to scan each department server at least once a quarter. The reports from the Nessus scan are organized into High, Medium and Low vulnerabilities and are provided to the Infrastructure team. We will implement a response process and devote resources to mitigate the high and medium vulnerabilities as soon as possible, but no later than June 2010.

Finding No. 7: Security Controls – User Authentication

Recommendation: The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of data and IT resources.

Response: We concur. A compensating control is currently in place to mitigate one issue identified. Additionally, the Department is researching options to improve the security involving the identified issues. Identified solutions will be implemented in the CAMS environment at Phase II statewide implementation scheduled for February 2012.

Finding 8: Because of limitations in CAMS access control functionality, many CAMS users inappropriately had the ability to perform enforcement override transactions on

3

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

cases. Additionally, the Department did not monitor enforcement override transactions to ensure that such users had not performed unauthorized overrides.

Recommendation: The Department should enhance CAMS functionality to provide the capability to assign view-only access privileges for the enforcement override screens. Upon implementation of the enhancements, the Department should restrict the ability to perform enforcement override transactions to authorized and appropriate users. Until such functionality can be established in CAMS, the Department should closely monitor the system activities of users with access to the override screens to ensure that only authorized users are performing override transactions.

Response: We concur. The Department will implement view-only access for the enforcement override screens. This will be implemented with Phase II of CAMS, scheduled for statewide implementation in February 2012.

Until the view-only access is available, the Department believes that the risk of unauthorized override entry or update is mitigated through the current procedure to conduct monitoring of enforcement overrides. Current procedures direct local offices to review a CAMS report to ensure appropriate entry of overrides. The Department will clarify the procedures to indicate the frequency of the reviews is quarterly. The target date for completion is November 2010.

Finding 9: The Department had not resolved some issues with address information in CAMS that were previously noted in our report No. 2008-020.

Recommendation: The Department should continue its efforts to identify and correct address issues with the CAMS application in order to promote the integrity of the data in CAMS and the FLORIDA System CSE Component and the effective and efficient operation of the CSE program.

Response: We concur. The Department will continue to make improvements and corrections on the issues identified. However, the majority of issues cannot be resolved at the current time due to the inability to make modifications to the CAMS system during the design, development and testing phase for Phase II of CAMS. Specifically the Child Support Program will correct the following deficiencies:

1) Stop loading non-standardized addresses which error during address standardization using the PostalSoft application. Currently, CSE loads any non-standardized address not recognized by the PostalSoft application for addresses received from all external interfaces and manual user entry. We anticipate completion and correction of this deficiency in 2012.

2) The problem caused by the address parsing between the PostalSoft application and CAMS and FLORIDA will be resolved with implementation of Phase II of CAMS. There will be no need to reconcile addresses between two systems because all address updates with be made in the CAMS CRM application. We have no way of correcting this issue now, other than not using the PostalSoft application for address standardization.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

3) The new design for Phase II of CAMS will correct the deficiency with verification of residential addresses. The will allow for residential addresses to be verified through postal verification letters.

4) The Child Support Program has included correction of the source and load date issue related to inbound addresses from external interfaces in the design for Phase II of CAMS. The changes will reduce the occurrence of the system updating a current address with an older or invalid address from an external interface file. The system must be modified to create a new 'load date' and re-programming of all external interface files is necessary. We anticipate completion and correction of this deficiency in 2012.

5) The Child Support Program is taking measures now to reduce the potential for redundant data loaded from the Federal Case Registry in-bound interfaces. We have requested the federal office of Child Support Enforcement to stop sending address information previously received. This should reduce the potential for loading address information previously received with a new more recent effective date (load date).

Finding No. 10: The Department did not have written procedures for supervisor monitoring and follow-up of unprocessed CAMS tasks.

Recommendation: The Department should document the procedures for monitoring tasks in CAMS to ensure that unprocessed tasks are completed in a timely manner consistent with management's expectations.

Response: We concur. The Child Support Program will develop written procedures requiring monitoring of CAMS tasks on a bi-weekly or monthly basis depending on the priority of the task. The target date for completion is November 2010.

5