REPORT NO. 2012-002
JULY 2011

# 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

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 Vickers served as Executive Director during the audit period.

The audit team leader was Wayne Revell, 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 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. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2010-130. As detailed throughout this report, the Department had not taken corrective actions for most of the prior audit findings included in our report No. 2010-130. Some of these findings were also noted in other prior audits of the Department.**

**The results of our audit are summarized below:**

**GENERAL CONTROLS**

**Finding No. 1: Authorization documentation for FLORIDA System CSE Component and CAMS access privileges for some users was missing, incomplete, or inaccurate.**

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

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

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

**Finding No. 5: The Department's review of the appropriateness of CAMS user access privileges was not conducted on a sufficiently frequent basis.**

**Finding No. 6: The Department did not document its evaluation of network vulnerability scans or subsequent actions to mitigate vulnerabilities.**

**Finding No. 7: Certain Department security controls related to user authentication needed improvement.**

**Finding No. 8: The Department's CAMS Disaster Recovery Plan was not complete and up to date and had not been thoroughly tested.**

APPLICATION CONTROLS

**Finding No. 9: 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. 10: The Department had not resolved some issues with address information in CAMS.**

**Finding No. 11: Although the Department had an informal process in place, the Department did not have written procedures for supervisor monitoring and follow-up of unprocessed CAMS tasks. Furthermore, the Department did not maintain a record of the tasks reviewed or the related decisions made during the monitoring process.**

ADDITIONAL MATTERS

**Finding No. 12: The Department's service-level agreement with Northwest Regional Data Center (NWRDC) lacked certain provisions required in State law.**

**Finding No. 13: Contrary to State law and rules, the Department did not timely notify the Agency for Enterprise Information Technology, Office of Information Security (AEIT) of an interruption in CAMS processing.**

## BACKGROUND

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 Department's CSE Program Office administers the CSE Program in five regions throughout the State. The CSE 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.

Most CSE Program services are provided through the CSE Program Office. However, CSE Program services in Miami-Dade County are provided by the Office of the State Attorney under a contractual agreement with the Department. In addition, CSE Program services in Manatee County are provided by the Clerk of the Circuit Court & Comptroller under a contractual agreement with the Department. CSE Program services provided under these contracts must meet the same Federal and State requirements as those provided by the Department.

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. On August 1, 2010, the Department moved CAMS operations to NWRDC as part of the State primary data center full-service transition.

## FINDINGS AND RECOMMENDATIONS

### General 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 region and headquarters security officers. Region security officers manage the FLORIDA System access privileges of staff 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. 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*. Similar issues were noted in our report No. 2010-130.

For a sample of 33 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 3 of the 33 user accounts included in our sample, Department staff could not provide the authorization forms.

For the remaining 30 user accounts in our sample, we inspected the authorization forms that Department staff provided to us. For 1 of the 30 user accounts, the authorization form was missing required information. Specifically, the form lacked the security profiles that were authorized for the user account.

**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. Access requests for systems staff are documented on a CAMS *User Request Form for Production Systems*. As similarly noted in prior audits of the Department, most recently our report No. 2010-130, the Department had not appropriately documented authorizations of user access privileges granted to some employees and contractors.

For a sample of 36 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 2 of the 36 end users and systems staff users included in our sample, Department staff could not provide the authorization forms.

For the remaining 34 end users and systems staff users in our sample, we inspected the authorization forms that Department staff provided to us. For 5 of the 34 users, the authorization forms were missing required information. Specifically, the forms lacked the appropriate security roles. 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. Specifically:

- The FLORIDA System CSE Component update access privileges for 3 of 32 users included in our sample were not necessary for their job responsibilities. A similar issue was noted in our report No. 2010-130.
- The CAMS update access privileges for 10 of 15 end-users included in our sample were not necessary for their job responsibilities. Similar issues were noted in prior audits of the Department, most recently our report No. 2010-130.
- The CAMS update access privileges for 19 of 21 IT staff included in our sample were not necessary for their job responsibilities. Similar issues were noted in prior audits of the Department, most recently our report No. 2010-130.
- Of the 19 IT staff with inappropriate access to CAMS, 6 had inappropriate system-level update access to CAMS, 11 had inappropriate end-user access privileges to CAMS, and 2 had both inappropriate system-level access and end–user access to CAMS. According to Department staff, the IT staff with end-user access privileges to CAMS had been granted the access for production troubleshooting and problem resolution that allowed the IT staff to make updates to production data in CAMS. Department staff acknowledged that the job responsibilities of the 13 IT staff did not require the ability to make data changes in production. However, the 13 IT staff had been given the end-user update privileges because 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 13 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 March 1, 2011, the Department had not developed access monitoring reports for this purpose. A similar issue was noted in prior audits of the Department, most recently our report No. 2010-130.

**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 IT staff for 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 CAMS and within the FLORIDA System CSE Component and CAMS 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. Similar issues were noted in prior audits of the Department, most recently our report No. 2010-130.

Two of the 21 IT staff included in our sample and previously discussed in Finding No. 2 (Bullet 3) who had access privileges not necessary for their job responsibilities had both a system administrator role and an end user role that allowed update access to all transactions in the CAMS production environment. This combination of roles was contrary to an appropriate separation of duties.

Within the FLORIDA System CSE Component, specific finance screens allow the user to create or assign payments. Our audit disclosed that one user, 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 68 users who had access privileges in either the CSE Component or CAMS. From our sample, we determined that 46 of the 68 users had access privileges in both systems. Of the 46 users who had been granted update access privileges to the CSE Component finance screens used to create or assign payments, 1 also had the capability in CAMS to change custodial family addresses.

**Recommendation: The Department should ensure that CAMS IT staff are not assigned access privileges that allow them to perform incompatible functions. The Department should also ensure that end users with access privileges to both the CSE Component and CAMS cannot create or assign payments and also update custodial family 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 lists of: (1) all 130 Department employees who terminated employment during the period July 1, 2010, through November 30, 2010; (2) the 43 contractors who terminated contractual services during the same period; and (3) the 30 employees of the Miami-Dade Office of the State Attorney

and the Manatee County Clerk of the Circuit Court & Comptroller who terminated employment during that same period. 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 FLORIDA System CSE Component and CAMS access privileges were noted in our report No. 2010-130. Similar issues regarding CAMS access privileges were also noted in our report No. 2008-020. Specifically:

- The FLORIDA System CSE Component access privileges of 3 former employees and 2 former contractors were disabled as of the dates of our test but had remained active for periods ranging from 2 to 12 days after termination.
- The FLORIDA System CSE Component access privileges of 7 former employees of the Miami-Dade Office of the State Attorney were disabled as of the dates of our test but had remained active for periods ranging from 2 to 14 days after termination.
- The CAMS access privileges of 10 former employees were shown as active in a Department access listing dated December 21, 2010, 24 to 174 days after the termination dates of the employees.
- The CAMS access privileges of an additional 11 former employees and 1 former contractor were disabled as of December 21, 2010, but had remained active from 3 to 119 days after the dates the employees and contractor terminated.
- The CAMS access privileges of 6 former employees of the Miami-Dade Office of the State Attorney and the Manatee County Clerk of the Circuit Court & Comptroller were shown as active in a Department access listing dated December 21, 2010, 39 to 92 days after the termination dates of the employees.
- The CAMS access privileges of an additional 12 former employees of the Miami-Dade Office of the State Attorney and the Manatee County Clerk of the Circuit Court & Comptroller were disabled as of December 21, 2010 but had remained active from 2 to 20 days after the dates the employees terminated.

In response to audit inquiry, Department staff provided documentation substantiating that the access privileges of all but one of the former Department employees, contractors, Miami-Dade Office of the State Attorney employees, and Manatee County Clerk of the Circuit Court & Comptroller employees had not been used to access the system after termination. For the remaining former Department employee, Department staff could not determine whether the access privileges had been used after termination.

Additionally, our examination of documentation of user access authorizations for the FLORIDA System CSE Component users previously discussed in Finding No. 1 disclosed that access privileges still existed for one contractor who had been terminated on December 29, 2006. This access was assigned inadvertently on March 9, 2007, which was after her termination. The access privileges remained active for 3 years, 10 months, and 19 days after the access was established; however, the access privileges were never used. In response to audit inquiry, Department security administration staff disabled the user identification code on January 28, 2011.

**Recommendation: The Department should ensure that the access privileges of former Department and other entity 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. AEIT Rule 71A-1.007, Florida Administrative Code, provides that agency information owners shall review access rights periodically based on risk, access account change activity, and error rate.

According to CAMS security administration staff, Departmental system owners were responsible for ensuring that the access granted to users was appropriate for their system. An initial review of all system users' access (for FLORIDA and CAMS) by supervisors and role owners was completed in September 2010. Furthermore, Department management indicated that they were in the process of implementing an annual review of CAMS access privileges. This user access review will be completed annually by the user's supervisor during the employees' annual performance reviews.

The importance of CAMS to the CSE Program, the presence of confidential and sensitive information therein, and the existence of excessive or unnecessary CAMS access privileges as described in Finding Nos. 2 through 4 indicate the need for the Department to review CAMS access privileges more frequently than annually. Similar issues regarding the review of CAMS access privileges were noted in our report No. 2010-130.

**Recommendation: The Department should reassess the frequency by which CAMS access privileges are reviewed and consider a more frequent review.**

## 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.

Department staff indicated that technical staff were scanning servers for vulnerabilities at least quarterly. The Department had developed, but had not implemented, procedures for documenting the results of scanning evaluation and mitigation activities. Additionally, Department staff indicated that these procedures did not include the primary data center (PDC) locations and that additional procedures were being developed to address scanning evaluation and mitigation activities for servers located at those locations. Similar issues were disclosed in prior audits of the Department, most recently our report No. 2010-130.

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. Our audit disclosed certain Department security controls related to user authentication that needed improvement. Similar issues related to user authentication were disclosed in prior audits of the Department, most recently our report No. 2010-130. 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 related to user authentication, 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.**

### Finding No. 8: CAMS Disaster Recovery Plan

A complete, cost-effective, and tested IT disaster recovery plan helps provide for the prompt and effective continuation of State services. Establishing a disaster recovery plan that is communicated to affected staff; identifies critical personnel, including their contact information; and provides an accurate timeline for recovery in the event of a disaster is critical to the continuity of governmental operations. AEIT Rule 71A-1.012(5), Florida Administrative Code, provides that IT disaster recovery plans shall be tested at least annually.

Although the Department had developed a disaster recovery plan for CAMS, Department management indicated that the CAMS disaster recovery plan had not been fully tested since April 2009. In response to audit inquiry, Department management indicated that the scheduled disaster recovery test for 2010 was postponed because the Department had contracted during the year with a new vendor for data storage and recovery services for CAMS. In February 2011, the Department conducted a limited disaster recovery test that included an assessment of the validity and accessibility of recovered CAMS production data as well as other functionality and recovery processes. However, the test did not include a validation of the interfaces between CAMS and other external systems and did not test batch jobs.

The most current version of the disaster recovery plan was required to be retained in the CAMS documents repository. However, upon audit request, Department management responsible for certain aspects of the CAMS disaster recovery tasks provided us with outdated versions of the plan instead of the most current version. In addition, the plan did not include a list of the personnel who should be notified in the event of an emergency or other critical event. The CAMS disaster recovery plan included a timeline for expectations for various steps within the recovery process and for the overall system and data recovery after a system interruption or failure. However, this timeline had not been updated to reflect current disaster recovery expectations. Without a complete, up-to-date, and thoroughly tested disaster recovery plan, the risk is increased that the Department may not be able to recover in a timely manner from a major disruption to its IT services.

**Recommendation: The Department should ensure that its disaster recovery plan is complete and up to date. In addition, the Department should, at least annually, conduct a comprehensive test of the plan including all critical Department IT resources.**

## Application Controls

### Finding No. 9: 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.

As also noted in our report No. 2010-130, 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 February 18, 2011, 704 users had access to enforcement override screens. In response to audit inquiry, Department management stated that, of the 704 users, 369 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 management further stated that they had not reviewed the appropriateness of the role assignments since the roles were initially established.

CSE management utilized CAMS case reports to monitor the status of cases with overrides in place to identify overrides that could be removed, track the number of cases with overrides, and assess whether such overrides were consistent with Program Office policy. The Department also implemented a policy on October 12, 2010, requiring CSE Region staff to perform a quarterly review of targeted cases with overrides to ensure that 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 monitor the system activities of users with access to the override screens to ensure that only authorized users are performing override transactions.**

## Finding No. 10: 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 transmitted between the FLORIDA System CSE Component and CAMS through an interface process. The interface process transmitted data between the two systems based on the transaction records of the case and case member data. When a new case was created in the FLORIDA System, the interface process converted the case and case member data to CAMS. Once the case member data was converted to CAMS, any further updates to the case member demographic data had to be completed in CAMS. If new case member data was received, or existing data was updated by a user or external interface in CAMS, the new or updated data was transmitted to the

FLORIDA System CSE Component. Transaction records could include new or changed addresses that would inactivate the existing address and insert a new address. Case member address information was derived from three sources:

- Manual entries made in CAMS as a result of a change of address after the case was loaded into CAMS.
- 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 one address issue noted in prior audits of the Department, most recently our report No. 2010-130. However, in response to audit inquiry, Department management acknowledged that other address issues noted in our prior audits 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.
- 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 automated 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 within CAMS 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. 11: 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 statistics reports were available for the CSE Program 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

[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.

supervisor monitoring and follow-up of unprocessed tasks to ensure that tasks were completed in a timely manner. A similar issue was noted in our report No. 2010-130. Furthermore, the Department did not maintain a record of the tasks reviewed or the related decisions made during the monitoring process. In response to audit inquiry, Department management provided draft procedures that had been developed, but not approved, for implementation. Without approved 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 provide staff with approved procedures for monitoring tasks in CAMS to ensure that unprocessed tasks are completed in a timely manner consistent with management's expectations.**

## Additional Matters

### Finding No. 12: Service-Level Agreement

A service-level agreement is a negotiated agreement between two parties where one is the customer and the other is the service provider. Service-level agreements are necessary to define IT services provided by service providers to State agencies and other governmental entities and to ensure that services provided by the service providers support the business objectives of the customer entities. Service-level agreements define the roles and responsibilities of each party, service renewal provisions, and termination requirements. Service-level agreements also set forth the billing methodology and the costs of the services to be paid by the customer entities.

Section 282.203(1)(i), Florida Statutes, provides that each primary data center shall enter into a service-level agreement with each customer entity to provide services as defined and approved by the data center Board of Trustees in compliance with AEIT rules. As previously discussed in the Background section of this report, NWRDC provides support services for the Department's CAMS operations.

Although the Department executed a service-level agreement with NWRDC, the service-level agreement did not include some of the minimum-required provisions set forth in Section 282.203(1)(i), Florida Statutes. The absence of such provisions increases the risk that the expectations of either party may not be met. Specifically, the executed agreement did not:

- Identify the legal authority under which the service-level agreement was negotiated and entered into by the parties.
- Identify applicable funds and funding streams for the services or products under contract.
- Provide that the agreement may be terminated by either party for cause only after giving the other party and AEIT notice in writing of the cause for termination of the service-level agreement and an opportunity for the other party to resolve the identified cause within a reasonable period.
- Provide for mediation of disputes by the Division of Administrative Hearings pursuant to Section 120.573, Florida Statutes.

**Recommendation: The Department should work with NWRDC to ensure that its service-level agreements include all provisions required by State law.**

**Finding No. 13: Reporting of Security Incidents**

Section 282.318(4)(i), Florida Statutes, provides that each agency head shall develop a process for detecting, reporting, and responding to security incidents and that suspected or confirmed information security incidents or breaches must be immediately reported to AEIT. AEIT Rule 71A-1.014(7), Florida Administrative Code, requires agencies to notify AEIT of computer security incidents within 24 hours of discovery.

Section 282.318(3)(b)2., Florida Statutes, requires AEIT to develop enterprise security rules and published guidelines for, among other things, responding to information security incidents. AEIT promulgated *Computer Security Incident Response Team (CSIRT) Agency Guidelines* effective July 2010. The *CSIRT Agency Guidelines* define a computer security incident as any action or activity (accidental or deliberate) that compromises the confidentiality, integrity, or availability of the State's data and IT resources.

CAMS processing was interrupted on August 28, 2010, and restored on September 3, 2010. Contrary to State law and AEIT rules, the Department did not notify AEIT of the CAMS processing interruption until September 27, 2010, 30 days after the interruption.

In response to audit inquiry, Department management indicated that internal CSIRT procedures had not been updated to reflect current AEIT requirements. The lack of timely Department notification to AEIT regarding security incidents may limit the effectiveness of AEIT in monitoring and evaluating threats to State IT resources.

**Recommendation: The Department should update its internal CSIRT procedures to ensure that AEIT is timely notified of future security incidents, should they occur.**

## PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for a few of the issues included in our report No. 2010-130. However, corrective actions were not taken for most of the prior audit findings as described in the findings above.

## 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 from November 2010 through March 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 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. 2010-130.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System CSE Component and CAMS. The audit included selected general IT controls over logical access to programs and data, network vulnerability and monitoring, business continuity, and IT disaster recovery. The audit also included selected application IT controls and selected user controls relevant to CAMS. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from July 2010 through March 2011.

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 and user controls.
- Observed 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.
- Evaluated on a sample basis the effectiveness of procedures for authorizing user access privileges to the FLORIDA System CSE Component and the appropriateness of the access privileges granted. Specifically, we sampled 33 user accounts of 32 users to determine whether the access was authorized in writing and the profiles and security levels granted were appropriate.
- Evaluated on a sample basis the effectiveness of procedures for authorizing user access privileges to CAMS and the appropriateness of the access privileges granted. Specifically, we sampled 36 user accounts to determine whether the access was authorized in writing and the roles and security levels granted were appropriate.
- Tested the effectiveness of the procedures for disabling the FLORIDA System CSE Component and CAMS access privileges of former employees and contractors. Specifically, we tested 130 former Department employees, 43 former contractors, and 30 former employees of the Miami-Dade Office of the State Attorney and Manatee County Clerk of the Circuit Court & Comptroller who terminated employment or contractual services between July 1, 2010, and November 30, 2010.
- Observed and evaluated key processes and procedures related to Department network and barrier controls, including password controls, network account administration, and vulnerability assessments.
- Tested the effectiveness of CAMS password settings to evaluate the effectiveness of the settings in adequately protecting resources.
- Observed and evaluated key processes and procedures related to CAMS exception reporting and follow-up.
- Tested CAMS exception reporting and follow-up procedures.
- 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.
- Observed and evaluated key processes and procedures related to the disaster recovery plan for CAMS.
- Observed and evaluated the service-level agreement between the Department and NWRDC for the support of CAMS operations.
- 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

## MANAGEMENT'S RESPONSE

In a letter dated July 6, 2011, 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 Vickers

**Child Support Enforcement**
Ann Coffin
Director

**General Tax Administration**
Jim Evers
Director

**Property Tax Oversight**
James McAdams
Director

**Information Services**
Tony Powell
Director

July 6, 2011

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).

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Teresa Wood, Director of Auditing, at 717-7598.

Sincerely,

Lisa Vickers

LV/tw

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

**Finding No. 1:** Authorization documentation 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 continue to periodically remind security officers and administrators for FLORIDA and CAMS of the requirements for accurate completion and retention of access request forms.

**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 IT staff for CAMS should be monitored as required by the Department's acceptance of risk forms.

***Response:*** We concur. As mentioned in response to finding 5, access privileges will continue to be reviewed annually by the user's supervisor during the employee's annual performance review, and at the time an employee's job duties are changed. The review will ensure the access privileges are in sync with employee job responsibilities. Additionally, the Department will research what is required to provide the capability to monitor IT staff with system update access privileges in CAMS production.

**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 ensure that CAMS IT staff are not assigned access privileges that allow them to perform incompatible functions. The Department should also ensure that end users with access privileges to both the CSE Component and CAMS cannot create or assign payments and also update custodial family addresses.

***Response:*** We concur. The security officers and administrators for FLORIDA and CAMS verify that there is no separation of duty conflict for selected profiles when granting access to FLORIDA and CAMS. The FLORIDA forms used to approve access privileges were revised and require a signature confirming that the review was completed. CAMS Security staff will start annotating on the CAMS access form when the review is completed.

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

**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 Department and other entity 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 CSE contract managers are entering all contracted staff into the Department's electronic termination notification process. The entry should be completed by September 2011. A monthly termination monitoring process is in place to verify privileges for terminated state employees are properly removed. A weekly review of state employee terminations has also been implemented so that access removal is more timely.

**Finding No. 5:** The Department's review of the appropriateness of CAMS user access privileges was not conducted on a sufficiently frequent basis.

***Recommendation:*** The Department should reassess the frequency by which CAMS access privileges are reviewed and consider a more frequent review.

***Response:*** We partially concur. The Department agrees that access privileges must be reviewed periodically. Access privileges will continue to be reviewed annually by the user's supervisor during the employee's annual performance review and at the time an employee's job duties are changed.

**Finding No. 6**: The Department did not document its evaluation of network vulnerability scans or subsequent actions to mitigate vulnerabilities.

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

***Response:*** The Information Security Management (ISM) office has a deployed and documented vulnerability scanning and remediation process. The process was in use by April 2011 which includes tracking planned actions to be taken to mitigate vulnerabilities. The procedural document was completed on June 16, 2011. A verification process will be implemented and documented to ensure the planned mitigations were completed.

**Finding No. 7:** Certain Department security controls related to user authentication needed improvement.

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

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

***Response:*** We concur. The deployment of CAMS Phase II scheduled for February, 2012, will offer improved security controls for user authentication.

**Finding 8:** The Department's CAMS Disaster Recovery Plan was not complete and up to date and had not been thoroughly tested.

***Recommendation:*** The Department should ensure that its disaster recovery plan is complete and up to date. In addition, the Department should, at least annually, conduct a comprehensive test of the plan including all critical Department IT resources.

***Response:*** We concur. The Department is scheduled to update the CAMS Disaster Recovery Plan during August – September 2011. The plan will be updated to reflect a requirement for an annual test each calendar year. The next annual test will include CAMS II, batch processing, data changes, and selected interfaces.

**Finding 9:** 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.

***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 initiate a system enhancement to provide the capability to assign view-only access privileges after Phase II of CAMS is implemented. In the interim, the Department believes the risk of unauthorized override entry or update is mitigated through the current procedure which directs local offices to review a CAMS report to ensure appropriate entry of overrides. The Department revised the procedures in December 2010 to indicate the frequency of the review is quarterly.

**Finding 10:** The Department had not resolved some issues with address information in CAMS.

***Recommendation:*** The Department should continue its efforts to identify and correct address issues within CAMS 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.

**EXHIBIT A (CONTINUED)**
**MANAGEMENT'S RESPONSE**

***Response:*** We concur. The Department is continuing to make improvements and corrections on the issues identified. The majority of issues will be resolved upon implementation of CAMS Phase II, scheduled for February 2012.

**Finding No. 11:** Although the Department had an informal process in place, the Department did not have written procedures for supervisor monitoring and follow-up of unprocessed CAMS tasks. Furthermore, the Department did not maintain a record of the tasks reviewed or the related decisions made during the monitoring process.

***Recommendation:*** The Department should provide staff with approved 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. Procedures addressing the frequency of review and the use of the Business Intelligence report by region management in monitoring tasks for their service sites were approved and signed by the director on March 25, 2011. These procedures were posted to the CSE Policy and Procedure intranet site on April 6, 2011.

**Finding No. 12**: The Department's service-level agreement with Northwest Regional Data Center (NWRDC) lacked certain provisions required in State law.

***Recommendation:*** The Department should work with NWRDC to ensure that its service-level agreements include all provisions required by State law.

***Response:*** We concur. The Service Level Agreement (SLA) with NWRDC is scheduled to go through an annual review and renewal process. During this year's review, State laws will be researched to identify additional provisions that should be included in the SLA with NWRDC.

**Finding No. 13:** Contrary to State law and rules, the Department did not timely notify the Agency for Enterprise Information Technology, Office of Information Security (AEIT) of an interruption in CAMS processing.

***Recommendation:*** The Department should update its internal CSIRT procedures to ensure that AEIT is timely notified of future security incidents, should they occur.

***Response:*** We concur. Prior to August, 2010, state agencies, including Revenue, did not typically report loss of service caused by a system error or malfunction. After this incident, the AEIT Office of Information Security (AEIT/OIS) communicated to the agency Information Security Managers (ISMs) that an availability incident that is classified as a Class 2 or 3 incident as defined in the AEIT CSIRT procedures that exceeds the agency's Service Level Agreement (SLA) should be reported to AEIT/OIS within 24 hours, and that the agencies and the Primary Data Center(s) (PDC) should work together to develop a process to report these incidents to AEIT/OIS.

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

The Revenue ISM is working with SSRC, NWRDC and Department of Education ISMs to add language to each agency's CSIRT procedures that provides a process for PDC and the agency working together on the appropriate joint CSIRT activities and for developing and reporting either a joint report or separate reports to the AEIT/OIS that provide consistent information regarding the incident. This process will include providing an initial report of the incident, then a final report with more detail.