



# Secretary of State Audit Report

## Department of Justice: Child Support Enforcement Automated System (CSEAS) Application Controls Review

### Summary

#### PURPOSE

This audit was performed at the request of the Oregon Attorney General. Its purpose was to evaluate the effectiveness of key general and application computer controls for the Department of Justice (department) Child Support Enforcement Automated System (system) computer application. Our specific audit objectives were to determine whether the department had adequate controls governing data integrity, system security, program change management, and system backup and recovery.

#### RESULTS IN BRIEF

We concluded that while some controls were sufficient, improvements should be made to ensure integrity of system data and overall accountability of child support assets. Specific issues included the following:

- Although 96 percent of receipts processed correctly, the error rate for complex cases requiring manual intervention averaged over 14 percent.
- System data did not reconcile to Oregon State Treasury and statewide accounting system balances. Approximately \$963,000 of the \$11.9 million on deposit as of April 13, 2005, could not be readily explained regarding its origin or intended disposition.
- Support end dates were not always valid.
- Internal controls did not always ensure dual custody of receipts or segregation of important system functions.
- The department's security framework did not adequately protect the system.
- Change management controls did not adequately ensure that code could not be altered after it was tested and approved.

- The department backed up system programs and files, but had not developed disaster recovery plans to restore the application in the event of a major disruption.

#### RECOMMENDATIONS

We recommend that the department:

- Correct identified distribution errors and develop processes governing overrides of system-calculated distributions.
- Establish procedures to routinely reconcile system data to Statewide Financial Management Application accounts and cash on deposit at the Oregon State Treasury and resolve system conversion errors.
- Correct identified errors and periodically validate support end dates.
- Provide additional internal controls over receipts and ensure transaction overrides are independently reviewed and approved.
- Implement recommendations included in our confidential security report.
- Further limit programmer access to tested and approved system code.
- Work with the Department of Administrative Services to establish a disaster recovery solution that will be congruent with the consolidated data center initiative.

Because of the sensitive nature of security, we issued a separate report outlining specific details of our findings and recommendations to improve security in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

#### AGENCY'S RESPONSE

The Department of Justice agrees with the recommendations.

## Background

The 2003 Legislative Assembly redirected responsibility for the child support program from the Department of Human Services to the Department of Justice, Division of Child Support (department). As part of this transfer, the department assumed full responsibility for the Child Support Enforcement Automated System (system).

Subsequent to the transfer, the Oregon Attorney General formally requested that the Oregon Audits Division perform a close examination of the system to validate controls and identify potential risks or opportunities for improvement.

The child support program establishes paternity and child support orders, and enforces child support obligations in cases involving families who are receiving or have received public assistance, and in certain non-assistance cases. The program's purposes are to increase support to children in need, encourage family self-sufficiency, return money to the public treasury and reduce the state's costs in providing public assistance.

The system tracked program data for approximately 250,000 active client cases, and processed child support payments that annually totaled over \$300 million. Approximately \$21.5 million of public assistance was recovered during calendar year 2004 from child support collections. System databases also included information regarding an additional 260,000 inactive child support cases.

The system was developed in the early 1980's and was significantly modified during the late 1990's. Although full responsibility for the system was transferred to the department in 2003, it continued to operate on the Department of Human Services' mainframe computer.

In November 2003, Governor Kulongoski publicly announced an initiative to consolidate many of the state's data centers. The Department of Human Services is scheduled to be one of the first agencies integrated into and serviced by the state's data center created under the Computing and Networking Infrastructure Consolidation (CNIC) initiative.

## Objectives and Purpose

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls for the Department of Justice Child Support Enforcement Automated System (system) application.

Our specific audit objectives were to determine whether the department has implemented controls to provide reasonable assurance that:

- Data remain complete, accurate, and valid during input, processing, and output.
- Information assets are protected against unauthorized use, disclosure or modification, damage or loss.
- System program modifications follow approved change management procedures.
- System files and data are appropriately backed up and could be timely restored in the event of a major disruption.

## Audit Results

### Application Controls Should Be Improved

Effective application controls include either manual or automated routines that ensure only complete, accurate, and valid data are entered into a computer system; processing performs correct functions and results remain accurate; and data are properly maintained.

We concluded that while some application controls for the system were sufficient, improvements should be made to ensure integrity of system data and overall accountability of child support assets. Specific areas needing improvement included application controls to ensure:

- Child support distributions are processed correctly.
- System data are routinely reconciled to Oregon State Treasury and statewide accounting system balances.
- Support end dates are valid.
- Cash receipts are safeguarded and adequate separation of duties maintained.

### Distribution Error Rate Was Too High for Certain Transactions

Application controls should ensure that processing performs correct functions and results are accurate and complete. When manual processes supersede automated controls, alternative or compensating controls should be implemented. Those controls should reduce, to acceptable levels, the risk that errors or fraud could occur and not be detected.

We tested 120 cash receipts processed during March 2005 to determine whether they were distributed according to legal requirements. Our sample included 69 receipts that were automatically processed by the system and 51 where those processes were overridden. Table 1 summarizes the results of these tests and further categorizes them according to the number of obligees involved in the distributions.

As shown on Table 1, the error rate for automatically processed receipts involving multiple obligees was 10.5 percent, whereas no errors were found in our sample of automatically processed receipts

**Table 1: Payment Distribution Error Rate – March 2005**

Distribution Method	Automated		Manual		Total
	Multiple	Single	Multiple	Single	
Number of Obligees	Multiple	Single	Multiple	Single	
Test Population	53,384	120,890	3,371	4,670	182,315
Population Distribution	29.3%	66.3%	1.8%	2.6%	100%
Projected Error Rate	<b>10.5%</b>	<b>0%</b>	<b>14.2%</b>	<b>13.0%</b>	<b>3.7%</b>

involving only one obligee. On the other hand, the error rate for manually processed receipts involving multiple and single obligees was 14.2 percent and 13 percent respectively. Because the majority of errors was isolated within minor segments of the population, the overall error rate for our sample was 3.7 percent.

Based on these tests, we concluded that controls governing the majority of receipt distributions provided adequate assurance that they would process correctly. However, controls over specific complex case distributions did not provide that same level of assurance.

The department primarily relied on automated routines and controls to ensure that child support distributions would be made according to legal requirements. However, some receipts would not process correctly using strictly automated means. In those cases, the department chose to manually override the system to ensure correct distribution. The effectiveness of the manual overrides depended on case managers' ability to properly select cases that should be overridden and make the required adjustments.

All of the errors we identified involved either receipts that should have been selected for manual processing, but were not, or receipts where overrides were incorrectly performed. The majority of exceptions involved complex situations such as receipts with obligors having multiple support cases.

We noted that department management provided little formal direction to case managers regarding which distributions should be overridden. In addition, the department did not have compensating controls, such as independent reviews of overrides, to ensure appropriate distributions.

We concluded that case managers' relatively unrestricted and unsupervised ability to alter cash distributions posed an unacceptable risk that errors or fraud could occur. This risk is further discussed in section, *Internal Controls Should Be Strengthened To Better Safeguard System Assets*, on page 4 of this report.

**We recommend** that department staff correct the distribution errors identified during our testing. We also recommend that department management develop specific manual or automated processes governing overrides of system calculated distributions. These processes should provide detail direction regarding which transaction types must be overridden as well as independent assurance that the overrides are complete, accurate and valid.

***Agency's Response:***

*We agree with these recommendations. By January 2006 we will develop a plan to provide adequate controls over manual distribution as well as procedures for determining when system distribution should be overridden.*

*The errors identified by the auditors relating to past distributions cannot be corrected without billing another family unit because they do not represent state-only funds. We will determine the appropriate action to resolve the distribution errors identified, given the amount of the error, the work required by DCS staff, and the potential for disruption to other families. On a go-forward basis, however, we will quickly correct any future errors that occur.*

**System Data Did Not Reconcile to the Oregon State Treasury Cash Balance**

Generally accepted information technology controls indicate that organizations should establish procedures for data processing that ensure adequate update controls such as run-to-run control totals and master file update controls are in place. In addition, data generated by financial systems should reconcile to corresponding account balances maintained in the organization's general accounting application.

Department staff routinely balanced various system control totals during processing runs to ensure integrity of daily transaction streams. However, they did not perform reconciliations to verify whether system data supported Statewide Financial Management Application (SFMA) accounts or the Oregon State Treasury (Treasury) cash account balance. In addition, a reconciliation between SFMA and Treasury had not been performed since June 2004.

Responding to our inquiries, department staff reconciled system data to the Treasury account balance as of April 13, 2005. That reconciliation indicated that about \$963,000 of the approximately \$11.9 million on deposit could not

be readily explained regarding its origin or intended disposition. The department attributed approximately \$886,000 of that amount to an “adjustments” account that stores undistributed deposits and other transactions needing further attention in order to process correctly.

Department staff indicated that a 1998 computer conversion resulted in errors to approximately 12,000 cases that represented approximately 27 percent of the adjustments account balance. The remainder of that account balance was not readily determinable at the time of the audit. During February 2004, the department began a project to analyze and correct the conversion errors and to reduce the amount of undistributed collections.

Department management estimated that conversion error cases would be resolved by August 2005, and it expects to address the remainder as part of its ongoing efforts to reduce undistributed collections. Ultimately, ownership and distribution of the approximately \$963,000 that the department could not explain remains uncertain, at least until the above project has been completed.

**We recommend** department management establish procedures to routinely reconcile system information to SFMA and Treasury accounts and timely resolve issues identified by those reconciliations. In addition, it should continue to provide resources to ensure that its ongoing project will be expeditiously completed.

**Agency’s Response:**

*We agree with these recommendations. We expect to complete our “adjust project,” including converting pre-1998 accounts, by October 2005. By November 2005, we will develop a plan for monthly reconciliations of the CSEAS account balance with the Treasury account balance.*

### Support End Dates Were Not Always Valid

Oregon law generally limits child support to 18 years, or a maximum of 21 years if the child is in school. However, under certain circumstances the court may extend the ending date for child support beyond those dates. The support end date is an important data element of each child support case record. Approximately 90 days prior to the child’s 18th birthday the system recognizes the support end date and generates notices to staff, then staff notifies obligees of the impending support terminations and requirements to extend benefits. The support end date also indicates to case managers the need to cease support enforcement for the child.

Based on our tests, support end dates did not always agree with legal requirements. The system contained 154 active records where the end date extended beyond the child’s 21st birthday. Department staff indicated that 108 of those dates were incorrectly calculated or entered by case managers, nine were the result of a system error, and 37 were correct dates resulting from court ordered extensions. While investigating the above exceptions, department staff identified an additional 444 records that did not contain support end dates.

Although a 1998 system change automatically populated support end dates, that process did not prevent dates from being overridden incorrectly by case managers or ensure that dates entered before 1998 were correct. In addition, a system change made in 2003 inadvertently caused the system to miscalculate support end dates. This system error was corrected immediately but not all of the affected case data were identified and corrected. In addition, department staff indicated that the missing support end dates

were likely the result of a system error because those dates should have been automatically populated. However, department staff could not propose a preventative solution because the specific cause was not known.

Case managers use support end dates to manage child support enforcement activities. Therefore, incorrect or missing data could result in inappropriate collections and distributions as well as inefficient use of department resources to correct the resulting errors.

**We recommend** that department staff correct the errors identified during our testing and periodically validate support end dates using automated analytical tests.

**Agency’s Response:**

*We agree with this recommendation. These errors have already been corrected. We corrected 447 cases with incorrect end dates. We believe these errors occurred prior to implementation of the CSEAS system and should not reoccur. We will retest the system in three months to ensure the error has not reoccurred.*

### Internal Controls Should Be Strengthened to Better Safeguard System Assets

Application controls should be designed and implemented to provide good internal controls. For financial systems, those controls should safeguard financial assets throughout the transaction life cycle, beginning with the receipt of source documents.

During the receipting process, dual custody of cash and negotiable instruments should be strictly enforced, checks restrictively endorsed, and all receipts logged to facilitate a subsequent independent reconciliation to data input and the bank deposit.

As transactions process, segregation of duties should be maintained to ensure individuals cannot abuse system privileges to inappropriately create or alter transactions and avoid detection. In addition, when manual processes override automated controls, alternative safeguards should be implemented to ensure that the desired level of control is maintained.

Although the department has implemented numerous internal controls over cash receipting, it did not always provide dual custody of cash and negotiable instruments. In addition, an appropriate level of segregation of duties was not maintained when automated controls were overridden.

During calendar year 2004, the department processed approximately \$1.2 million of child support payments daily. Most of those monies were checks received through the mail. Although dual custody of incoming mail containing checks was initially provided, that control was not maintained as staff logged the checks and prepared them for input. In addition, checks were not restrictively endorsed until after they were prepared for entry into the system. Likewise, the department had not provided similar controls over child support checks that had been returned to the department. By not promptly endorsing checks or providing dual custody, the risk was greater that checks could be inadvertently lost or stolen without detection.

As discussed in section, *Distribution Error Rate Was Too High For Certain Transactions*, on page 2 of this report, manual overrides were typically used to accommodate complex or unusual case circumstances that automated procedures were not designed to handle. The manual overrides, in combination with case managers' other duties, allowed users to create

support case records, establish the payee, move money between cases, authorize disbursement of case monies, and issue payments to an alternate payee. Both case managers and reconciliation staff could accomplish each of these actions that, in combination, could allow those users to divert or modify distribution of monies without additional review, approval or other compensating control.

We concluded that the above internal control weaknesses collectively posed an unacceptable risk that errors or fraud could occur and not be detected.

**We recommend** the department provide dual custody of negotiable instruments and ensure checks are restrictively endorsed and logged as mail is opened. In addition, the department should provide compensating controls to ensure that manual overrides are independently reviewed and approved before they are finalized.

***Agency's Response:***

*We agree with these recommendations. We are currently in the process of procuring a new receipting system, and we believe the new system will address some of the control concerns raised. We expect to have the new system in place by June 2006. When operational, we will have improved controls with restrictively endorsed checks and appropriate dual control. In addition, we will prepare a remediation plan to address the issue of manual overrides by January 2006.*

**Security of System Data and Programs Should Be Improved**

Executive management is responsible for establishing an overall approach to security and internal control to ensure protection of resources and to maintain integrity of computer systems.

Based on our tests of security, we concluded that the department's security framework was not adequate to protect the system from unauthorized use, disclosure or modification, damage or loss.

Because of the sensitive nature of system security, we have issued a separate report outlining specific details of our findings as well as recommendations to improve security. That confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

**We recommend** department management implement the recommendations included in our confidential report.

***Agency's Response:***

*We agree that system security is critical. We will address the specific issues in a separate response.*

**Program Change Management Procedures Were Insufficient**

Effective change management procedures should ensure that program modifications are appropriately authorized, documented, thoroughly tested and approved by management before they are placed in production.

The department's change management processes ensured formal consideration and prioritization of change requests, as well as compliance with established programming and documentation standards. However, those procedures did not ensure that program code could not be altered after it was formally tested and approved. As a result, errors or unauthorized code could be introduced into the system without being detected.

**We recommend** department management further limit programmer access to prevent

unauthorized changes to tested and approved system code.

**Agency's Response:**

*We agree with this recommendation. We will analyze the business need for current access levels and determine the appropriate extent of programmer access. Based on specific job duties and business requirements we will work closely with technical staff and security personnel at the Department of Human Services to limit programmer access to only those areas where access is essential. We expect to implement restricted access by February 2006.*

**Disaster Recovery Plans Were Not Developed**

Disaster recovery plans are critical controls for safeguarding assets in the event of a major disruption. Backup and offsite storage of critical system files are also necessary for recovering information systems should a major disruption of services occur.

Although the department backed up system programs and files, it had not developed disaster recovery plans to restore the application or business operations in the event of a disaster.

The system is a critical application for managing state child support cases and ensuring recovery of public assistance payments. We concluded that the inability to recover or a significant delay in recovering this system would pose an unacceptable risk.

**We recommend** the department work with the Information Resources Management Division of the Department of Administrative Services to establish a disaster recovery solution that will be congruent with the consolidated data center initiative.

**Agency's Response:**

*We agree with this recommendation. We plan to complete the department's business continuity planning (BCP) effort by December 2005. Once this effort is complete, our technology staff will address the technology required to support the BCP through creation and testing of a full disaster recovery plan. We will work with DAS IRMD to establish an appropriate disaster recovery plan in conjunction with the implementation of the new consolidated state data center.*

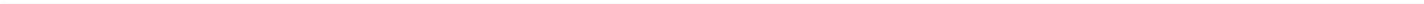
**Scope and Methodology**

During our audit we interviewed various department personnel, examined system documentation, and analyzed electronic data. We performed fieldwork between September 2004 and May 2005.

We tested data from the system's master file as of March 18, 2005, and other data files containing transactions from that entire month of March. During those tests, we used automated tools to verify data validity, format, and relationships.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (CobiT) to identify generally accepted and applicable internal control objectives and practices for information systems.

We conducted our audit according to generally accepted government auditing standards. We also conducted our audit according to Information Systems Audit and Control Association standards for information systems auditing.





**Secretary of State  
Audits Division**

**255 Capitol St. NE, Suite 500  
Salem, OR 97310**

**Auditing to Protect the  
Public Interest and Improve  
Oregon Government**

AUDIT MANAGER: *Neal E. Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Dale Bond, CPA, CISA, CFE  
Erika Ungern, CISA  
Jennifer Crain  
Chris Knutson*

DEPUTY STATE AUDITOR: *Charles A. Hibner, CPA*

*The courtesies and cooperation extended by the officials and staff of  
the Department of Justice were commendable and much appreciated.*

*This report, a public record, is intended to promote the best possible  
management of public resources. Copies may be obtained from our website on  
the internet at:*

*<http://www.sos.state.or.us/audits/audithp.htm>*

*by phone at 503-986-2255*

*or by mail from:*

*Oregon Audits Division  
255 Capitol Street NE, Suite 500  
Salem, OR 97310*