An Audit Report on

The Child Support Enforcement Program at the Office of the Attorney General

March 2004

Report No. 04-024

State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on the

Child Support Enforcement Program at the Office of the Attorney General

SAO Report No. 04-024
March 2004

Overall Conclusion

The Office of the Attorney General (Office) generally administers the Child Support Program so that child support payments are disbursed to custodial parents accurately and in a timely manner. The majority of payments are processed by the Office's State Disbursement Unit (SDU) vendor, and we determined that the vendor processes payments in accordance with federal law and the terms of the contract. We also determined that the Office's contract monitoring function generally does a good job of managing the $130 million SDU contract.

Child Support Program

Federal law requires the Office to establish and operate a state disbursement unit for centralized collections and disbursement of child support payments in Texas (Chapter 234 of the Family Code and 42 USC Sections 654(a)(e) and 654b). The Office has contracted with Affiliated Computer Services, Inc. (ACS) to provide these services in a $130 million, five-year contract that expires in August 2005. The contract amount for fiscal year 2003 was approximately $40 million.

Child support collections totaled approximately $1.5 billion in fiscal year 2002 and $1.9 billion in fiscal year 2003. According to the Office, its State Disbursement Unit processed approximately $1.1 billion of the collections in fiscal year 2002 and $1.5 billion in fiscal year 2003.

However, the Office needs to improve the physical security and tracking of the payments processed by its Payment Processing section, which totaled more than $172 million in fiscal year 2002. In addition, weaknesses in controls over access to child support information systems create a risk that unauthorized individuals could make inappropriate changes to case information. Child support collections totaled approximately $1.5 billion in fiscal year 2002.

We did not identify any irregularities in our tests of the accuracy of data shared between the major information systems used for processing child support transactions, the Texas Child Support Enforcement System (TxCSES) and Stradus.

Key Points

Child support payments are distributed accurately and on time.

During fiscal year 2002, the Office's State Disbursement Unit (SDU) distributed $1.1 billion in child support payments from noncustodial parents to custodial parents accurately and on time. Our testing of a sample of payments showed that the vendor with which the Office contracts to run the SDU processed payments within the timeframes required by federal law and the contract.

Improvements are needed in the security and tracking of child support payments processed by the Payments Processing section.

The Office needs to improve physical security and tracking of payments processed by its Payment Processing section, which totaled more than $172 million in fiscal year 2002. Payment Processing is responsible for payments that are sent to a suspense account

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This audit was conducted in accordance with Government Code, Sections 321.0131 and 321.0133.

For more information regarding this report, please contact Sandra Vice, Audit Manager, at (512) 936-9500.

because they cannot be linked to a specific case or were sent back for other reasons such as an incorrect address. The Office keeps returned warrants in a vault while Office employees attempt to determine the correct address or case. Weaknesses in the physical security and tracking of these items increase the risk that they could be misappropriated without detection.

The two major systems used to process child support transactions, TxCSES and Stradus, appear to have controls in place to share data accurately; however, insufficient access controls leave them vulnerable to unauthorized access.

Our review of the controls and processes involved in the exchange of information between TxCSES and Stradus, two systems that maintain child support data, did not identify any irregularities. However, during our review of users' access to TxCSES and Stradus, we noted significant security risks such as easy-to-guess passwords and terminated employees who still had system access.

The Office effectively manages its $130 million State Disbursement Unit contract with the exception of not collecting in a timely manner $446,000 owed by the vendor for processing errors.

The Office generally managed its $130 million SDU contract in fiscal year 2002 effectively. This assessment is based on our audit of the SDU vendor's compliance with three key contract provisions. These provisions are (1) "payments received by 2:00 p.m. shall be processed and transmitted to TxCSES the same day," (2) "balance and deposit of payments," and (3) "billing and invoicing."

The Office's Monitoring Division did not recoup in a timely manner at least $446,000 in funds that the SDU vendor owed the Office for SDU processing errors. For errors that occurred between July 2000 and May 2003, the Monitoring Division did not request repayment from the SDU until September 2003, during our fieldwork. According to management, the SDU vendor has since repaid the funds. These processing errors allowed the vendor to keep State funds for six months to more than three years in some instances.

Summary of Management's Response

The Office generally agrees with our recommendations. However, the Office took exception to some specific issues related to payment processing and monitoring of the SDU contract. We provided auditor follow-up comments for the findings with which the Office took exception.

Summary of Information Technology Review

The Office uses two systems to maintain child support data. Stradus is the SDU's collection and disbursement system. This system receives and disburses child support payments and manages case data for the State of Texas. TxCSES is the Office system that was certified by the federal government in July 1999 and that maintains case information for cases in which a guardian parent is receiving child support services offered by state and local agencies.

Due to the complexity of the interfaces between TxCSES and Stradus, we were not able to re-create all the steps the systems take to exchange electronic data. However, we looked at the controls and processes related to these TxCSES and Stradus interfaces and did not note any irregularities.

We also reviewed the access of users with edit capabilities (which can include adding, deleting, or changing information related to child support cases) to TxCSES and Stradus. We identified weaknesses in the areas of access controls and user access to these systems that need to be addressed.

Summary of Objective, Scope, and Methodology

The overall objective of the audit was to determine whether the Office is administering the Child Support Program so that child support payments are disbursed to custodial parents in a timely manner.

Our audit scope covered information technology, contract monitoring, payment processing, and financial reporting for fiscal years 2001 to 2003 at the Child Support Division of the Office and the SDU. Testing of SDU payment transactions and contract monitoring work focused on fiscal year 2002. We also reviewed current security and access control processes at offices in Tarrant, Dallas, and Harris Counties.

The audit methodology consisted of collecting information and documentation, creating detailed process maps, performing selected tests, analyzing and evaluating the results of tests, and conducting interviews with the Office, SDU, and county management and staff.

Table of Results and Recommendations 💻 **denotes entry is related to information technology**
Child support payments are generally distributed accurately and on time. (Page 1)
(no recommendation)
Inadequate security access levels for the vault and payment processing areas could allow inappropriate access. (Page 2)
The Office should develop procedures for granting and removing access to the vault and payment processing area. Specifically, it should: • Develop follow-up procedures to ensure that requested changes were made to the payment processing and vault areas. • Review employees' access regularly to ensure that it aligns with their job responsibilities. • Ensure that the active start and stop dates in the system allow for periodic review of appropriate access levels by management. Also, it should maintain records of who requests access level changes and who makes those changes.
Management does not sufficiently monitor the status of returned payments. (Page 5)
The Office should: • Develop an internal policy that establishes a suitable timeframe for resolving problems with returned warrants. • Continue to conduct biweekly inventories of returned warrants in the vault and follow policies and procedures, including conducting a supervisory review to ensure the accuracy of the Returned Warrant Inventory. • Change the system to include a final disposition of the returned warrants in order to determine who removed a returned warrant from inventory and when it was removed. • Use internal systems to electronically generate a monthly report for management decision making that includes suspense items and returned warrants. For suspense items, the Office should coordinate the production of the manual spreadsheets to minimize duplication of efforts until the monthly report is available. • Reconcile the Returned Warrant Inventory against the SDU vendor's monthly reports for accuracy and completeness.
The Office does not track the total dollar amount of payments that the SDU sends to Payment Processing in error. (Page 9)
The Office should monitor the amount that is sent back to the SDU for reprocessing and hold the SDU accountable for putting items in suspense unnecessarily.
TxCSES and Stradus appear to have controls in place to share data accurately; however, insufficient access controls leave them vulnerable to unauthorized access. (Page 11) 💻
The Office should: • Ensure that the information technology department is notified of staff terminations so that user access is modified in a timely manner to minimize the risk of unauthorized access. • Establish a process to review users' access to Stradus on a regular basis. • Limit the number of invalid access attempts to three in Stradus. • Change Stradus and TXCSES minimum password requirements to at least eight characters with alphanumeric and special characters.
The Office effectively manages its $130 million SDU contract, with the exception of not collecting in a timely manner $446,000 by the vendor for processing errors. (Page 15)
We recommend that the Office identify, verify, and recoup funds associated with vendor processing errors on a monthly basis.
Administrative funds for the Child Support Enforcement Program are spent in accordance with state restrictions. (Page 17)
(no recommendations)
Quality control reviews reduce the risk that applications will be entered inaccurately or not processed in a timely manner. (Page 18)
(no recommendations)

Recent SAO Work		
Number	**Product Name**	**Release Date**
03-048	A Review of State Entities' Preparedness for Compliance with the Health Insurance Portability and Accountability Act	August 2003
03-703	A Summary of the Texas State Workforce for Fiscal Year 2002	December 2002
02-065	An Audit Report on the Compensation to Victims of Crime Fund and the Accuracy of Financial Information at the Office of the Attorney General	August 2002
02-049	An Audit Report on Funds Collected as Court Costs	May 2002

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

Child Support Payments Are Generally Distributed Accurately and On Time

During fiscal year 2002, the Office of the Attorney General's (Office) State Disbursement Unit (SDU) distributed $1.1 billion in child support payments from noncustodial parents to custodial parents accurately and on time. Our testing of a sample of payments showed that the vendor with which the Office contracts to run the SDU processed payments within the timeframes required by federal law and the contract.

The SDU is meeting its contractual agreement with the Office to process payments received by 2:00 p.m. on the same business day. In some instances, our tests revealed that the SDU exceeded this contract provision because it processed payments received after 2:00 p.m. on the same business day. We selected a random sample of payments that the Office's Contract Monitoring Division reviewed in fiscal year 2002 and verified the results. This division is responsible for reviewing the SDU's compliance with the above contract provision, and it has consistently concluded that the SDU is compliant.

Federal law requires states to process and mail child support payments to custodial parents within two business days. The Office's requirements are more stringent and generally result in payments being processed in one business day. (See Chapter 2 for additional information on the processing of child support payments.)

Chapter 2

Improvements Are Needed in the Security and Tracking of Child Support Payments Processed by the Payment Processing Section

The Office needs to improve the physical security and tracking of payments processed by its Payment Processing section, which totaled more than $172 million in fiscal year 2002. Weaknesses in the physical security and tracking of these payments increase the risk that payments could be taken without detection. Specifically:

- Inadequate security access levels for the vault and payment processing areas could allow inappropriate access.
- Management does not sufficiently monitor the status of returned payments.

Suspense Items

Suspense items are payments from noncustodial parents that cannot be linked to a specific case for numerous reasons. For example, blank money orders or checks that do not have two of four identification points (recipient name, case number, cause number, and social security number) are put into the suspense account. Payment Processing researches suspense items upon receipt.

Of the $1.5 billion in child support collections the Office received in fiscal year 2002, $2.8 million was in suspense items.

In addition, the Office does not track the total dollar amount of payments that the SDU sends to Payment Processing in error. This information would help the Office measure the effect of the SDU's errors, which we determined to be more than $400,000 per month for the three months of data we compiled.

Payment Processing is responsible for payments that are sent to a suspense account because they could not be linked to a specific case or were sent back for other reasons such as an incorrect address (see text box). The Office keeps returned warrants in a vault while Office employees attempt to determine the correct address or case (see text box on page 5).

Chapter 2-A

Inadequate Security Access Levels for the Vault and Payment Processing Area Could Allow Inappropriate Access

Weaknesses in the Office's security access levels for the vault and the payment processing area could allow inappropriate access to these areas. Access to the payment processing and vault areas are controlled by a scan-card security system, which only allows access based on the security level approved by management in these areas. Payments totaling approximately $172 million were processed by the Payment Processing section during fiscal year 2002. There are no documented procedures for assigning or removing staff members' access to these areas. We noted the following issues:

- **Requested changes to security profiles were not made in a timely manner.** We identified employees who still had active access cards up to five months after a request was made to remove their access to the payment processing area. One of these employees left employment with the Office prior to our audit.
- **Some employees had inappropriate levels of access to the vault.** We identified one employee whose access was not appropriately aligned with current job responsibilities. According to the Lead Security Officer, another employee was

mistakenly given access to the vault instead of to the payment processing area. Furthermore, both an internal audit and an internal payment processing security review noted that several cardholders had high levels of access to the payment processing area even though such access was not requested by the Payment Processing section. Only Payment Processing section managers are allowed to request access changes. However, we did not note any instances in which these employees gained access to the payment processing area subsequent to the request date.

- **The Office is not maximizing controls within the security system.** The system includes a control that would automatically disable the use of an employee's access card on a certain date, but the Office renders this control ineffective by entering a date that is 95 years in the future. We noted instances in which an employee's effective stop date (the date until which an employee is allowed access) in the system was December 2099. The Lead Security Officer informed us that the stop date is entered this way to eliminate the need to update it on a regular basis. Periodic expiration dates allow management an opportunity to determine whether access is still appropriate. In addition, the system can maintain records of information about the employees with access, such as who authorized the access and how long the employee should have access. However, this system feature is not being used.

Recommendations

The Office should develop procedures for granting and removing access to the vault and payment processing area. Specifically, it should:

- Develop follow-up procedures to ensure that requested changes were made to the payment processing and vault areas.
- Review employees' access regularly to ensure that it aligns with their job responsibilities.
- Ensure that the active start and stop dates in the system allow for periodic review of appropriate access levels by management. Also, it should maintain records of who requests access level changes and who makes those changes.

Management's Response

Generally, the OAG agrees with the recommendations and recognizes that additional controls should be put in place to improve physical access to the payment processing area. However, there is an issue that warrants clarification.

The report states that payments totaling $172M were processed by the payment processing section. The OAG disagrees that the entire amount processed is at risk based on findings in this section of the report. Given the context of the report, it is implied that all payments passed through the vault. They did not. A substantial portion of this amount was actually processed electronically, including $137M in IRS payments. These electronic payments are deposited directly with the Texas Comptroller of Public Accounts (TCPA) and never pass through the payment *processing section or vault. The only items actually handled by the section are payments that are inadvertently mailed to the State Office and returned warrants. For FY02, these totaled $41M. Generally mail that is inadvertently sent to the State Office is removed from the vault within one business day. Returned warrants are re-mailed if a current address can be obtained within 5 business days. Otherwise they are cancelled and returned to the TCPA. Warrants associated with deceased custodial parents require additional research and are held in the vault for longer periods. As noted in this report, at the end of fiscal year 2003, there were only 587 returned warrants in the OAG's vault. As of February 24, 2004, there were only 279 items in the vault.*

The Audit Recommends the Office should:

- *Develop follow-up procedures to ensure that requested changes were made to the payment processing and vault areas.*

Management Response:

The office agrees with this recommendation. Prior to adding or renewing the employee's security access level, an assessment will be made to determine the proper alignment of access level with each staff member's job responsibility. These procedures will also include a tracking mechanism to document the requestor and the approval of all security access level additions, revisions, and deletions. The targeted date for finalization of these corrective actions is fall of 2004.

The Audit Recommends the Office should:

- *Review employees' access regularly to ensure that it aligns with their job responsibilities.*

Management Response:

The office agrees with this recommendation. Effective immediately, the Payment Processing section will implement a monthly review of personnel with access to the secured area, including the vault.

The Audit Recommends the Office should:

- *Ensure that the active start and stop dates in the system allow for periodic review of appropriate access levels by management. Also, it should maintain records of who requests access level changes and who makes those changes.*

Management Response:

The office agrees with this recommendation. The Agency will implement periodic expiration dates for all employees. Automated enhancements are being developed causing each employee's access level to expire annually. This action will eliminate the present stop date of 2099. As noted above, these procedures will also include a tracking mechanism to document the requestor and the approval of all security access level additions, revisions, and deletions. The targeted date for finalization of these corrective actions is fall of 2004.

Auditor's Follow-up Comment

The Office disagrees that $172 million is the appropriate amount of dollars at risk. However, the $172 million represents all payment transactions that Payment Processing is responsible for disbursing. In addition to concerns about physical access, we also noted information technology security issues within the Office's security information system, which apply to all dollars whether or not they are physically located in the vault. Therefore, our statement that the Payment Processing area processed $172 million in fiscal year 2002 accurately indicates the dollars at risk.

While the Office refers to an amount of $41 million in the vault, we have not been provided with any supporting documentation to substantiate this amount. During fieldwork, we requested that the Office provide the total dollars held in the vault for fiscal year 2002, but the Office staff informed us that this amount was not available because returned warrants are tracked on a daily basis and are not summarized.

The Office's response indicates that some returned warrants can be held in the vault for longer periods. We found multiple instances in which returned warrants were maintained in the vault for up to 180 days, which we considered excessive. See Chapter 2-B.

Chapter 2-B

Management Does Not Sufficiently Monitor the Status of Returned Payments

Management does not sufficiently ensure that returned child support payments (also called returned warrants; see text box) are properly inventoried and processed in a timely manner. This situation creates a risk that someone could remove a payment from the vault and from the inventory list and not be detected.

Returned Warrants

Returned warrants are child support payments that the SDU has mailed to custodial parents but that are returned for numerous reasons, such as not having the custodial parent's correct address. When warrants are returned to the SDU, the SDU staff research the warrants for bad addresses and remail the warrants. If the SDU is unable to resolve the returned warrants, the SDU forwards them to the Office's Payment Processing section, where they are kept in a vault until they are posted to a case or canceled. This section is responsible for locating the proper address and ensuring that the custodial parent of the child receives the child support payment.

If a suitable address or an appropriate custodial parent cannot be located, the warrant is canceled and the funds are returned to the Office of the Comptroller of Public Accounts.

In both fiscal years 2002 and 2003, there were approximately 10,000 returned warrants sent to Payment Processing for further research. There are no summary reports for returned warrants that list their total value. However, at the end of fiscal year 2003, there were only 587 returned warrants in the Office's vault.

We tested a sample of returned warrants and noted the following issues:

- The Office has not established a suitable timeframe by which problems with the warrants should be resolved and the warrants mailed to custodial parents. For our tests, we considered more than 180 days in the vault as excessive for returned warrant processing, and we found warrants that exceeded this timeframe. Without such a timeframe, the Office cannot evaluate the Payment Processing section's efforts.

- Management asserts that it recently started conducting biweekly inventories in order to monitor the returned warrant inventory. However, we found that these inventories are not consistently accurate. We identified a warrant that had been canceled by Payment Processing staff and was no longer in the vault, but it was still listed in the Returned Warrant Inventory. Two inventories failed to identify this discrepancy. It was finally resolved approximately 40 days later and removed from the list.

The Payment Processing section did not have written policies and procedures on conducting inventories until December 2003 (during our audit). As a result, inventories were not conducted in a consistent manner. In addition, the Returned Warrant supervisor received a copy of the inventory, but documentation was not maintained to prove that a supervisory review occurred. New policies now require a signature. These issues were also noted in a February 2003 internal audit report.

- While the Office tracks the individual payments removed from inventory, it does not track who removed an item from the inventory or what date the item was removed. Without the ability to trace changes or updates back to the individuals who made them, there is no way to hold the vault personnel accountable in the event items are incorrectly removed from the inventory list, either erroneously or intentionally.

There is an opportunity for efficiency gain within the Office's Payment Processing section. We noted an opportunity for the Payment Processing section to make its reporting process more efficient by using its automated system to generate monthly reports. Currently, the Office does not have the ability to automatically generate summary level reports for suspense items and returned warrants. To create monthly summary reports for management decision making, multiple Payment Processing staff members and the vendor duplicated their efforts by manually entering the same daily information regarding suspense items into separate spreadsheets. While the differences were not significant, we observed that the amounts listed on the different spreadsheets did not match due to typographical errors. For returned warrants, staff members pull information from their system, which as discussed above is not consistently accurate. The Payment Processing section receives a monthly list of returned warrants from the SDU vendor; however, Payment Processing does not reconcile this list with the payments it has actually received.

Recommendations

The Office should:

- Develop an internal policy that establishes a suitable timeframe for resolving problems with returned warrants.

- Continue to conduct biweekly inventories of returned warrants in the vault and follow policies and procedures, including conducting a supervisory review to ensure the accuracy of the Returned Warrant Inventory.

- Change the system to include a final disposition of the returned warrants in order to determine who removed a returned warrant from inventory and when it was removed.

- Use internal systems to electronically generate a monthly report for management decision making that includes suspense items and returned warrants. For suspense items, the Office should coordinate the production of the manual spreadsheets to minimize duplication of efforts until the monthly report is available.

- Reconcile the Returned Warrant Inventory against the SDU vendor's monthly reports for accuracy and completeness.

Management's Response

The OAG takes exception to a number of the statements in this section. Each is addressed below.

Due to the nature of returned warrants, system-generated returned warrant reports are not available; however, manual reports are reviewed by payment processing management on a daily basis. The OAG can and does evaluate the section's efforts using these reports. Aging information, alone, for returned warrants does not provide substantial information to measure the section's efforts. All warrants could be cancelled upon receipt thus significantly reducing the timeframe in the vault. However it would undermine efforts to get the money to the recipient in a timely manner.

Regarding vault inventory policies and procedures, these were being re-written during the audit time frame. Previously used procedures were not available to SAO staff. Process improvements continued to be made throughout the course of the audit. Finalized procedures have been implemented and are currently being followed.

The report states that the OAG does not track who removed an item from the inventory or what date the item was removed. This is not accurate. Such information is readily available online and can be used to hold vault personnel accountable. The confusion may be associated with an enhancement being implemented to add this detail to an existing report.

The report states that the OAG does not have the ability to automatically generate summary level reports for suspense items and returned warrants. Currently the OAG does have the ability to automatically generate summary level reports for Full Service (IV-D) suspense and returned warrants (e.g., CL2008R1 and DB0004R1, 2 for suspense and DB0002R1, 2, 5, and 6 for returned warrants). Registry Only (Non IV-D) returned warrants are tracked separately by the SDU. The Payment Processing section spreadsheets are used to monitor suspense activity on a daily basis. Further, daily reports are provided to and reviewed by executive management at the beginning of each workday. As noted by the SAO in this report, of the $1.5 billion in child support collections in fiscal year 2002, $2.8 million was in suspense items. This represents two-tenths of one percent (.2%) which is one of the lowest percentages in the nation. Texas continues to be a leader nationwide in the reduction of undistributed collections, including suspense items.

The Audit Recommends the Office should:

- *Develop an internal policy that establishes a suitable timeframe for resolving problems with returned warrants.*

Management Response:

The OAG agrees with this recommendation. The payment processing section procedures prescribe that warrants are cancelled within 5 days. However, there are exceptions that merit keeping the warrant longer (e.g., when a custodial parent has died and the agency is working with the estate to forward the warrant appropriately). It should be noted that on February 24, 2004, there were only 279 items in the vault compared to 587 as of August 31, 2003. The payment processing section will work with the OAG Policy Formulation Group (PFG) to address the official policy regarding returned warrant cancellation timeframes by summer 2004.

The Audit Recommends the Office should:

- *Continue to conduct biweekly inventories of returned warrants in the vault and follow policies and procedures, including conducting a supervisory review to ensure the accuracy of the Returned Warrant Inventory.*

Management Response:

The OAG agrees with this recommendation. Biweekly inventories are currently being developed in accordance with prescribed procedures. Section management will review results of the findings on a regular basis with payment processing management.

The Audit Recommends the Office should:

- *Change the system to include a final disposition of the returned warrants in order to determine who removed a returned warrant from inventory and when it was removed.*

Management Response:

Although the OAG takes exception to specific findings associated with this recommendation, we are modifying an existing report to include final disposition. As stated earlier, such information is readily available online and can be used to hold vault personnel accountable. The confusion may be associated with an enhancement being implemented to add this detail to an existing report. Once the enhancement is implemented, the report can be used, along with the online TXCSES feature currently available, to track the disposition to an individual who made the change or update.

The Audit Recommends the Office should:

- *Use internal systems to electronically generate a monthly report for management decision making that includes suspense items and returned warrants. For suspense items, the Office should coordinate the production of the manual spreadsheets to minimize duplication of efforts until the monthly report is available.*

Management Response:

Although the OAG takes exception to specific findings associated with this recommendation, payment processing management will review/revise various daily/monthly reports and reconciliation procedures as appropriate by the summer of 2004.

The Audit Recommends the Office should:

- *Reconcile the Returned Warrant Inventory against the SDU vendor's monthly reports for accuracy and completeness.*

Management Response:

Management agrees with this recommendation. By the summer of 2004, payment processing management will review/revise various daily/monthly reports and reconciliation procedures as appropriate.

Auditor's Follow-up Comment

While we recognize the Office's ability to generate daily reports, the issue is that management does not have summary level information to effectively monitor the status of returned warrants and suspense items.

The Office is currently taking daily reports and manually summarizing the information to create monthly suspense reports. To increase efficiency and accuracy, we recommend that the Office instead have the system generate monthly summary reports to assist in decisions regarding productivity, allocation of resources, and SDU trend activity. Management indicates in its response "all warrants could be cancelled upon receipt thus significantly reducing the timeframe in the vault." The State Auditor's Office is recommending an improvement to establish suitable timeframes for returned warrants. We are not recommending that the Office cancel returned warrants upon receipt, as noted in management's response.

Management responded that it does track who removes an item from the inventory or what date the item was removed. This is inconsistent with information that the Returned Warrant Supervisor provided us during fieldwork.

Chapter 2-C

The Office Does Not Track the Total Dollar Amount of Payments that the SDU Sends to Payment Processing in Error

We noted that the Office does not track the total dollar amount of payments that the SDU sends to Payment Processing in error. This information would help the Office measure the effect of the SDU's errors, which we determined to be more than $400,000 per month for the three months of data we compiled. We determined that the SDU may not be effectively researching payments that it cannot readily tie to a case in its system.

Specifically, we tested a sample of suspense items for fiscal year 2003 and noted that the Payment Processing section returned almost 50 percent of items to the SDU for reprocessing. Payment Processing staff indicated that the SDU had sent several items to Payment Processing in error, and these items had to be reprocessed by the SDU. The Office appears to have controls in place to prevent the SDU from being paid twice for reprocessed payments. In August 2003, approximately $405,000 in undistributed child support payments was sent back to the SDU for reprocessing, which lengthened the time spent to distribute the money to custodial parents.

Further, when the SDU sends a payment to the suspense account, the SDU is not penalized for not processing the payment on time, even if it sent the payment to suspense in error. For payments that are not sent to suspense, the Office charges the SDU penalties for not meeting contracted timeframes. If penalties are not associated with the SDU sending items to the suspense account in error, this situation could create an incentive for the SDU to send payments to the suspense account rather than perform the necessary research.

Recommendation

The Office should monitor the amount that is sent back to the SDU for reprocessing and hold the SDU accountable for putting items in suspense unnecessarily.

Management's Response

The OAG supports the recommendations. However, the OAG takes exception to the statement that the OAG does not track the total dollar amount of payments that the SDU sends to payment processing in error. The payment processing section monitors and reports this information on a daily basis. They proactively work with SDU staff to address these errors.

In order to hold the SDU accountable, Contract Monitoring uses two oversight routines:

- *A monthly sample evaluation of suspense items to determine the appropriateness of placement in suspense and proper handling, resulting in remedy enforcement.*
- *Calculates a ratio of all SDU processing errors, including suspense items, to all collections processed in order to measure the overall accuracy of SDU collections processing.*

Auditor's Follow-up Comment

Our recommendation is meant to provide a best practice to the Office to increase its ability to monitor efficiently the amount sent from the SDU to the Office in error (approximately $1.4 million for the three months of data we compiled). If the Office tracked payments sent in error on a summary level, it could perform various types of analysis to determine the extent of the problem.

One of the Office's oversight routines is performed on a sample basis, but does not include a review of these types of errors as a whole. The other routine combines errors sent back for reprocessing with all other types of SDU processing errors. These oversight routines limit the Office's ability to hold the SDU accountable for placing items in suspense unnecessarily and to determine appropriate remedies.

Chapter 3

TxCSES and Stradus Appear to Have Controls in Place to Share Data Accurately; However, Insufficient Access Controls Leave Them Vulnerable to Unauthorized Access

Our review of the controls and processes involved in the exchange of information between TxCSES and Stradus, two systems that maintain child support data (see text box), did not identify any irregularities. However, during our review of users' access to TxCSES and Stradus, we noted significant security risks.

TxCSES and Stradus

The Texas Child Support Enforcement System (TxCSES) is the Office system that was certified by the federal government in July 1999 and that maintains case information for cases in which a guardian parent is receiving child support services offered by state and local agencies.

Stradus is the SDU's collection and disbursement system. This system receives and disburses child support payments and manages case data for the State of Texas. Stradus also provides an automated means for local counties to supply State Case Registry information that is required by the federal government. Stradus maintains information for cases in which the case or legal order is privately entered into the system and for which state or local agencies do not provide location, enforcement, or collection services.

Controls and processes for sharing data. Because of the complexity of the interfaces between TxCSES and Stradus, we were not able to re-create all the steps the systems perform during electronic data exchanges for all interfaces. However, we reviewed the controls and processes in place for these interfaces, and we did not note any irregularities.

Access controls. Critical data in the Office's information systems is at risk for unauthorized access. We found access control issues in both the TxCSES and Stradus information systems. TxCSES has the following weaknesses in its access controls:

- **User access is not properly terminated**. The list of active TxCSES users with edit capabilities provided by Office management contained 31 users who should not have access to the system. Some of these users were terminated employees who had not been removed from the system promptly. On average, 78 days elapsed after termination before access was removed. By not properly terminating access to the system, the Office risks unauthorized additions, deletions, or other changes to case or payment information. We did not identify any access violations related to these 31 users.

- **Password security is inadequate**. TxCSES passwords are not sufficiently complex and could allow unauthorized users to guess them. The Office is in the process of changing its password requirements. However, it has been waiting for password guidance that the Internal Revenue Service is expected to issue.

Stradus's access control issues consist of the following:

- **User access is not reviewed on a regular basis**. Of the Office staff members with edit access to Stradus, four were terminated but were still listed in the system as active. According to the Office, the access rights of these users have been revoked as a result of our inquiry. Various field offices and counties do not notify the Office about terminations in a timely manner. Additionally, there is no process for reviewing users' access to Stradus.

  Stradus has 1,858 users, consisting of Office and county employees, with update capabilities, which include adding, deleting, or changing case information. In fiscal year 2002, $1.5 billion in child support payments were received and $1.1 billion were processed in Stradus.

- **Users are not locked out after failed access attempts**. Stradus does not lock a user out of the system after a certain number of failed access attempts. Industry standards suggest that systems should lock out users after three failed attempts.

- **Password security is inadequate**. Like those for TxCSES, Stradus passwords are simple and at risk of easy detection. In addition, the current minimum length required does not meet the industry standard for passwords. The passwords for Stradus expire every 30 days, and the user IDs expire annually.

Recommendations

The Office should:

- Ensure that the information technology department is notified of staff terminations so that user access is modified in a timely manner to minimize the risk of unauthorized access.

- Establish a process to review users' access to Stradus on a regular basis.

- Limit the number of invalid access attempts to three in Stradus.

- Change Stradus and TxCSES minimum password requirements to at least eight characters with alphanumeric and special characters.

Management's Response

CSD recognizes the importance of promptly removing system access when users are terminated from employment. The findings also bear out the importance of improving the notification process. Nearly all of the examples cited in the report are due to the delays in notifying the Information Technology Section's Help Desk. Primarily, these delays occur because work assignments tied to those accounts must be reassigned to a different user or a new hire. Typically management notified the Help Desk when this process is complete and the account access is then removed. The Help Desk also conducts a security profile of internal users by region every six months. This control process was instituted to assist the Help Desk in properly administering account access. The user profile review was moderately successful in detecting accounts that should have already been deleted. To further advance the notification process, CSD now produces a monthly report which identifies internal accounts that have not been used in at least 62 days, which will further assist the Help Desk.

Other internal control considerations, such as limiting the number of invalid access attempts before locking out the user and increasing the number of user access internal reviews, are currently being analyzed. The agency has targeted the fall of 2004 to have completed its analysis, testing and installation of security measures per these control issues.

The Audit Recommends the Office should:

- *Ensure that the information technology department is notified of staff terminations so that user access is modified in a timely manner to minimize the risk of unauthorized access.*

Management Response:

The agency agrees with this recommendation. Over the past several months, payment processing has been forwarding OAG terminations to Stradus security administrators. County terminations are more difficult to enforce as we are reliant upon the counties to forward that information to the OAG. By summer 2004, we will revise procedures for inactivating Stradus accounts for terminated users, including county users.

Regarding TXCSES access, additional action taken to further the notification process involves the creation of two (2) additional user accounts per local field office. This creation will enable the reassignment of the separated staff's caseloads, thus relieving management from maintaining accounts until replacements can be either reassigned or hired. Several procedural enhancements have been installed to expedite the Help Desk's notification. These include the following:

1. *All Employee Clearance Checklists must be completed and forwarded to Human Resources Department (HRD) the last day of employment.*

2. *Office management is required to notify the Help Desk of employee, intern and volunteer terminations/transfers the <u>same</u> day the event occurs. This can be achieved in two ways. The preferred way is to send a request via the Intranet (UserID Request Form). However, it can also be achieved by sending a request to CSD-UserID. In either event, this must be done no later than the day the employee terminates.*

3. *Managers must monitor the time of volunteers and interns closely. If they are no longer performing work on behalf of the OAG, their access must be revoked.*

4. *Each local field office manager and managing attorney has had their individual performance plan expanded to include a Task Statement which reads:*

   "Ensures the Help Desk is notified of employee, intern and volunteer terminations/transfers the same day the event occurs. ***[No Exceptions Allowed.]****"*

   - *The task statement requirement of "No Exceptions Allowed" means that a single violation of the statement will result in a rating of "Needs Improvement".*

The Audit Recommends the Office should:

- *Establish a process to review users' access to Stradus on a regular basis.*

Management Response:

The agency agrees with this recommendation. At a minimum, we will implement monthly reviews of system access. We are also investigating the feasibility of suspending accounts that have not been used for 30-60 days.

The Audit Recommends the Office should:

- *Limit the number of invalid access attempts to three in Stradus.*

Management Response:

The agency agrees with this recommendation and is working with SDU management to implement the modifications to Stradus. OAG management will weigh costs of implementing this change against other priorities, especially given the TXCSES Stradus Integration (TSI) schedule and the Child Support State Disbursement Unit contract procurement.

The Audit Recommends the Office should:

- *Change Stradus and TxCSES minimum password requirements to at least eight characters with alphanumeric and special characters.*

Management Response:

The agency agrees with the recommendation to change TXCSES. CSD is proceeding with the audit's recommendation by expanding the TXCSES minimum password requirement to an 8 character password with alpha-numeric and special characters. The implementation of this automation and the transition upon programming completion will be realized by October 2004. However, given the circumstances, additional analysis is needed to weigh the cost of the change to Stradus. Stradus currently requires 5-8 characters. OAG management will review costs associated with implementing this recommendation against other priorities, especially given the TXCSES Stradus Integration (TSI) schedule and the Child Support State Disbursement Unit contract procurement.

Chapter 4

The Office Effectively Manages Its $130 Million SDU Contract, with the Exception of Not Collecting in a Timely Manner $446,000 Owed by the Vendor for Processing Errors

The Office effectively managed its $130 million SDU contract in fiscal year 2002, with one exception. The Office's Monitoring Division did not recoup in a timely manner at least $446,000 in funds that the SDU vendor owed the Office for SDU processing errors. These processing errors delayed payments to the affected custodial parents. For errors that occurred between July 2000 and May 2003, the Monitoring Division did not request repayment from the SDU vendor for the $446,000 until September 2003, which occurred during our fieldwork. This allowed the vendor to keep State funds—for six months to more than three years in some instances—rather than reimburse the Office for any expenses incurred in correcting these processing errors. According to the SDU contract, the Office should recoup expenses for payments its sends out in error as a result of SDU processing errors at least every six months once the Office's Adjustments Section verifies the SDU's errors.

The Contract Monitoring Division is responsible for ensuring that the SDU vendor processes child support payments on time and provides other related services as required by the contract. The SDU vendor is responsible for the accurate and timely processing of child support payments.

If the Office's Adjustments Section verifies that the SDU vendor caused a processing error (for example, posting a payment to the incorrect account) and the processing error affects a child support case of the Office's, the Office must pay the custodial parent who should have received the payment. The Office then attempts to recoup the funds from the parent to whom they were incorrectly sent.

Other than not recouping funds in a timely manner, the Office effectively manages the SDU contract to ensure that services are delivered according to contract terms. This assessment is based on our audit of the SDU vendor's compliance with three key contract provisions:

- **"Payments received by 2:00 p.m. shall be processed and transmitted to TxCSES the same day."** As discussed in Chapter 1, the SDU processes payments received by 2:00 p.m. and transmits them to TxCSES the same day.

- **"Balance and deposit of payments."** The Office ensures that the SDU vendor balances and reconciles all payments in Stradus before they are sent to the Office of the Comptroller of Public Accounts (Comptroller) to be entered into the Uniform Statewide Accounting System (USAS). The Office conducts a daily reconciliation to ensure that all payments collected at the SDU are accurately recorded in USAS.

- **"Billing and invoicing."** After randomly selecting five months to test, nothing came to our attention to indicate that the Office does not ensure that all invoices paid to the SDU are accurate before they are paid. Furthermore, after reviewing the work conducted by the Office's Contract Monitoring Division, we conclude that the Office is conducting an accurate review of the SDU's monthly transactions.

Recommendation

We recommend that the Office identify, verify, and recoup funds associated with vendor processing errors on a monthly basis.

Management's Response

The OAG concurs with the recommendation and will comply once TXCSES processing and reports are fixed to accurately calculate contractor liability for IV-D processing errors. Prior to a one time data correction by OAG technical staff, TXCSES reports significantly overstated vendor liability and impeded settlement of IV-D processing errors and will continue to impede ongoing settlements until a final solution is implemented. Therefore, the recommendation would be more informative to readers if it reflected the cause of the settlement delay.

The OAG also wishes to note that Non IV-D settlements were timely made throughout the contract Term, IV-D settlement was made for the period before TXCSES automation, and efforts were made to settle subsequent IV-D errors before this audit. Documentation to substantiate these assertions will be provided to the SAO upon request.

Auditor's Follow-up Comment

Management did not provide the auditor any documents to support that the SDU was billed prior to September 2003 for the $446,000 in IV-D transactions. By delaying recoupment, the Office allowed the vendor to keep State funds up to three years rather than reimburse the Office at least every six months in accordance with contract provisions. Also, our finding and recommendation address $446,000 in recoupments related to "IV-D" cases only. This section does not include any issues related to "non-IV-D" cases.

Chapter 5

Administrative Funds for the Child Support Enforcement Program Are Spent in Accordance with State Restrictions

The Office's administrative expenses for operating its child support enforcement program are reasonable and conform to state restrictions. We tested a random statistical sample of administrative expenses and determined that all expenditures tested were allowable, reasonable, and in compliance with statute.

We compared appropriated with actual expenditures for fiscal years 2001–2003 and determined that the Office spends appropriated funds within its limits. For example, for appropriation year 2002, the Office was appropriated approximately $228 million and spent approximately $225 million. The Office has carryover authority, which means the $3 million difference can be spent over the next two years (see Table 1).

Table 1

Comparison of Appropriated Funds with Actual Expenditures by Appropriation Year

State Funding	Appropriation Year 2002	Appropriation Year 2003
State Disbursement Unit	$ 26,433,239	$ 21,307,035
Child Support Orders	197,193,686	191,240,979
Total Appropriated (Excluding Special Riders)	$ 223,626,925	$ 212,548,014
Appropriation Adjustments	$ 4,383,723	$ 52,380,908[a]
Total Adjusted State Funding	$ 228,010,648	$ 264,928,922
Total Expenditures	**$ 224,544,732**	**$ 238,361,375**
Difference Between Appropriation and Expenditures	**$ (3,465,916)**	**$ (26,567,547)**

[a] This amount consists of adjustments made in several appropriations act riders, including one that allowed the Office to carry forward $36 million from appropriation year 2002 to appropriation year 2003 (Rider 12).

Sources: Appropriation information, including adjustments, comes from the General Appropriations Act, 77th Legislature. Expenditure data come from the Office of the Attorney General.

Chapter 6

Quality Control Reviews Reduce the Risk that Applications Will Be Entered Inaccurately or Not Processed in a Timely Manner

The quality control review process and other controls should reasonably ensure that applications for child support enforcement services are entered into TxCSES and processed accurately and in a timely manner. We base this assessment on interviews with regional office management and our observation of a case analyst's work. Because we determined that the risk in this area is low, we did not perform further audit tests in this area.

The regional office we observed used several key controls to help ensure accurate and timely processing of applications:

- There are multiple verifications of and sampling for data accuracy by multiple layers of staff.
- The regional office samples a large percentage of the entire population of both case initiations and order entry for testing.
- The timeliness of application processing is verified when the analyst reviews the court order entries.
- The analyst compares data entered at the field offices with actual documents.

In addition, the eight regions that process applications take the following quality control steps:

- A case analyst takes a random sample of applications and reviews them to ensure the accuracy and timeliness of the information. This sample is a random, statistically valid sample that exceeds the parameters for testing at a 99 percent confidence level.
- The analyst ensures that addresses on the system are complete, that each case is properly classified, and that all necessary documents have been obtained.
- Each analyst also receives a sample every day to test accuracy of court order data entry. The analyst compares the information in TxCSES with the hard copy documents to ensure data integrity using 39 test attributes and verifies that the names, numbers, dates, amounts, payments, medical support, and all other orders are accurate. Several of these attributes involve calculating the number of days between certain activities to ensure timeliness of case processing.
- Test results are tracked automatically using the IDEAS tracking system. Management is able to query this system and create various reports to determine performance at the regional level and at the field office level.
- Each week, the Program Specialist in the Office's Field Operations Division pulls a random sample for that day from each analyst's work to re-review and ensure analyst accuracy.

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Office of the Attorney General (Office) is administering the Child Support Program so that child support payments are disbursed to custodial parents in a timely manner.

We focused on answering the questions:

- Are payments distributed accurately and in a timely manner?
- Does the Office effectively manage its State Disbursement Unit (SDU) contract to ensure that services are delivered according to contract terms?
- Are major information technology (IT) interfaces for systems related to child support operating in a manner that ensures complete and accurate data transfer?
- Is the Office administering the Child Support Program so that funds are spent as intended?
- Are applications and claims processed accurately and in a timely manner?

Scope

Our scope included reviewing the Office's Contract Monitoring Division's work covering the period from September 1, 2001, to August 31, 2002. We reviewed the most current reconciliation for the balance and reconciliation test.

We reviewed back-end transactions (suspense items, returned warrants, and abandoned property) for the Payment Processing section and SDU Operations Division for September 1, 2001, through August 31, 2003.

We also reviewed the annual financial reports and supporting schedules for fiscal years 2001–2002 during the course of this audit. We additionally tested administrative expenditures to determine whether they were allowable, reasonable, and in compliance with requirements.

We visited counties (Tarrant, Dallas, and Harris) and reviewed the access controls on county systems maintaining child support data as well as their data preparation, submittal, and retrieval procedures for child support information.

Methodology

The methodology used on this audit consisted of obtaining and reviewing procedures and data, conducting random sample tests, and analyzing and evaluating data and test results.

Information obtained, reviewed, tested, and analyzed included the following (see the following four bullets for methodology used):

- Interviews with Office management and staff
- Walk-through and mapping of the payment process at the SDU
- Process maps of other areas within the Office's Child Support Division
- Documentary and analytical evidence such as:
  - Current SDU contract
  - Review of contract monitoring methodology
  - Tests of 40 randomly selected collections and payments processed by the SDU
  - Tests of five months' worth of invoices submitted by the SDU
  - Tests of 30 randomly selected returned warrants in the vault as of the end of fiscal year 2003
  - Test of 30 randomly selected suspense transactions as of the end of fiscal year 2003
  - Review of fiscal years 2001, 2002, and 2003 suspense reports for accuracy
  - Comparison of fiscal year 2001 through 2003 data from the Office and from the SDU
  - Review of reporting policies and procedures related to abandoned property
  - Review and tests of current access lists for payment processing areas, including the vault
  - Observation of the quality control review process over child support applications and observation of a case analyst's work related to applications and claims processing
  - Tests of 30 randomly selected expenditure transactions from fiscal years 2001–2003 for reasonableness, compliance, and allowability
  - Review of Annual Financial Reports and supporting schedules from fiscal year 2001 to fiscal year 2002
  - Review of Texas Child Support Enforcement System (TxCSES) and Stradus access lists of users with edit access
  - Tests of TxCSES's and Stradus's monthly reconciliation process and county data exchange processes

Project Information

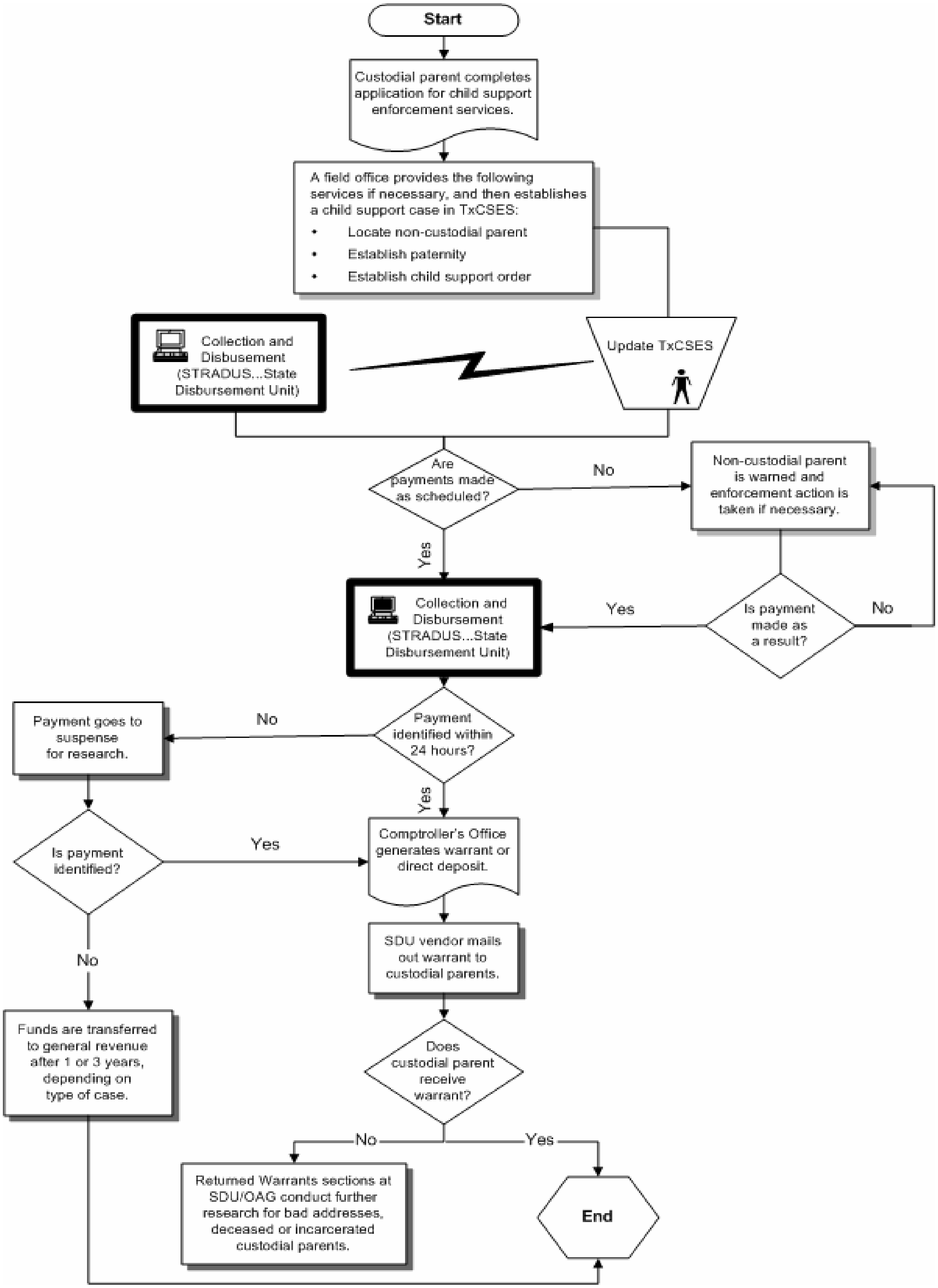
The audit was conducted in accordance with applicable professional standards, including generally accepted government auditing standards. We conducted fieldwork from July 2003 through January 2004.

The following members of the State Auditor’s staff conducted this audit:

- Nicole J. Merridth-Marrero, MBA (Project Manager)
- Courtney Ambres-Wade (Assistant Project Manager)
- Dinah Arce, CPA
- Cara Hardy
- C.Y. Ihekwoaba, CPA
- Cesar Saldivar
- Serra Tamur, MPAff, CIA, CISA
- Rebecca Tatarski
- Jennifer Wiederhold
- Lisa R. Collier, CPA (Quality Control Reviewer)
- J. Scott Killingsworth, CIA (Quality Control Reviewer)
- Sandra Vice, CIA, CGAP(Audit Manager)
- Frank Vito, CPA (Audit Director)

Appendix 2

Flowchart of the Child Support Enforcement Process


Start
Custodial parent completes application for child support enforcement services.
A field office provides the following services if necessary, and then establishes a child support case in TxCSES:
• Locate non-custodial parent
• Establish paternity
• Establish child support order
Collection and Disbusement (STRADUS...State Disbursement Unit)
Update TxCSES
Are payments made as scheduled?
No
Non-custodial parent is warned and enforcement action is taken if necessary.
Yes
Collection and Disbusement (STRADUS...State Disbursement Unit)
Yes
Is payment made as a result?
No
Payment goes to suspense for research.
No
Payment identified within 24 hours?
Yes
Is payment identified?
Yes
Comptroller's Office generates warrant or direct deposit.
SDU vendor mails out warrant to custodial parents.
No
Funds are transferred to general revenue after 1 or 3 years, depending on type of case.
Does custodial parent receive warrant?
No
Yes
Returned Warrants sections at SDU/OAG conduct further research for bad addresses, deceased or incarcerated custodial parents.
End

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Talmadge Heflin, House Appropriations Committee
The Honorable Ron Wilson, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Office of the Attorney General

The Honorable Greg Abbott, Attorney General
Mr. Barry McBee, First Assistant Attorney General

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact Production Services at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.