Audit Report

Department of Juvenile Services

July 2007

OFFICE OF LEGISLATIVE AUDITS

DEPARTMENT OF LEGISLATIVE SERVICES

MARYLAND GENERAL ASSEMBLY

- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.

- Electronic copies of our audit reports can be viewed or downloaded from our website at http://www.ola.state.md.us.

- Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.

- The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410- 946-5400 or 301-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

July 11, 2007

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Nathaniel J. McFadden, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Department of Juvenile Services (DJS) for the period beginning November 1, 2002 and ending July 31, 2006.

Our audit disclosed that DJS needs to continue its efforts with the Judiciary to ensure that court decisions, such as court orders, relating to the removal of youths from their homes and their subsequent placement, meet all federal requirements for the recovery of federal Title IV-E revenue. DJS estimated that insufficient legal language in court orders contributed to a reduction of more than $2 million in its federal claims for eligible youths between fiscal years 2005 and 2006. Furthermore, additional federal revenue totaling approximately $100,000 was potentially lost because eligibility determinations were not always prepared for youths in a timely manner.

We also noted numerous internal control and record keeping deficiencies with respect to cash receipts, accounts receivable, corporate purchasing cards, disbursement transactions, information systems security and control, payroll, and property. Many of these findings have been included in several of our preceding audit reports, some since 1989.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

* **Denotes item repeated in full or part from preceding audit report**

Executive Summary

Legislative Audit Report on the Department of Juvenile Services
July 2007

- **DJS needs to continue to work with the Judiciary to ensure that court decision language regarding the removal of youths from the their homes and their subsequent placement meets all federal requirements for the recovery of federal Title IV-E revenue. DJS estimated that insufficient legal language in court orders contributed to a reduction of over $2 million in certain Title IV-E claims by DJS between fiscal years 2005 and 2006. Furthermore, additional federal revenues may have been lost because Title IV-E eligibility determinations for youths were not always prepared in a timely manner.**

  DJS should continue its efforts to work with the Judiciary to ensure that court decision language meets all federal requirements for the recovery of Title IV-E revenue. Furthermore, all youth eligibility determinations should be prepared in a timely manner.

- **Employee access to the automated restitution accounts receivable system and the Automated Statewide Support and Information System (ASSIST) was not adequately controlled. Furthermore, recorded transactions were not always subject to supervisory review and approval. DJS uses ASSIST to help monitor and facilitate the movement and treatment of all youths entering the juvenile services system, and to verify youth placement for vendor payment purposes.**

  DJS should adequately control employee access to its automated systems, and should establish procedures to verify that only authorized transactions have been recorded.

- **The DJS information systems were not adequately secured. For example, the internal network was not properly protected from security risks, the administration and monitoring of critical network devices need improvement, and a complete disaster recovery plan was not in place.**

  DJS should take the recommended corrective actions to improve security over its information systems.

- **Certain transactions were not recorded or accounted for in accordance with requirements established by the Comptroller of the Treasury's General Accounting Division (GAD). For example, DJS recorded accrued revenue at June 30, 2006, totaling approximately $475,000, which it does not expect to collect.**

  DJS should ensure that transactions are recorded and accounted for in accordance with requirements established by GAD.

- **Numerous internal control and record keeping deficiencies were noted with respect to cash receipts, accounts receivable, corporate purchasing cards, disbursements, payroll, and property. Many of these findings have been repeated in several of our preceding audit reports, some dating back to 1989.**

  DJS should take the recommended action to improve internal controls and record keeping in these areas.

Background Information

Agency Responsibilities

The Department of Juvenile Services (DJS) is the central administrative agency for juvenile intake, detention authorization, probation, protective supervision, and aftercare services. In addition, DJS provides residential care, diagnosis, training, education, and rehabilitation to juveniles in State facilities, and supervises community facilities operated under contractual agreements. DJS responsibilities also include the collection and disbursement of restitution payments for individuals or organizations that have sustained damages caused by juvenile offenders. DJS has a headquarters office located in Baltimore City and 34 field offices located throughout the State, and has approximately 2,080 permanent and 180 contractual positions. According to DJS records, the number of youth placements under its care (including detention programs, committed programs, probation, and aftercare) during fiscal year 2006 totaled approximately 32,000. In addition, the average daily population of youths under its supervision for residential care totaled approximately 2,300 for the same period. According to the State's records, fiscal year 2006 DJS expenditures totaled approximately $208 million.

Current Status of Findings From Preceding Audit Report

Our audit included a review to determine the current status of the 17 findings contained in our preceding audit report dated September 9, 2003. We determined that DJS satisfactorily addressed 6 of these findings. The remaining 11 findings are repeated in this report, one of which is separated into two comments in this report.

Findings and Recommendations

Federal Funds

Background
DJS may obtain Title IV-E federal revenue for costs incurred when eligible youths are placed in certain out-of-home settings, such as in State-licensed foster care homes or group homes. In order to recover Title IV-E revenue, federal regulations require specific language to be included in the judicial orders and determinations (court decisions) relating to the removal of youths from their homes and their subsequent placement by DJS. This language is intended to address the requirements that reasonable efforts have been made to prevent removal of youths from their homes. Those regulations also stipulate that claims for reimbursement must be made within two years of when the eligible costs are incurred. According to DJS records, for fiscal year 2006, DJS received Title IV-E revenue totaling approximately $9.4 million.

Finding 1
DJS needs to continue its efforts with the Judiciary to ensure that individual court decisions contain the requisite language necessary to enable the State to recover Title IV-E funding.

Analysis
Based on the results of a federal review of the State's Title IV-E program, conducted in 2005 at the Maryland Department of Human Resources, DJS determined that it was unable to claim Title IV-E funding for many youths in its care, even though all eligibility requirements had been met, because the related court decisions (such as court orders) for the removal of the youths from their homes did not meet specific federal language requirements. For example, when applicable, the court orders must state that it is contrary to the welfare of the juvenile to remain in his/her home and that reasonable efforts have been made to prevent the juvenile's removal from the home. DJS determined that insufficient legal language contributed to a reduction of over $2 million in Title IV-E claims for youths' room and board costs between fiscal years 2005 and 2006.

DJS has noted that it does not control the judicial process, but that it has been actively working with the Judiciary to resolve this issue. For example, in a September 2006 letter from the Secretary of DJS to the Chief Judge of the Maryland Court of Appeals, the Secretary noted a tightening of federal requirements regarding the form and content of court orders for the removal of youths from their homes, and requested assistance in ensuring that all orders issued by the court meet these requirements. We were advised by DJS management that, while improvement has been noted in some jurisdictions throughout the State, other jurisdictions continue to issue court decisions without the required federal language. We believe that it is imperative that DJS continue its efforts to work with the Judiciary to help ensure that court decisions meet all federal requirements for Title IV-E eligibility.

Recommendation 1
We recommend that DJS continue its efforts to work with the Judiciary to ensure that court decisions contain the federally-required language to facilitate the recovery of Title IV-E revenue.

Finding 2
Title IV-E eligibility determinations were not always completed promptly, potentially resulting in a loss of federal revenue to the State.

Analysis
At our request, as of January 23, 2007, DJS identified 187 youth placements for which Title IV-E eligibility determinations had not been completed within the two-year requirement. Although not all of these placements would necessarily be eligible for federal reimbursement, because eligibility determinations were not completed timely, DJS was unable to recover costs for those that were.

Also, at our request, DJS reviewed the 187 placements and determined that 21 were in eligible out-of-home settings and, therefore, the related expenditures would have been recoverable if the applicable youths had also been determined to be Title IV-E eligible. Based on data provided by DJS regarding the percentage of incoming youths normally found to be Title IV-E eligible, we estimated that DJS could have recovered federal reimbursements totaling approximately $100,000 relating to these 21 placements if eligibility determinations had been made timely. However, without conducting eligibility determinations for all youths, it is not possible to know exactly how much could have been recovered. Our tests of the data used by DJS to identify the 187 youth placements and the related expenditures determined that it was reliable. A similar condition was commented upon in our two preceding audit reports.

Recommendation 2
We again recommend that, in the future, DJS ensure that federal Title IV-E program eligibility determinations and requests for reimbursement of

eligible costs are processed for all youth placements in a timely manner. In addition, we again recommend that, for all youth placements and vendor payments already made, DJS identify any eligible and reimbursable payments for which available Title IV-E funding has previously gone unclaimed, and seek recovery to the extent permitted by federal regulations.

Cash Receipts

Finding 3
Procedures for controlling and accounting for collections at two locations were not sufficient.

Analysis
Procedures at two locations were not sufficient to ensure that collections were adequately controlled and accounted for. Specifically, we noted the following conditions:

- Although the DJS headquarters location had established a procedure to independently verify recorded collections to deposit, the verification was not being performed. Our test of 15 deposits, totaling approximately $256,000, disclosed a lack of verification for 14 of the deposits, totaling approximately $224,000. According to DJS records, collections received and initially recorded directly at headquarters during fiscal year 2006 totaled approximately $839,000.

- Collections initially received in the DJS lockbox account which, according to DJS records, totaled approximately $786,000 during fiscal year 2006, were not transferred to the State's depository account in a timely manner. For example, over the first five months of calendar year 2006 only two transfers were made to the State's account: approximately $83,600 on February 10, 2006, and approximately $222,800 on May 1, 2006. We were advised by the State Treasurer's Office that transfers should be made daily. The lack of timely transfers reduces State accountability over the funds, and results in lost interest since funds in the lockbox account do not earn interest for the State.

  In addition, the DJS record of restitution lockbox account activity had not been reconciled to periodic statements received from the bank since March 2003. As of June 30, 2006, the lockbox account balance on the DJS records (approximately $169,000) exceeded the bank's records (approximately $139,000) by $30,000.

- The employee who verified that all Western Region collections initially recorded on prenumbered receipt forms agreed with deposit documentation received from the bank could also receive collections and prepare the related deposit when the employees who normally performed these duties were absent. This employee also had access to the safe where collections were maintained overnight. Furthermore, although this employee verified the numerical sequence of pre-numbered cash receipt forms used on a day-to-day basis, a complete accounting of the forms issued, voided, and still on hand (unused) was not performed on a periodic basis. Under these conditions, errors or other discrepancies could occur without timely detection. According to DJS records, collections received in the Western Region totaled approximately $122,000 in fiscal year 2006.

Recommendation 3
We recommend that an employee without access to collections verify that all recorded collections were subsequently deposited. We also recommend that DJS transfer funds from its lockbox account to the State's bank account in a timely manner. Specifically, we recommend that DJS contact the State Treasurer's Office to determine the appropriate transfer schedule. In addition, we recommend that DJS periodically reconcile its records of lockbox activity with corresponding records maintained by the bank. Finally, we recommend that a complete independent accounting of pre-numbered cash receipt forms as to issued, voided, and on hand be performed on a periodic basis, such as quarterly. We advised DJS on accomplishing the necessary separation of duties using existing personnel.

Accounts Receivable

Background
DJS processes two types of accounts receivable: restitution amounts due from juvenile offenders or their guardians, and non-restitution amounts such as amounts resulting from audits of contracts with private vendors. Restitution payments collected by DJS are subsequently forwarded to the applicable individuals or organizations that have sustained damages by the juvenile offenders. Separate automated systems are maintained for restitution and non-restitution receivables. As of August 10, 2006, there were approximately 17,500 restitution accounts totaling approximately $8.8 million. The total value of non-restitution accounts receivable approximated $2.4 million as of June 30, 2006.

Finding 4
Adequate internal controls and record keeping procedures had not been established for accounts receivable.

Analysis
Controls and record keeping procedures for both restitution and non-restitution accounts receivable were not sufficient. Specifically, we noted the following conditions:

- DJS did not verify that non-cash credit adjustments (approximately $242,000 in fiscal year 2006) recorded in the automated restitution system had been properly approved. Although the system was capable of generating output reports of adjustments made, the reports were not being generated and used to verify that only authorized adjustments had been recorded.

- The employee who initially received non-restitution account payments also prepared and mailed account billings, initially recorded billings in the automated accounts receivable records, and provided a copy of the payments to another employee for posting in the receivable records. Under these conditions, errors or other discrepancies could occur without timely detection.

- The control account for non-restitution receivables was not maintained on a current basis. As of June 30, 2006, the control account had not been updated since May 2004. Proper maintenance of the control account, and periodic reconciliation of the account to the related detail records, would help to ensure the accuracy and completeness of the accounts receivable records.

- The Department did not always record non-restitution account payments in the detail accounts receivable records and, consequently, the records did not always reflect accurate account balances. For example, our review of documentation relating to 10 accounts, with balances totaling approximately $220,000, disclosed that 3 account payments, totaling approximately $85,000, had been received in fiscal year 2004, but were never posted to the detail records.

- DJS had not reconciled its record of certain restitution account activity with the corresponding balance on the State Comptroller's records since January 1997. As of September 8, 2006, the balance of the unmatched payments fund on the Comptroller's records (approximately $1,241,000) exceeded the fund balance on DJS records (approximately $127,000) by $1,114,000. Unmatched payments are payments that cannot be immediately identified to a specific case. DJS explained that the vast majority of this difference occurred because the Comptroller's balance included financial activity unrelated to restitution; however, a formal reconciliation had not been performed.

Similar comments regarding non-cash credit adjustments and incompatible employee duties have been included in our two preceding audit reports, and comments regarding the lack of an adequate control account have been included in our reports dating back to 1989. A lack of critical reconciliations was commented upon in our preceding audit report.

Recommendation 4
To improve internal controls and record keeping for accounts receivable we again recommend that non-cash credit adjustments recorded in the restitution system be verified, at least on a test basis, to approved supporting documentation by personnel independent of the adjustment preparation and recording functions, and that these verifications be documented. We also again recommend that employees who process non-restitution billings not have access to related collections. We further again recommend that the non-restitution control and detail records be properly maintained and periodically reconciled. Finally, we again recommend that DJS periodically conduct reconciliations of critical restitution records with corresponding records maintained by the State Comptroller. We advised DJS on accomplishing the necessary separation of duties using existing personnel.

Finding 5
DJS did not always comply with certain regulations and provisions of the law relating to the collection of delinquent accounts.

Analysis
Collection procedures for delinquent restitution and non-restitution accounts were not sufficient. Specifically, overdue payment notices were not always sent to debtors, and delinquent accounts were not being forwarded to the Department of

Budget and Management's Central Collection Unit (CCU) as required. Furthermore, DJS did not always inform the court of delinquent restitution accounts as required.

- Our review of 10 delinquent non-restitution accounts, totaling approximately $193,000, disclosed that, for 7 of the accounts, with initial billing dates that ranged from September 2002 through November 2003, no requests for payment had been made after the initial billings. Furthermore, as of June 30, 2006, there were approximately 100 non-restitution accounts, totaling approximately $700,000 that, according to DJS records, had been outstanding for over 19 months but had not been referred to CCU.

  CCU regulations generally require that three written demands for payment be made on accounts at 30-day intervals and that outstanding accounts that remain uncollected after the third written demand for payment be transferred to CCU for further collection activity. Comments regarding a lack of compliance with CCU regulations for non-restitution accounts have been included in our audit reports since 1995.

- Our examination of 8 unpaid overdue restitution accounts (totaling approximately $28,000) disclosed 4 accounts totaling $9,900 which were overdue from 5 to 37 months as of September 11, 2006, that had not been referred to the court. None of the accounts we examined had been forwarded to CCU.

State law stipulates that DJS will notify the court when an obligor's restitution payment is overdue. In addition, DJS written procedures stipulate that, absent a revised court order, delinquent accounts should be forwarded to CCU.

Recommendation 5
We again recommend that DJS comply with CCU regulations. Furthermore, we recommend that DJS notify the court of delinquent restitution accounts as required by State law.

Corporate Purchasing Cards

Finding 6
Controls over the issuance of corporate purchasing cards were not adequate, and certain required documentation was not always maintained.

Analysis
Controls over the issuance of corporate purchasing cards were not adequate, and certain required documentation was not always maintained. Consequently, there was a lack of assurance that all purchasing card transactions were authorized and valid. According to the State's records, during fiscal year 2006, DJS purchasing card expenditures totaled approximately $1.1 million, and DJS had about 60 cards issued. Specifically, we noted the following conditions:

- The employee designated as the DJS Purchasing Card Program Administrator (PCPA) was responsible for completing online applications to obtain cards from the card vendor (bank), for receiving the cards from the bank, and for giving the cards to another employee for distribution to the applicable DJS employees. Consequently, cards could be inappropriately issued and unauthorized purchases could be made without timely detection.

- Our test of 15 corporate cardholder agreements disclosed that, although 14 of the agreements were approved by the DJS program administrator, 6 were not authorized by the DJS fiscal officer, and 5 of these 6 were not approved by the employees' immediate supervisors. All three approvals are required by the Comptroller of the Treasury's Corporate Purchasing Card Program Policy and Procedures Manual. A similar condition was commented upon in our preceding audit report. Cardholder agreements stipulate each cardholder's request for a card, as well as his or her assurance that it will be used only for approved purchases. The cardholder also agrees that all purchasing card policies and procedures will be complied with.

- Our test of 25 purchasing card transactions, totaling approximately $23,000, disclosed 3 transactions, totaling $3,600, for which receipts were not on file to support the purchases. We noted a fourth transaction for which no documentation could be located, including receipts and the corresponding monthly activity log.

The Comptroller of the Treasury's *Corporate Purchasing Card Program Policy and Procedures Manual* states that the employee who receives purchasing cards from the bank should not be the agency PCPA (the employee who orders the cards from the bank). The *Manual* also specifies requirements for preparing and approving cardholder agreements, and for properly maintaining documentation, including transaction receipts and monthly activity logs.

Recommendation 6
We recommend that DJS comply with the requirements of the *Corporate Purchasing Card Program Policy and Procedures Manual*. Specifically, we recommend that the employee who orders cards from the bank not be responsible for receiving and distributing the cards in any manner, and that the employee who receives the cards verify, prior to distribution, that the cards have been authorized in accordance with the *Manual*. We also again recommend that cardholder agreements be approved as required. In addition, we recommend that all documentation required to support purchasing card transactions be maintained. Finally, we recommend that DJS review the propriety of the agreements and transactions with missing documentation noted above.

Disbursement Transactions

Finding 7
Proper internal controls were not established over critical functions on the State's Financial Management Information System.

Analysis
DJS did not fully use the security features available on the State's Financial Management Information System (FMIS) to establish proper internal controls. Specifically, four employees had the capability to initiate, process, and release disbursement transactions to the Comptroller of the Treasury – General Accounting Division for payment. As a result, unauthorized transactions could be processed which may not be readily detected. During fiscal year 2006, DJS processed disbursements totaling approximately $79 million. A similar condition was commented upon in our preceding audit report.

Furthermore, DJS did not regularly review reports of FMIS access privileges (profiles) granted to its employees to help ensure that control deficiencies, such as that noted above, do not occur, and that critical access to FMIS is granted only to current employees who need it for their job responsibilities. As of September 2006, the last review of access profiles performed by DJS was as of November 2004. The *FMIS Internal Control and Security Policy and Procedures*, issued by Department of Budget and Management, requires agencies to review these reports to ensure that FMIS access profiles are accurate and are appropriate to ensure a proper separation of duties and adequate internal approvals. In addition, agencies are required to document such reviews for future audit verification.

Recommendation 7
We again recommend that DJS fully use the available FMIS security features by establishing independent approval requirements for all disbursement transactions. Specifically, we recommend that employees who have the capability to initiate and process disbursement transactions on FMIS not have the capability to release these transactions for payment. We also recommend that DJS regularly review FMIS security reports to ensure the accuracy and propriety of employee access profiles. Furthermore, we recommend that DJS document such reviews.

Access to Critical Data

Finding 8
Employee access to critical automated systems was not adequately controlled.

Analysis
Employee access to the automated restitution accounts receivable system and the system used to monitor juvenile activity, the Automated Statewide Support and Information System (ASSIST), was not adequately controlled.

For example, 10 employees were granted access that allowed them to add and update case data (including the party receiving restitution) on the restitution accounts receivable system, as well as to post unmatched payments to individual accounts. One of these employees could also record non-cash credits on the system. Furthermore, these transactions could be processed without supervisory review and approval. Unmatched payments are payments that, for certain reasons, cannot be immediately identified to a specific case. By posting such payments to a case, a payment to the specified victim will be processed. Therefore, employees who can establish or update case data on the system or record non-cash credits should not be able to post unmatched payments.

We also noted eight employees who were granted access privileges to establish youth data, change existing data, and add a vendor to ASSIST without supervisory review and approval. DJS uses ASSIST to help monitor and facilitate the movement and treatment of all youths entering the juvenile services system, and to verify youth placement for vendor payment purposes. Consequently, it is imperative that DJS ensure the propriety of all critical system data by ensuring that all additions and changes are subject to supervisory review and approval. DJS advised us that there are approximately 8,000 active cases currently on ASSIST.

The fact that an employee could record non-cash credits on the restitution system, establish restitution accounts, and initiate disbursements from the accounts was also commented upon in our preceding audit report.

Recommendation 8
We again recommend that DJS restrict access so that employees who can establish or adjust case data on the restitution system not have the capability to post and initiate payments on the system. Furthermore, we recommend that procedures be established to verify, at least on a test basis, that all critical transactions posted to the restitution system and ASSIST are valid.

Information Systems Security and Control

Background
The DJS Office of Information Technology (OIT) provides information technology services to all units of DJS. The OIT staff operates and maintains the DJS internal network and critical applications, including its youth tracking system (ASSIST) and expenditure tracking system (Cost Management) that is used to recover federal funds. In addition, OIT provides DJS with Internet connectivity, and operates and maintains the Department’s website and email system.

Finding 9
The internal network was not properly protected from security risks.

Analysis
The internal network, which hosts critical applications, databases, email and network support servers, was not properly protected from security risks. Specifically, we noted the following conditions:

- Firewall rules were not configured to adequately protect the DJS internal network from external untrusted networks. Accordingly, the DJS network was unnecessarily exposed to attack, which could result in a loss of data integrity, the destruction of critical files, and the interruption of services. A similar condition was commented upon in our preceding audit report.

- Several untrusted third parties had direct connections to the DJS internal network, and resulting traffic was not filtered by any DJS network devices (for example, a firewall). Accordingly, these untrusted third parties could access all servers and workstations on the DJS internal network. A similar condition was commented upon in our preceding audit report.

- IDP (intrusion detection prevention) systems were not used to protect critical portions of the network. We were advised by DJS personnel that the firewall was providing IDP protection; however, the firewall did not have IDP features installed. IDP systems gather and analyze network traffic to identify and block network security breaches and attacks, and alert network administrators of these situations.

- Three critical publicly accessible servers were located on the internal network rather than in a separate network zone to minimize security risks. These servers, which could potentially be compromised, exposed the internal network to attack from external sources.

Recommendation 9
We recommend that DJS improve security over its internal network. Specifically, we made detailed recommendations, which if implemented, should provide for adequate security over the internal network.

Finding 10
Administration and monitoring of critical network devices need improvement.

Analysis
Administration and monitoring of the critical network devices, capable of protecting the internal network from security risks, need improvement. Specifically, we noted the following conditions with respect to the firewalls and core network device:

- Numerous individuals had unnecessary administrative access to these devices and an insecure connection protocol was enabled on these devices for administration purposes. Access rules for critical network devices should use a “least privilege” security strategy which gives individuals only those privileges needed to perform assigned tasks.

- Logs were stored on these devices and were not recorded on a separate logging server. Log files stored on the device itself are overwritten when filled, resulting in lost logging information. Additionally, because the log files were stored on the device, they were not adequately safeguarded from alteration or deletion. A similar condition was commented upon in our prior audit report.

- Administrators did not regularly review the logs for these devices. A similar condition was commented upon in our prior audit report. In addition, no documentation of reviews performed was retained.

Recommendation 10
We recommend that administrative access to critical network devices be limited to personnel requiring such access and that only secure connection protocols be enabled on these devices. We further again recommend that log files for critical network devices be recorded on a separate logging server, and that these logs be reviewed on a daily basis. Finally, we recommend that these reviews be documented and retained for audit verification.

Finding 11
DJS did not adequately secure its web access to two sensitive applications.

Analysis
DJS did not adequately secure access to its web-enabled email, which included sensitive youth information and its incident reporting database. For example, DJS allowed employees to remotely access their email by an Internet link on the DJS website. Employees using web-enabled email would authenticate to the DJS network (using accounts and passwords) and transmit both user authentication information and the email messages in an unencrypted (plaintext) format. Unencrypted communications are subject to being intercepted and read by unauthorized individuals. Accordingly, the potential existed for improper disclosure of confidential employee network accounts, passwords, email, and incident reports. Methods exist to provide secured encrypted connections for these connections. The Department of Budget and Management (DBM) *Information Technology Security Policy and Standards* requires State agencies ensure that

encryption is used to protect any nonpublic information when it is stored or transmitted through any environment. This same condition regarding email was commented upon in our prior audit report.

Recommendation 11
We again recommend that communications between remote users and sensitive web-enabled systems be encrypted.

Finding 12
Network and database accounts and related passwords were not adequately controlled, and certain system activities were not monitored.

Analysis
Security features involving network and database accounts and passwords, and monitoring activities for a critical system and database were not adequate to protect various network resources and critical applications. Specifically, we noted the following conditions:

- Network passwords had no minimum password length or complexity requirements and never expired. In addition, for a critical database, we noted 83 identical accounts and passwords that existed on both the production and non-production version of the database.

- Numerous personnel had unnecessary administrator status on a critical network server which allowed them full control over many critical network devices. In addition, a factory-installed user account was not properly renamed on two critical servers.

- Audit features were not properly enabled for a critical network server tested and database auditing was not enabled for a critical database. As a result, most security-related events were not logged or monitored on this server and database.

Similar conditions regarding passwords, accounts, and monitoring critical systems were commented upon in our preceding audit report. The DBM *Information Technology Security Policy and Standards* establishes minimum password, user account, and security monitoring procedures for State agencies.

Recommendation 12
We recommend that DJS comply with the account, password, and monitoring provisions of the DBM *Information Technology Security Policy and Standards*.

Finding 13
DJS did not have a complete information technology disaster recovery plan.

Analysis
DJS did not have a complete information technology disaster recovery plan (DRP) for recovering from disaster scenarios (for example, a fire). In accordance with the DBM *IT Disaster Recovery Guidelines*, dated July 2006, a complete information systems disaster recovery plan should, at a minimum, address the following requirements:

- DRP overview, which should include plan purpose and objectives, organization applicability, scope provisions for various situations and conditions and record of changes
- Concept of operations, which should include system descriptions, detailed roles and responsibilities of both the disaster teams and the recovery teams, and line of succession
- Notification and activation, which should include notification procedures, damage assessment, and plan activation
- Recovery strategies, including consideration of alternate sites, equipment replacement, restoration of network connectivity, and prioritization of systems/applications for recovery
- Reconstitution procedures needed to transition back to normal operations once the original or replacement system is ready to resume normal operations

Without a formal information technology disaster recovery plan, a disaster could cause significant delays (for an undetermined period of time) in restoring operations above and beyond the expected delays that would exist in a planned recovery scenario. A similar condition was commented upon in our prior report.

Recommendation 13
We again recommend that, in accordance with the aforementioned *IT Disaster Recovery Guidelines*, DJS develop and implement a comprehensive information systems disaster recovery plan that covers all DJS critical

functions. We also recommend that, at a minimum, the plan address the required items noted above.

Payroll

Finding 14 **Critical documents were not adequately reviewed and there was a lack of control over procedures for removing employees from the payroll.**

Analysis
Certain controls over the DJS payroll, which totaled approximately $118 million during fiscal year 2006, were inadequate. Specifically, the employee who approved time reports for several locations and submitted them electronically to the Central Payroll Bureau for processing did not compare the entries on the reports to supporting documentation, such as approved timesheets documenting overtime. Without conducting such a comparison, there was a lack of assurance that critical entries on the reports, which serve as the basis for adjustments to employee wage payments, were valid and accurate.

Furthermore, the employee responsible for preparing and submitting required documentation to remove employees from the payroll for two locations, also received and distributed the related payroll checks. As a result, unauthorized payroll payments could be processed without detection.

Recommendation 14
We recommend that employees responsible for approving time reports compare entries on the reports to approved supporting documentation, at least on a test basis, prior to releasing the reports to the Central Payroll Bureau, and that this approval be documented. We also recommend that employees responsible for processing documentation to remove employees from the payroll be denied access to payroll checks.

Property

Finding 15
Physical inventories of equipment were not conducted at required intervals and record keeping for property was deficient.

Analysis
DJS did not adequately account for its property. In particular, physical inventory and record keeping procedures were inadequate and were not in accordance with the Department of General Services (DGS) *Inventory Control Manual*. As of June 30, 2006, the book value of DJS property, as reported on the State's records, totaled approximately $122.9 million (buildings - $87.6 million, construction in progress - $27.5 million, land and improvements - $3.6 million, and equipment - $4.2 million). However, based on our findings, we question the accuracy of these values. Our audit disclosed the following conditions:

- Physical inventories were not completed as required. As of June 2006, DJS had not conducted a complete physical inventory of all sensitive and non-sensitive equipment, including a reconciliation to detail records, since 1993. The Manual requires that State agencies conduct a complete physical inventory of sensitive equipment items at least once every year and of non-sensitive equipment items at least once every three years.

- Equipment records were not maintained on a current basis and an equipment control account was not being maintained, as required. As a result, the records could not be used to effectively control equipment. Our test of 10 equipment purchases, totaling approximately $238,000, disclosed 3 purchases, totaling approximately $48,000, that had not been recorded in the detail equipment records even though the purchases were made at least seven months prior to our test. In addition, DJS was unable to physically locate equipment associated with 5 of the 10 purchases, including the 3 unrecorded purchases.

- Detail records and/or control accounts were not maintained at all for land, buildings, and construction in progress, as required.

- DJS did not report the value of its property to DGS for fiscal years 2003 through 2006, as required.

- Certain equipment went untagged for extended periods of time. The *Manual* requires that equipment items be tagged for identification and control purposes. According to DJS records, as of June 2006, there were approximately 280 untagged computer units located in a storeroom which had been purchased a year earlier in July 2005 at a cost of approximately $156,000.

Similar deficiencies relating to record maintenance and physical inventories have been commented upon in our proceeding audit reports dating back as far as 1989.

Recommendation 15
We again recommend that DJS comply with the requirements of the DGS *Inventory Control Manual*. In addition, we recommend that DJS take immediate action to locate the five aforementioned missing purchases, and to tag all equipment on hand.

Revenue Transactions

Finding 16
Certain transactions were not recorded or accounted for in accordance with General Accounting Division requirements.

Analysis
Certain transactions were not recorded in accordance with requirements established by the Comptroller of the Treasury's General Accounting Division (GAD). Specifically, we noted the following two conditions:

- DJS recorded accrued revenue at June 30, 2006 totaling approximately $475,000 which it does not anticipate collecting. These funds represent unreimbursed costs associated with an agreement DJS had with a local jurisdiction (county) to pay certain expenditures related to an out-of-home placement program operated by the jurisdiction. DJS was to be reimbursed through a State appropriation budgeted with another State agency. We were advised that the agreement ended in June 2003 and, although DJS had recouped the majority of costs incurred for this program, it will be unable to recoup the aforementioned amount. Nevertheless, DJS recorded these unreimbursed costs as accrued revenue even though GAD procedures stipulate that accrued revenues should be recognized when they are collectible within 60 days of the end of the fiscal year.

- DJS recorded telephone and vending machine commissions totaling approximately $186,000 as special funds, and carried these funds forward from fiscal year 2006 to fiscal year 2007. However, GAD's *Accounting Procedures Manual* requires State agencies to deposit commissions from public telephones and vending machines as General Fund revenue unless approval is obtained from the Board of Public Works (BPW) to apply such funds otherwise. DJS advised us that it had received BPW approval to apply the funds as special funds and to carry these funds forward from one year to the next; however, DJS did not have documentation of this approval.

Recommendation 16
We recommend that DJS refrain from recording accrued revenue which it does not anticipate collecting. We also recommend that DJS contact the Department of Budget and Management and GAD to determine the appropriate action to take to properly account for and resolve these unreimbursed costs. We also recommend that DJS deposit telephone and vending machine commissions, including the aforementioned $186,000, to the General Fund as required, unless documented approval is obtained from BPW to apply such funds otherwise.

Audit Scope, Objectives, and Methodology

We have audited the Department of Juvenile Services (DJS) for the period beginning November 1, 2002 and ending July 31, 2006. The audit was conducted in accordance with generally accepted government auditing standards.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine DJS financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the current status of the findings contained in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DJS operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

DJS provides support services (such as payroll and purchasing) to the following budgetary units: Maryland Youth Residence Center, William Donald Schaefer House, J. DeWeese Carter Center, Cheltenham Youth Facility, Alfred D. Noyes Children's Center, Thomas J. S. Waxter Children's Center, Baltimore City Juvenile Justice Center, Charles H. Hickey, Jr. School, and Lower Eastern Shore Children's Center. Since these support services represent the major part of our audit effort with respect to the activities of these units, the units were included in the scope of this audit.

Our audit scope was limited with respect to DJS's cash transactions because the Office of the State Treasurer was unable to reconcile the State's main bank accounts during the audit period. Due to this condition, we were unable to determine, with reasonable assurance, that all DJS cash transactions were accounted for and properly recorded on the related State accounting records as well as the banks' records.

DJS management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect DJS's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes conditions regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to DJS that did not warrant inclusion in this report.

The DJS response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the Office regarding the results of our review of its response.

APPENDIX

MARYLAND
Department of Juvenile Services
Together... Reshaping Young Lives Together... Reshaping Young Lives

DEPARTMENT OF JUVENILE SERVICES
One Center Plaza
120 West Fayette Street
Baltimore, Maryland 21201

Martin O'Malley
Governor

Anthony G. Brown
Lt. Governor

Donald W. DeVore
Secretary

July 6, 2007

Bruce A. Myers, CPA, Legislative Auditor
Office of Legislative Audits
301 W. Preston St., #1202
Baltimore, MD 21201

Dear Mr. Myers,

I want to thank you and your audit team for your professionalism and cooperation during the audit process. Attached are the Department of Juvenile Services' (DJS') detailed responses to your findings.

DJS is in agreement with 13 of your 16 findings and recommendations. In many cases, we have already implemented the actions needed to come into compliance. There are three recommendations with which we disagree in part.

Finding 1. DJS needs to continue to work with the Judiciary to ensure that Federal Title IV-E revenue is recovered to the fullest extent possible.

DJS Response: We agree with this finding.

Finding 2. Federal revenue was potentially lost because Title IV-E eligibility determinations for youths were not timely completed.

DJS Response: We agree with this finding.

Finding 3. Procedures for controlling and accounting for collections at two locations were not sufficient.

DJS Response: We agree with this finding.

Finding 4. Adequate internal controls and record keeping procedures had not been established.

DJS Response: We agree with this finding

Finding 5. DJS did not always comply with certain regulations and provisions of the law related to the collections of delinquent accounts.

DJS Response: We agree with this finding

Finding 6.   Controls over card issuances were not sufficient and required documentation of purchases was not always on file

DJS Response: We disagree that controls are not adequate but agree that improvement is required in documentation and timely reporting.

Finding 7. Proper internal controls were not established over critical functions on the State's Financial Management Information System.

DJS Response: We agree with this finding

Finding 8. Employee access to critical automated systems was not adequately controlled.

DJS Response: We agree with this finding.

Finding 9. The internal network was not properly protected from security risks.

DJS Response: We agree in part and disagree in part with this finding.

Finding 10. Administration and monitoring of critical network devices need improvement.

DJS Response: We agree in part and disagree in part.

Finding 11. DJS did not adequately secure its web access to two sensitive applications.

DJS Response: We agree with this finding.

Finding 12. Network and database accounts and related passwords were not adequately controlled, and certain system activities were not monitored.

DJS Response: We agree with this finding.

Finding 13. DJS did not have a complete information technology disaster recovery plan.

DJS Response: We agree with this finding

Finding 14. Critical documents were not adequately reviewed and there was a lack of control over procedures used to remove employees from the payroll.

DJS Response: We agree with this finding.

Finding 15. Equipment inventories were not conducted as required and record keeping was deficient.

DJS Response: We agree with this finding.

Finding 16. Certain transactions were not recorded or accounted for in accordance with General Accounting Division requirements.

DJS response: We agree with this finding.

Overall, by addressing the issues you have highlighted, we will improve DJS' operations. If we can be of further assistance, or if you would need any additional information, please do not hesitate to contact me. Thank you again.

Sincerely yours,

Donald W. DeVore
Secretary

Attachment

Cc: Mr. John Dixon, DJS Deputy Secretary for Operations
Mr. Francis Mendez, DJS Deputy Secretary for Administration
Mr. Neil Bergsman, DJS Chief Financial Officer
Mr. Michael DiBattista, DJS Director of Accounting
Mr. Peter Keefer, DJS Director of Investigations and Audits
Mr. Alan Small, DJS Director of Audit & Compliance
Mr. Christopher McCully, DBM, Office of Budget Analysis
Ms. Elizabeth Wright, Acting Asst. Secretary for Departmental Support

Department of Juvenile Services
Response to Legislative Audit

July 6, 2007

Federal Funds

Finding #1
DJS needs to continue to work with the Judiciary to ensure that federal Title IV-E revenue is recovered to the fullest extent possible.

DJS Response: DJS agrees with this finding and recommendation. The Department will continue to work with the Judiciary to enhance these recoveries.

Finding #2
Federal revenue was potentially lost because Title IV-E eligibility determinations for youths were not timely completed.

DJS Response: DJS agrees. DJS has been in compliance with this recommendation since April, 2005. DJS has taken a number of steps to improve the flow of eligibility determinations and avoid the lapsing of potential recoveries: DJS instituted a systematic review of cases awaiting an eligibility determination to prioritize the oldest cases in which the youth resided in a IV-E reimbursable placement. Consideration was also given to those cases which had the greatest likelihood of being IV-E eligible.

In addition, DJS entered into a new Memorandum of Agreement with DHR which authorizes DJS to make IV-E eligibility determinations for DJS youth. DJS has also secured three additional positions to staff this function.

Further, DJS has also negotiated memorandums of agreement with the Department of Labor, Licensing and Regulation, and the Department of Health and Mental Hygiene. Each agency maintains computer database information which is essential for the making of IV-E eligibility determinations.

Currently all cases that await an eligibility determination are assigned to the DJS Eligibility Specialist at the beginning of a 90 day cycle. The Specialist has a 90 day period to complete the determinations. The most recent case for which unclaimed funds were identified has an eligibility determination date of August 5,

2004. DJS has received some clarifying instructions from the US Department of Health and Human Services, and is in the process of reviewing cases in which court order language, although not fully "child-specific," may be sufficient to meet minimal standards to claim reimbursement.

Cash Receipts

Finding #3
Procedures for controlling and accounting for collections at two locations were not sufficient.

DJS Response: DJS agrees. The Department has taken action to now be in compliance with this recommendation. The verification of cash receipts will be a component of the resolution of other audit recommendations. Transfer of funds from the Restitution Lockbox to the State account will be completed on a weekly basis at a minimum. That process has been implemented effective March 6, 2007. The Department is in the process of working with SunTrust Bank and the Treasurer's Office to determine if an automated daily transfer is viable. That determination and any necessary set-up should be made by the end of August... The recommendations offered by OLA Auditors to Region III during this audit (the Western Region) were implemented in October 2006.

Accounts Receivable

Finding #4
Adequate internal controls and record keeping procedures had not been established.

DJS Response: DJS agrees. DJS has initiated processes to document adjustments and perform the necessary reviews. DJS is in the process of realigning staff to create the appropriate separation of duties. It is anticipated that training will be implemented and completed in the first six months of fiscal year 2008.

Finding #5
DJS did not always comply with certain regulations and provisions of the law related to the collection of delinquent accounts.

DJS Response: DJS agrees. The Department will review the procedures related to delinquent accounts. Where necessary the procedures will be updated and training of appropriate staff conducted. It is anticipated that procedures will be distributed and training completed by December 31, 2007. Accounts marked for submission to the Central Collection Unit will be transferred on a monthly basis. The monthly transfer of accounts to CCU began with the transfer of accounts on April 2, 2007.

Corporate Purchasing Cards

Finding #6
Controls over card issuances were not sufficient and required documentation of purchases was not always on file.

DJS disagrees that controls over the issuance of purchasing cards is not adequate. DJS agrees with the finding related to documentation and timely reporting.

The Department is in compliance. The Budget Director acts as the Assistant Purchasing Card Program Administrator (PCPA). Another individual, the DJS' FMIS security officer, receives and distributes the credit cards as required by the manual.

With the advent of a new contractor operating the Corporate Purchasing Card (CPC) program, DJS has obtained new CPC agreements from all of our cardholders, authorized and signed by their supervisors and signed by a fiscal officer. The file will be maintained in the procurement office with a duplicate in the Office of Budget and Finance. In addition, the justifications of each card holder have been documented, reviewed, and approved by management and the number of card holders has been reduced to less than thirty.

Disbursement Transactions

Finding #7
Proper internal controls were not established over critical functions on the State's Financial Management Information System.

DJS Response: DJS agrees. The Department has reviewed the FMIS security of the staff identified by the auditor. Security changes have been implemented to prevent the initiation, processing, and release of disbursement transactions to the Comptroller of the Treasury- General Accounting Division for payment. The Department will review the responsibilities of all staff as they relate to the accounts receivable process. Appropriate segregation of duties as they relate to critical transactions will be established. Procedures will be reviewed and updated where appropriate and training will be conducted. We anticipate that this will involve reassignment of duties for several accounting unit staff. The initial phase, assigning of new responsibilities, will be completed by July 31, 2007. Complete compliance with the recommendation will be achieved by December 31, 2007.

The Department now reviews the security reports of employee access profiles that are provided by the Department of Budget and Management (DBM) on a bi-monthly basis. The Department also seeks to ensure that all users listed on the report are currently active within the agency and will work with the Chief Internal Auditor to ensure that documentation is sufficient for future audit verifications.

Finding #8
Employee access to critical automated systems was not adequately controlled

DJS response: The Department agrees with this finding. The Department is currently researching and will implement procedures for audit of critical privileges where appropriate. The target date for the completed implementation will be December 31, 2007.

Finding #9
The internal network was not properly protected from security risks.

DJS response: DJS agrees in part and disagrees in part with this finding.

With respect to bullet 1, dealing with firewall rules: the Department agrees with this finding. The Department has already made significant changes to create network security logs. The Department has implemented procedures to monitor these logs.

With respect to bullet 2, Dealing with network access by third parties: the Department respectfully disagrees with this finding. The Department routes third-party entity networks through a dedicated segment away from any access to the internal DJS network. Third-party entities do not have access to the internal DJS network.

With respect to bullet 3, dealing with instruction detection prevention (IDP): the Department agrees with this finding. The Department has purchased and began implementation of an IDP system to block network security attacks as well as alert network administrators to attack from external sources. Full deployment is anticipated to be complete by the end of September, 2007.

With respect to public access to servers: the Department agrees with this finding. The Department is in the process of migrating and testing web applications on a publicly accessible server in a separate network zone and projects deployment by the end of September, 2007.

Finding #10
Administration and monitoring of critical network devices need improvement.

DJS response: DJS agrees in part and disagrees in part.

With respect to bullet 1, dealing with the number of individuals with administrative access to devices: The Department respectfully disagrees with this finding. The Department has: limited administrative access to critical network devices to four key network administrators, limited connection protocols for these devices to "least privilege", and taken additional security measures to protect these devices. DJS believes that the remaining individuals with administrative access are not excess, and that these individuals need this level of access for the Department to maintain reliable service levels.

With respect to bullets 2 and 3, dealing with log files: the Department agrees with this finding. The Department is now compliant. The Department now stores device logs on a separate server and is monitoring these logs on a daily basis. Currently these logs are being retained without deletion until an IT Security Policy is implemented. The Department is drafting an IT Security Policy addressing a log monitoring process and establishing log retention policies compatible with DJS internal audit requirements.

Finding #11
DJS did not adequately secure its web access to two sensitive applications

DJS response: The Department agrees with this finding. The Department is now compliant. The Department now encrypts non-public information between remote users and web based applications including based upon current DBM *Information Technology Security Policy and Standards*.

Finding #12
Network and database accounts and related passwords were not adequately controlled, and certain system activities were not monitored.

DJS response: The Department agrees with this finding. The Department is now partially compliant. The Department has made the necessary changes and is now in compliance with DBM *Information Technology Security Policy and Standards* for passwords.

DJS anticipates implementation of auditing of critical network servers and databases prior to December 31, 2007.

Finding #13
DJS did not have a complete information technology disaster recovery plan.

DJS response: The Department agrees with this finding. The Department has maintained an updated Disaster Recovery Quick Plan since 2003. Completion of a full IT Disaster Recovery Plan is projected for December 31, 2007. This is contingent upon completion of other internal planning by November, 2007.

Payroll

Finding #14
Critical documents were not adequately reviewed and there was a lack of control over procedures used to remove employees from the payroll.

DJS response: DJS agrees. The Department will review the procedures related to the approval and release of the payroll to Central Payroll. Where feasible we will work to establish procedures for the review, on a test basis, of supporting documentation. However, time constraints on the submission of payroll will likely dictate that the review of supporting documentation be completed after the release of the payroll to Central Payroll. The review will be documented. The Department will discontinue access to paychecks for those employees responsible for processing documentation to remove employees from the payroll. DJS will complete these actions by September 30, 2007.

Property

Finding #15
Equipment inventories were not conducted as required and record keeping was deficient.

DJS Response: DJS agrees. DJS maintains proper inventory controls for information technology and communications equipment, and for all equipment in the Western Maryland youth camps and the field offices in Allegany, Garrett and

Washington Counties. DJS agrees that proper inventory controls were not maintained for other equipment.

Since the last audit in 2003, the DJS IT Unit has made several positive changes to track and maintain all sensitive and non-sensitive computer equipment. DJS has met with the Department of General Services to develop a plan to improve inventory compliance.

The Department shall design a plan of action to include designating Accountable Inventory Officers for each DJS location or facility. These individuals will be responsible for documenting and maintaining the Department's assets. The Department will coordinate with DGS a formal training for the Accountable Inventory Officers to include the DGS guidelines outlined in the Inventory Control Manual.

DJS estimates that two to three additional staff will be needed to fully implement the required inventory controls. DJS will work with DBM to obtain the required staffing. DJS is not able to commit to a time frame for complying with these recommendations.

Revenue Transactions

Finding #16
Certain transactions were not recorded or accounted for in accordance with general Accounting Division requirements.

DJS Response: DJS agrees. The receivable arises from an arrangement in which the Local Management Board for Montgomery County received a fixed allotment for services to youth from the County referred to DJS. When the cost of the services exceeded the amount of the allotment, the receivable of $475,000 resulted. The Department will work with the Department of Budget and Management and the General Accounting Division to close the referenced revenue accruals. The ultimate resolution of this issue may require a new general fund appropriation. DJS cannot therefore commit to a specific time frame to correct this finding.

The Department has historically collected and recorded commissions from vending machines and telephones as Special Funds. These expenditures are appropriated in the budget bill each year as Special Funds. The total amount approximated $150,000 to $200,000 annually. They are used to provide recreational opportunities, behavior management incentives, and special programs to benefit juveniles in the care of the Department. If necessary, DJS will seek legislation to clearly authorize the use of these proceeds as special funds, and will seek to change the description of the special funds in the budget books to accurately describe their source. DJS cannot commit to a time frame for resolving this finding.

AUDIT TEAM

Paul R. Denz, CPA
Audit Manager

Stephen P. Jersey, CPA, CISA
Information Systems Audit Manager

Bekana Edossa, CPA, CFE
Senior Auditor

Edwin L. Paul, CPA
Albert E. Schmidt, CPA
Information Systems Senior Auditors

Dionne E. Fletcher
Lindsay T. Howarth
David S. Propper
Athenia M. Rock
Staff Auditors

Amanda L. Trythall
Information Systems Staff Auditor