The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

No. 2005-0142-4T

OFFICE OF THE STATE AUDITOR'S

REPORT ON

INFORMATION TECHNOLOGY CONTROLS

AT THE COMMONWEALTH OF MASSACHUSETTS

CHILD SUPPORT ENFORCEMENT PROGRAM

July 1, 2003 through January 4, 2006

OFFICIAL AUDIT

REPORT

JUNE 29, 2006

2005-0142-4T

TABLE OF CONTENTS

INTRODUCTION

Chapter 119A, Section 1, of the Massachusetts General Laws established the Child Support Enforcement Commission within the Executive Office for Administration and Finance. The Commission consists of six members: the Secretary of the Executive Office for Administration and Finance, who serves as chairman; the Commissioner of Revenue; the Attorney General; the Chief Administrative Justice of the Trial Court; the Commissioner of Public Welfare (the Department of Transitional Assistance); and a district attorney designated by the governor. The Commission monitors the child support enforcement system of the Commonwealth and advises the IV-D agency and other agencies of the Commonwealth, including the appropriate divisions within the Commonwealth's trial courts, in matters regarding the improvement of the child support enforcement system of the Commonwealth. The term "IV-D" comes from Title IV, Part D, of the federal Social Security Act, which established the Child Support Enforcement Program in 1975.

The Department of Revenue (DOR) is the single state agency within the Commonwealth that is designated the IV-D agency pursuant to Title IV, Part D, of the Social Security Act. A IV-D case involves the custodial parent receiving welfare benefits or applying for child support services pursuant to Title IV-D of the federal Social Security Act. The Commissioner of DOR was authorized to establish a Division of Child Support Enforcement (CSE) to implement the provisions of Chapter 119A of the General Laws. CSE's mission is to (1) identify and locate absent parents, (2) establish and enforce support obligations, and (3) collect and distribute support payments for children receiving public assistance payments under the Transitional Assistance to Families with Dependent Children (TAFDC) Program as well as a portion of court-ordered non-TAFDC payments. The Office of the Deputy Commissioner directs the strategic planning for CSE and sets operational priorities for its approximately 750 employees.

The mission of CSE is to protect the economic wellbeing of the Commonwealth's children by enforcing the financial responsibilities of parenthood. CSE's core functions are to establish paternity and establish, enforce, and modify child support and health insurance orders. CSE currently issues, on average, monthly financial assistance to approximately 50,000 custodial parents representing approximately 200,000 payments per month. CSE relies heavily on information technology to help carry out its mission and business objectives. For fiscal year 2005, CSE collected more than $495 million in child support for Massachusetts families and was supported by a budget of approximately $64 million.

CSE personnel establish case files for custodial parents and track data on each case. Information on parents is also kept on file to help establish paternity and child support orders, and enforce child support orders, if necessary. CSE personnel also track information on employers, insurance availability, and addresses. In addition to paper documents in case files, all case records (collections and disbursements included) are maintained on a computerized case management and tracking system known as the Commonwealth of Massachusetts Enforcement and Tracking System (COMETS). CSE uses COMETS to

track the payments and people involved in all child support cases referred to them by public assistance programs, the courts, and parents who apply directly to CSE for assistance in collecting child support payments. The COMETS application, which became fully functional in December 1997, supports program functions including case initiation, location, establishment, case management, enforcement, financial management, reporting, and security/privacy. Prior to COMETS and since the 1980s, CSE used a data system called Model II. When COMETS was introduced, all Model II data was migrated onto the new system. COMETS consists of two separate environments, COMETS and CSE's financial module (COMETS-FM). The COMETS system shares the backend-mainframe with MASSTAX and is connected to both the EMC Symmetrix 5 and the DMX2000 storage systems. COMETS-FM is an n-tiered application based in Oracle Forms/Oracle DB running on Unisys enterprise servers (ES7000) using Windows Datacenter. COMETS-FM communicates with the other remaining modules of COMETS (e.g., case management, intake, location, litigation) that employ a DMS1100 database currently running on Unisys ClearPath IX 6800.

The CSE information technology (IT) infrastructure used to support COMETS and administrative applications consists of local area networks (LANs) installed at the central office and at regional and area offices linking over 800 workstations within a Novell network providing access to print and file servers. The primary production data center is located in the greater Boston area. CSE offices are able to access COMETS data files and software directly through the WAN to the Commonwealth's file server containing the COMETS database. Through the network, the microcomputer workstations also provide access to the state's Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

Our examination focused on a review of selected internal controls over COMETS, specifically physical security and environmental protection controls over IT resources at CSE's production site and administrative offices, system access security, business continuity planning, and on-site and off-site storage of computer-related media. In addition, we performed an assessment of enforcement actions via the Commonwealth of Massachusetts Enforcement and Tracking System, specifically the license suspension program, to ensure that administrative enforcements were effectively used to collect unpaid child support obligations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Department of Revenue's Child Support Enforcement (CSE) Division for the period of July 1, 2003 through January 4, 2006. Our audit scope included a general control examination of internal controls related to the organization and management of IT activities and operations, including strategic and tactical planning, physical security and environmental protection over the CSE IT infrastructure, business continuity planning, and on-site and off-site backup magnetic media storage. We also performed an evaluation of IT-related contract management, system access security, and inventory controls over IT equipment.

Our audit scope included identifying and reviewing mechanisms available to CSE to collect past-due child support payments or arrears owed to custodial parents. Consequently, we performed an assessment of enforcement actions via the Commonwealth of Massachusetts Enforcement and Tracking System (COMETS), specifically the license suspension program, to ensure that administrative enforcements were effectively used to collect unpaid child support obligations. The audit was conducted from June 2, 2005 through January 4, 2006.

Audit Objectives

Our primary audit objective was to determine whether CSE's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support CSE's business functions. In this regard, we sought to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.

Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether CSE had implemented IT-related strategic and tactical plans to assist CSE in fulfilling its mission, goals, and objectives, and whether CSE had appointed a steering committee to oversee its information technology department and activities.

We further sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the data center and the on-site and off-site media storage areas was limited to authorized personnel. Moreover, we sought to determine whether sufficient environmental protection was being provided to prevent or detect damage or loss of IT-related equipment and media.

Regarding systems availability, we sought to determine whether adequate business continuity plans were in effect to help ensure that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable or inaccessible. Moreover, we sought to determine whether adequate controls were in place to provide reasonable assurance that appropriate magnetic backup copies of application systems and data files would be available on-site and off-site to support disaster recovery and business continuity planning objectives.

We sought to determine whether contractual relationships with third-party IT-related service providers were covered by written contracts, contract agreements sufficiently detailed services or deliverables to be provided, and contracts were properly signed and dated. We sought to determine whether third-party contracts contained standard terms and conditions as promulgated by the Operational Services Division and whether incorporated vendors were properly registered with the Office of the Secretary of State. We evaluated whether the CSE had implemented adequate controls with regard to IT contract management to provide reasonable assurance that monitoring and evaluation were being performed. In addition, we determined whether selected contractor car rental expenses were properly authorized and whether they met the requirements of CSE's travel guidelines and were reasonable and economical.

We sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to CSE's data files. We sought to determine whether procedures were in place to prevent or detect unauthorized access to automated systems and IT resources including the UNIX, COMETS, Oracle, LAN file servers, and microcomputer systems. In addition, we determined whether the COMETS data was sufficiently protected against unauthorized disclosure, change, or deletion.

With regard to inventory control over IT equipment, including notebook computers, we evaluated whether an annual physical inventory and reconciliation was conducted and whether IT equipment was accurately reflected, accounted for, and properly maintained in the system of record.

We performed an assessment of enforcement actions via the Commonwealth of Massachusetts Enforcement and Tracking System, specifically the license suspension program, to ensure that these administrative enforcements were effectively used to collect unpaid child support obligations.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of CSE's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of CSE's organization and operations, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant

functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical by CSE.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of CSE's IT Department. We obtained, reviewed, and analyzed relevant IT-related policies and procedures and strategic and tactical plans to determine their adequacy. To determine whether CSE's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technological expertise requirements, we obtained a current list of the personnel employed by the IT Department, including their duties and job descriptions, and compared the list to the IT Department's organizational chart, each employee's statements concerning their day-to-day IT-related responsibilities, and the technology in use at the time. We inspected the data center and the central office in Boston, reviewed relevant documents, such as the network configuration, internal control plan, and business continuity plan, and performed selected preliminary audit tests.

We interviewed CSE management to discuss internal controls regarding physical security and environmental protection over and within the data center housing the file servers, the business offices where microcomputer workstations are located, and the on-site and off-site storage areas for mission-critical and essential magnetic media storage. In conjunction with our audit, we reviewed written, authorized, and approved policies and procedures for control areas under review. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with regulations and to meet generally accepted control objectives for IT operations and security.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft, or damage, we performed audit tests at the central office and the data center. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with CSE management and staff.

To determine whether adequate controls were in effect to prevent or detect unauthorized access to the selected business offices housing IT resources, we inspected physical access controls, such as the presence of security personnel on duty, locked entrance and exit doors, the presence of a receptionist at the entrance point, intrusion alarms, and whether sign-in/sign-out logs were required for visitors. We reviewed physical access control procedures, such as the lists of staff authorized to access the data center, and magnetic key management regarding door locks to the central office's entrance and other restricted areas within the central office. We determined whether CSE maintained incident report logs to record and identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the data center or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in business offices and the data center that houses the file servers. Further, we reviewed control procedures to prevent water damage to automated systems, agency records, and magnetic backup media stored on site.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and the microcomputer workstations be unavailable for an extended period. We interviewed senior management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place and had been periodically reviewed. Further, we reviewed and evaluated procedures in place to resume normal business functions should the file servers or the microcomputer workstations be rendered inoperable.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed CSE management responsible for generating backup copies of magnetic media for administrative work processed at CSE and applications such as COMETS residing on the file servers. Further, we reviewed the adequacy of provisions for on-site backup copies of mission-critical and essential magnetic media at the data center. We did not review the off-site storage location for backup copies, because it was under a third-party contract reviewed in prior audits. We did not review the Information Technology Division's backup procedures for transactions processed through MMARS and HR/CMS.

We sought to assess the internal control process for awarding, paying, and monitoring third-party provider service IT contracts. We sought to determine whether provider service contracts have been properly put out to bid and awarded, and whether vendor payment vouchers were reviewed, approved, and contained the required authorized signatures. In addition, we sought to determine whether the CSE had implemented adequate controls to provide reasonable assurance that monitoring and evaluation of provider service contracts was being performed in accordance with applicable Massachusetts General Laws and generally accepted business practices. We reviewed and evaluated all fiscal year 2004 and 2005 IT contract related expenses. Specifically, we analyzed rental car use by looking for documentation supporting the need for the car, evaluating alternatives, and reviewing mileage data for the car while in

travel status. In addition, we reviewed department policies, procedures, and documentation supporting the car rentals and discussed these expenses with senior management.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer systems. To determine whether CSE control practices regarding system access security would prevent unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the senior management responsible for the network and evaluated selected controls to the automated systems.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the LAN Manager responsible for access to the file servers and microcomputer workstations on which the CSE's application systems operate. In addition, we reviewed control practices used to assign and grant staff access privileges to the application programs and data files. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted to only authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application systems and related data files. We reviewed documents recording the granting of authorization to access automated systems and requested and received a current listing of users. In order to confirm whether access privileges to the automated systems were granted to authorized users only, we compared the user lists received to an active employee list. To determine whether CSE users with active privileges were current employees, we obtained the list of individuals with access privileges to the network and microcomputer workstations and compared all users with active access privileges to CSE's personnel roster of current employees. Further, we determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for CSE's computer equipment, we reviewed inventory control policies and procedures and requested and obtained CSE's inventory system of record for computer equipment. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related fixed assets. We also performed a data analysis on the inventory and made note of any distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the system of record for computer equipment for fiscal year 2005 was current, accurate, complete, and valid, we used Audit Command Language (ACL) to select a statistical sample of 247 items out of a total population of 999 items in order to achieve a 98% confidence level. We traced the inventory tags and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To verify the relevance and completeness of CSE's system of record for IT-related equipment, we randomly selected 176 additional computer hardware items in adjacent locations and determined whether they were properly recorded on CSE's inventory record. To determine whether selected computer hardware purchases in fiscal years 2004 and 2005 were accurately listed, we randomly selected 196 items, valued at $121,530, and verified whether the amounts recorded on CSE's purchase orders and invoices could be located on the inventory system of record. To determine whether CSE had appropriate control practices in place and in effect to account for and safeguard notebook computers, we interviewed representatives from the IT Department. Further, we reviewed the control form used by each area regarding their computer equipment loan policies for employees, and requested for review CSE's documented policies and procedures to control the assignment and use of notebook computers.

To determine whether CSE complied with Commonwealth of Massachusetts regulations for accounting for assets, we reviewed evidence supporting CSE's performance of an annual physical inventory of IT assets. Further, to determine whether CSE complied with Commonwealth of Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that CSE plans to request Commonwealth approval to dispose of as surplus. Finally, to determine whether CSE was in compliance with Chapter 647 of the Acts of 1989, regarding reporting requirements for missing or stolen assets, we reviewed incident reports for missing or stolen IT-related equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess the effectiveness and compliance with laws, rules, policies, and procedures of the CSE in enforcing child support orders, we analyzed and tested selected administrative enforcement tools and actions taken for cases with significant arrearages. We selected the license suspension program for our audit testing, as it was identified as an effective administrative enforcement technique utilized by CSE. According to CSE policy, suspension of driver's licenses, recreational licenses, or professional/occupational licenses are available enforcement actions once non-custodial parents (NCPs) in arrears meet specific criteria, such as being:

- At least 56 days delinquent in their child support payments.
- In arrears for over $500 in child support payments.

To evaluate factors adversely affecting CSE efforts to collect current child support payments owed to IV-D custodial parents, as well as past-due support or arrears, we conducted tests to determine whether license suspension had been aggressively pursued. We reviewed, for a two-month period, all NCPs that were eligible for license suspension warning letters, as identified within the COMETS Warehouse Database. We then compared the records pertaining to the 26,991 NCPs identified as being eligible for license suspension warning letters to the number of letters actually received by NCPs notifying them of

CSE's intent to suspend their driver's license, to determine whether adequate enforcement actions had been taken. Next, we provided CSE with the names of 55 NCPs eligible for license suspension warning letters, (of which 20 NCPs were in arrears in excess of $150,000), for possible matches to active Massachusetts driver's licenses. We discussed and reviewed sampling methodology with the Associate Deputy Commissioner of CSE, who concurred with the sampling approaches used. We did not assess the reliability of the division's data recorded on the computerized system.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Child Support Enforcement Division (CSE), we found that adequate controls were in place to provide reasonable assurance that information technology (IT)-related control objectives would be met with respect to IT organization and management, physical security, environmental protection, on-site and off-site storage of backup copies of magnetic media, and system access security. However, CSE should be more aggressive in its pursuit to suspend driver's licenses of individuals in arrears for child support payments. We determined that the driver's licenses of thousands of non-custodial parents (NCPs) eligible for license suspension were not aggressively pursued by caseworkers. In addition, controls needed to be strengthened to provide reasonable assurance that control objectives regarding system availability, monitoring, and evaluation of IT vendor service contracts and inventory controls over IT equipment will be met.

Our review of IT-related organizational and management controls indicated that CSE had a defined IT organizational structure, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for IT staff that reflected current responsibilities. Our review of IT-related planning found that CSE had developed a comprehensive strategic/tactical plan to address IT functions within the IT Department and across the five regional and two satellite offices. With respect to the use and the safeguarding of information technology, we determined that formal policies and procedures were in existence, but needed to be strengthened for business continuity and contingency planning and inventory controls over IT equipment. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced.

Our examination of physical security revealed that controls provided reasonable assurance that CSE's IT resources were safeguarded from unauthorized access. We found that the data center was locked, and that a list was maintained of individuals who had access to keys. CSE had full-time security guards on duty 24 hours per day, seven days per week, and the facility was equipped with intrusion alarms. Our examination also disclosed that these areas have restricted keycard access to only approved individuals. In addition, visitors are escorted when accessing the data center, to minimize the risk of damage and/or theft of computer equipment. Our review of selected areas housing microcomputer workstations disclosed that on-site security personnel make periodic rounds nightly to verify that all office doors are locked and secure.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply, were in place in the building housing CSE to help prevent

damage to, or loss of, IT-related resources. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an uninterruptible power supply (UPS) was in place to prevent sudden loss of data and that hand-held fire extinguishers were located within the data center. Moreover, evacuation and emergency procedures were documented and posted within the data center. According to management, staff had recently been trained in the use of these emergency procedures.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media. We determined that CSE had implemented procedures and schedules for generating backup copies of magnetic media and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site, and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies.

Although on-site and off-site storage of backup media was in place, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. Specifically, our audit disclosed that CSE did not have a comprehensive disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for the Commonwealth of Massachusetts Enforcement and Tracking System (COMETS) could be regained effectively and in a timely manner should a disaster render automated systems inoperable. Although we found that there was a plan from December 1999, and that a potential alternate processing site had been selected, the plan had not been updated. Also, user area plans had not been established to document the procedures required to regain business operations in the event of a disaster.

Our review of CSE's IT-related service contracts revealed that all contracts reviewed were properly signed and approved, and all vendors incorporated, as either a foreign or domestic corporation, were found to be properly registered with the Commonwealth's Office of the Secretary of State. We determined that the CSE used the competitive bid process to award IT-related service contracts. We also determined that CSE had in place sound policies regarding reimbursements for travel expenses, including the reimbursement of contracted employee expenses. However, during the course of our audit, we observed certain contracted employee reimbursement items regarding automobile rentals that appeared questionable. The submitted receipts raise concerns with respect to the validity and appropriateness of the expenses, in that they appear to be outside of the guidelines used within CSE to support authorization of payment.

Regarding system access security, our audit revealed that CSE had developed and documented appropriate procedures regarding the granting of access privileges to automated systems and activation of

logon IDs and passwords. Regarding procedures to deactivate access privileges, we found that formal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. Audit tests of access security that compared 150 (20%) randomly-selected users to CSE's payroll roster of current employees confirmed that the users were current employees. Further, we determined that appropriate control procedures were in place with respect to monitoring user privileges and password administration and the granting of limited access privileges to individuals working in other entities.

Our audit revealed that CSE could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since an annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. We found that 27 IT purchases made during fiscal years 2004 and 2005 were not included in the inventory system of record, and our data analysis of the entire population of 999 IT hardware items indicated that there were missing fields of information with respect to value. However, our test of 176 hardware items, traced from multiple physical locations back to the inventory listing, indicated that all of the selected items were on the inventory list. Also, our inventory test of 209 items taken from the inventory list and traced back to their actual location indicated that all pieces of computer equipment could be located. Furthermore, an inventory test of 38 notebook computers indicated that all notebook computers could be found.

Regarding surplus property and equipment, our audit revealed that CSE was aware of the Operational Services Division's (OSD) policy and procedures and was in compliance. We found that, although CSE's Internal Control policies included control and reporting requirements set forth in Chapter 647 of the Acts of 1989, our audit revealed that CSE did not comply with the requirements of Chapter 647 of the Acts of 1989 when CSE had failed to notify the Office of the State Auditor of 32 pieces of stolen computer equipment.

Based on CSE's data, approximately $1.5 billion dollars in uncollected child support existed at the time of our audit. Of the $1.5 billion, CSE's data indicated that $569 million of the arrearage cases were eligible for the license suspension program. Our review of information and administrative procedures incorporated into the COMETS application indicated CSE has a variety of collection tools. Our review focused on whether all eligible cases and associated non-custodial parents (NCP) identified within the COMETS Warehouse Database as being eligible for license suspension warning letters did, in fact, receive one. Our audit disclosed that CSE should more aggressively pursue suspending the driver's licenses of individuals whose child support payments are in arrears. We determined that the driver's licenses of thousands of NCPs eligible for license suspension were not suspended. For example, our

analysis of the May and June eligibility report determined that 26,991 NCPs were eligible for license suspension warning letters as an administrative enforcement to collect past-due support. However, CSE personnel only notified 818 NCPs, or 3% of the potential suspensions, of the Division's intent to suspend the person's driver's license. Consequently, based on our probability of 90% and a study population of 26,173 NCPs, our analysis estimated that 18,894 NCPs met the criteria to be issued a license suspension warning letter where past-due support is owed. Projecting our analysis and CSE's own average of $2,602 per collection, we determined that there is over $49 million in lost potential income to the Commonwealth and some of its most needy children.

AUDIT RESULTS

1. License Suspensions Not Aggressively Pursued

Our audit determined that the Child Support Enforcement (CSE) Division should be more aggressive in its pursuit to suspend the driver's licenses of individuals who are in arrears for child support payments. We determined that the driver's licenses of thousands of eligible non-custodial parents (NCPs) were not suspended, resulting in over $49 million in lost potential income to the Commonwealth and some of its most needy children.

When NCPs do not make child support payments, caseworkers can take administrative actions to enforce compliance with orders of support. Automatic and manual actions include income withholding, real and personal property liens, state and federal income tax refund interceptions, unemployment compensation and workers' compensation benefits interceptions, and referral to consumer reporting agencies. CSE's Commonwealth of Massachusetts Enforcement and Tracking System (COMETS) notifies technicians through an electronic message called an alert when an automated enforcement action occurs. The system also alerts caseworkers to cases suitable for other manual actions, but it does not specify the needed action. Automatic enforcement actions are documented on case records by the computerized system, as are most manual actions involving system-generated forms and letters. Also, the computerized system automatically records new address and employment information when NCPs are located. If caseworkers cannot locate the NCP or cannot secure payment, COMETS tracks the amount of child support owed to the custodial parent. The unpaid amount is considered "past-due support."

Caseworkers can take other administrative actions to collect payments. For example, caseworkers have the ability to initiate action to suspend licenses for recreational activities, professional licenses, and driver licenses in accordance with Massachusetts General Law, Chapter 119A, Section 16. CSE identifies eligible NCPs for license suspension by performing automated and manual data matches with external agencies. These matches would alert caseworkers of professional, occupational or recreational licenses eligible for suspension. Since license suspension is a manual enforcement remedy requiring a License Suspension Warning Letter notification to the delinquent parent, enforcement action in this area has occurred solely by caseworker initiative. Caseworkers have online access to the Registry of Motor Vehicles (RMV) records to manually identify parents owing child support that appear on the "8 Weeks No Pay/Case Review" task with a valid driver's license. According to CSE policy, suspension of driver's licenses, recreational licenses, or professional/occupational licenses are available enforcement actions once NCPs meet specific criteria, such as being:

- At least 56 days delinquent in their child support payments.
- In arrears for over $500 in child support payments.

License suspension was identified as an effective technique utilized by CSE. Senior management stated that they do not want to suspend NCPs' licenses, but that the threat that the suspension is to take place generally encourages delinquent NCP's to work out a payment schedule or to start making payments. According to CSE reports for fiscal year 2005, collections of past due child support totaled approximately $17.9 million following the suspension of drivers licenses, professional licenses, and vehicle registrations for delinquent NCPs. Records indicated that CSE caseworkers took action against 217 professional licenses and 6,363 driver's licenses. According to administration reports, this program has resulted in collections of approximately $47.5 million since its inception in 2002.

CSE's Eligible License Suspension Warning Letter report for May to June 2005 disclosed that caseworkers' use of license suspensions as an enforcement tool has been limited. For example, although the May and June eligibility report identified 26,991 NCPs who were eligible to receive License Suspension Warning Letters, only 818 NCPs, or 3% of those eligible, were actually notified of CSE's intent to suspend their licenses. CSE's own analysis of payment agreements reached with NCPs that had been sent a License Suspension Warning Letter averaged $2,602.

In order to determine the disposition of the remaining 26,173, or 97% of the total NCPs reported as eligible for suspension, we provided CSE with a judgmental sample of 20 NCPs, each of whom had past-due support exceeding $150,000. Of the 20 NCPs, we matched nine cases having past-due support totaling $1.9 million who could have received a license suspension warning letter. Our review of a statistical sample of 35 NCPs, achieving a 90% confidence level, disclosed 70%, or 25 NCPs, met CSE's criteria for a license suspension warning letter. We found for the 25 NCPs, where driver's license suspension was an option and could be matched by online records of operators' licenses, unpaid support totaling $2.6 million. Based on probability of 90% and a study population of 26,173 NCPs, our analysis estimated that 18,894 NCPs met the criteria to be issued a license suspension warning letter where past-due support is owed. Projecting our analysis and CSE's own average of $2,602 per collection, then $49,162,188 in lost potential income to the Commonwealth and some of its most needy children.

Caseworkers may, at their discretion, choose to pursue license suspension. Since license suspension is a manual enforcement remedy requiring pre-suspension notification to the delinquent parent, enforcement action in this area has occurred solely by technician initiative. However, our discussions with senior management showed that many of the caseworkers do not use driver's license suspension as an enforcement tool because they do not have time to review the report.

Recommendation:

We recommend that CSE pursue expanding the use of license suspensions statewide as an enforcement tool for collecting arrearages and encouraging NCPs to be current in their support payments. We also recommend that CSE automate the data match with the Registry of Motor Vehicles. Automation has enabled CSE to streamline formerly manual processes and provided their employees with interfaces and access to data that was previously unavailable (e.g., Federal Case Registry, State Lottery Intercept, and Credit Bureau Reporting). Automating activities, such as driver's license suspension and generating daily tasks for employees, will enable CSE to create consistent processes that can be monitored and adjusted based on performance. To complement other metrics used, we recommend that management implement additional metrics that would indicate the level of recovery activity and collections to the total eligible population. We recommend that senior management track cases eligible for license suspension using a monthly eligibility report that would identify the total number of NCPs eligible for license suspension from the total number of all delinquent NCPs. Using a metric that would trend the usage of license suspension as an administrative enforcement tool, senior management would be able to better monitor the degree of use of license suspension enforcement activities.

Auditee's Response:

> *The license suspension program is among the most effective and successful tools CSE has implemented for collection of past due support. Total collections from the program now exceed $65,000,000. Monthly collections have risen steadily since May of 2005 when they totaled $1.19M to March of 2006 when collections reached an all time high monthly total of $2.5M. CSE has introduced additional automation to the process through the systemic generation of notices by COMETS.*
>
> *CSE agrees that more improvements can and should be implemented. CSE is engaged in an extensive Division wide business process redesign that is examining all work flows. We are using business process modeling software that examines each process to identify efficiencies that could be achieved. This new workflow design will also provide us with the functionality to establish and track the metrics the State Auditor recommends.*

Auditor's Reply:

We acknowledge that CSE has been able to increase monthly collections of past due support by automating license suspension notices within COMETS. We believe CSE management's decision to introduce business process modeling software will enhance the use of license suspensions statewide as an enforcement tool for collecting arrearages and encouraging NCPs to be current in their support payments. We also believe that this software will help provide CSE with a metric that would trend the usage of license suspension and enable senior management to

better monitor the degree of use of license suspension enforcement activities. We further acknowledge that CSE collected $495 million during fiscal year 2005 using a variety of administrative collection procedures. Given that the total arrearage at the time of our audit was approximately $1.5 billion dollars, we continue to encourage CSE to aggressively pursue collections of past due support through all collection tools available, including the license suspension program.

2. Disaster Recovery and Business Continuity Planning

We determined that CSE did not have an up-to-date and tested disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems be rendered inoperable or inaccessible. The primary document relating to business continuity planning that was available from CSE was a plan developed by an outside contractor in 1999 that had not been updated since. Although CSE had procedures for testing the recovery of its database to resume operations in the event that the COMETS system (which is used to track the payments and people involved in all child support cases) goes off line, there was no policy regarding recovery testing. In addition, although the CSE had on-site and off-site storage of backup media available for recovery, CSE had not formalized its agreement for an alternate processing site to be used to regain processing should the data center be damaged or inaccessible for an extended period of time. According to CSE, the financial impact due to outage of COMETS for the over 211,000 families that receive payments distributed daily could be over $1.8 million. This lack of processing capability could restrict a family's ability to satisfy their daily needs for food, clothing, and housing.

A comprehensive disaster recovery and business continuity plan should reflect current conditions, clearly assign responsibilities for recovery, and include detailed instructions for restoring operations. We found CSE's 1999 plan had not been updated to address subsequent changes to the computerized system, to reestablish CSE's computerized system capability on a statewide basis, and to identify specific responsibilities of those carrying out the disaster recovery and business continuity plan. We also determined that the disaster recovery and business continuity plan does not document specific disaster recovery procedures for the recovery of department systems. Instead, it establishes disaster recovery teams that will meet once a disaster occurs to develop disaster recovery action plans. Furthermore, the plan does not identify resources and data necessary in the event of a disaster, backup and recovery capabilities needed for successful disaster recovery, and facilities used to house sensitive and critical equipment and data.

Without a formal, comprehensive recovery and contingency plan that includes required user area plans and network communication components which have been sufficiently tested, CSE could be inhibited from processing information for the COMETS system or other applications residing on CSE's local area network (LAN), or from accessing information or processing transactions related to the Massachusetts Management Accounting and Reporting System (MMARS) or the Human Resources Compensation Management System (HR/CMS) residing on the Information Technology Division mainframe. As a result, CSE would be hindered from obtaining information needed to continue critical business operations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted control practices and industry standards for IT operations support the need for CSE to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, CSE should reassess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop recovery plans based on the critical requirements of its information systems to support business functions.

The reassessment of impact should identify the extent to which departmental business objectives and functions are affected from loss of processing capabilities over various time frames. The reassessment of criticality and impact of loss of processing should assist CSE in triaging its business continuity planning and recovery efforts.

CSE should perform a risk analysis of its IT systems to more clearly identify the impact of lost or reduced processing capabilities. This risk analysis should identify the relevant threats that could damage or preclude the use of the systems and the likelihood and potential frequency of each threat. The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative critical character and importance of systems, and that adequate resources are available. The recovery strategies should address potential scenarios of loss of IT operations and should be based upon the results of risk analysis and an assessment of processing requirements. Without a formal, tested recovery plan, critical and essential information related to CSE's clients and programs might be unavailable should the automated systems be rendered inoperable.

Sound management practices, as well as industry and government standards, advocate the need for comprehensive and effective backup and disaster recovery and business continuity planning to ensure that mission-critical and essential operations can be regained. Disaster recovery and business continuity planning should be viewed as a process to be incorporated within the functions of the organization, rather than as a project that would be considered as completed upon the drafting of a written recovery plan. Since the criticality of systems, importance of business objectives, and the risks and threats associated with IT operations may change, a process should be in place to identify the change in criticality, business requirements, or risks, and assess the need to amend and test recovery and contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans. Business continuity and contingency planning has taken on added importance given that potential processing disruptions could be caused by man-made events.

Recommendation:

CSE should establish a business continuity planning framework that incorporates criticality and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of CSE's systems is evaluated on an annual basis, or upon major changes to user or business requirements, IT configuration, or identified risks. CSE should also conduct a formal risk analysis of its IT-related components, including outsourced services provided by ITD, on an annual basis, or upon major changes to the relevant IT infrastructure or to business operations or priorities. Based on the results of the risk analysis and criticality assessment, CSE should confirm its understanding of business continuity requirements and, if necessary, amend recovery plans to address mission-critical and essential IT-supported business functions.

CSE should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical and essential operations within the needed time frames. In addition, CSE should ensure that appropriate user area plans are in place and are sufficiently understood by administrative and operational management, as well as staff, to enable business areas to continue their operations should automated processing be lost for an extended period of time. The user area plans should take into account unavailable processing due to a loss of mainframe, LAN, or microcomputer-based system operations.

We recommend that CSE determine a viable alternate processing site that meets CSE's requirements be identified and tested. We recommend that the business continuity plan identify the alternate site that have been approved for business operations and data processing.

We further recommend that the business continuity plan be tested and formally reviewed and approved. The plan should be periodically reviewed and updated when necessary to ensure that it remains appropriate to recovery needs. CSE should ensure that management and staff are adequately trained in the execution of the plan. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location. Since recovery actions may need to be made in concert with ITD or other third parties, we recommend that recovery tests be coordinated with ITD and any other required third parties and that a copy of the plan be available to appropriate ITD and third-party personnel. Moreover, the plan should specify off-site storage of backup media and required physical security and environmental protection of on-site storage of backup media.

Auditee's Response:

> *DOR signed a hot site agreement on January 1, 2006 with SunGuard Recovery services, this contract makes available computer infrastructure for mission critical applications as defined in the ADVIZEX Business Impact Analysis. Currently DOR is working with ADVIZEX and appropriate Tax and Child Support Divisions to develop Business Continuity Plans to be executed in the Fall of 2006.*

Auditor's Reply:

We are pleased that the CSE is in the process of developing a viable and comprehensive business continuity strategy. Once a plan is fully developed and adopted, it should be reviewed and updated annually, or whenever there are significant changes to processing requirements, risks, or changes to CSE's IT infrastructure. The business continuity planning framework needs to also address testing, user reviews and sign-offs, and the development and approval of user area plans. Designation of an alternate processing site and procedures for the generation and storage of backup copies of magnetic media are an integral part of any recovery strategy and should be appropriately addressed and monitored.

3. Inventory Controls over Computer Equipment

Our audit disclosed that CSE's inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in CSE's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being

maintained. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not in place. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders CSE's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although we determined that CSE had documented internal controls regarding the purchasing and receiving of IT resources, we found that documented policies and procedures needed to be enhanced regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. For example, although documented procedures were in place requiring an annual inventory to be conducted at the end of each fiscal year, we could not find documentation to support an annual physical inventory. Also, although CSE had adequate policies and procedures for the disposal of surplus property and Chapter 647 requirements, they were not being followed, as evidenced by CSE's failure to submit required Chapter 647 reports to the Office of the State Auditor.

Our analysis of CSE's inventory system of record indicated that most of the appropriate data fields, including description, identification tag, user name, serial number, and location, were present. However, the listing lacked a data field for historical cost that is required by Commonwealth of Massachusetts regulations for all departments to provide a comprehensive, auditable inventory record of fixed assets. By failing to record the historical cost of purchased computer hardware items and their purchase dates on CSE's inventory system of record, CSE was not in compliance with the Office of the State Comptroller's 2005 fiscal year fixed-asset requirements and Office of the State Comptroller (OSC) Memorandum No. 313A.

With respect to the recording of IT-related assets, we found that CSE lacked appropriate and adequate management oversight to prevent and detect errors in the recording of identifying data for received computer equipment into CSE's inventory system of record for IT equipment. Our tests indicated a significant error rate and inconsistency in identifying data recorded by staff on CSE's computer hardware inventory listing. Specifically, our audit tests comparing data recorded on invoices for purchased computer equipment to the CSE inventory listing detected 27 errors in recorded identifying data for our sample, or an error rate of 13.8% in the recording of serial numbers for the 196 tested hardware items purchased in fiscal year 2004 and 2005. Because of the rate of data input errors, the failure to record asset costs and acquisition dates, and inadequate management of the system of record, an acceptable level of data integrity did not exist for CSE's inventory system of record for IT equipment at

the time of our audit. CSE needs to ensure that appropriate controls are in place for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database.

Our inventory tests were conducted against the 999 IT-related assets on the CSE inventory record. Based on a statistical sample of 209 items of computer equipment selected from the inventory record, we verified by inspection the existence and the recorded location of the computer equipment as listed on CSE's inventory record. We found that all of the 209 items that were selected from the system of record were at the locations as indicated on the inventory record. Moreover, all of the 209 computer equipment items were properly tagged, and the correct serial numbers and manufacturers were listed on the inventory. We further noted that all item descriptions for the 209 items were reasonably correct. Furthermore, to verify the integrity and completeness of the inventory system for computer equipment, we randomly selected 176 additional items of computer equipment as found in actual floor locations and determined that all items were on CSE's system of record. In addition, our audit test of notebook computers indicated that all of the 38 notebook computers tested could be found.

Our audit further indicated that CSE's monitoring of IT equipment inventory needed to be strengthened. Specifically, CSE's senior management had not performed an annual physical inventory during our audit period and could not provide verification records supporting any annual physical inventory or a reconciliation of IT-related equipment to CSE's inventory system of record. The absence of documented policies and procedures regarding inventory verification hindered CSE's ability to ensure the integrity of its inventory system of record as it pertained to IT-related assets.

Our examination of computer equipment that had been designated as surplus property indicated that CSE had complied with Commonwealth of Massachusetts regulations for the disposal of surplus equipment. Adequate documentation was in place to support requests to obtain approval from the State Surplus Property Officer, as outlined in the Surplus Property policies and procedures. However, our audit revealed that CSE had not complied with Chapter 647 of the Acts of 1989 by failing to submit reports of lost or stolen equipment to the Office of the State Auditor. We determined that incident reports over the audit period for 32 missing or stolen IT equipment had been filed with the Inspectional Services Division. However, no reports regarding these incidents had been forwarded to the Office of the State Auditor.

Generally accepted industry standards and sound management practices require that adequate controls be implemented to account for and safeguard fixed assets against loss, theft, or misuse. Chapter 647 of the Acts of 1989, states, in part, "the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that]

periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Moreover, the OSC's "Internal Control Guide for Departments," promulgated under Chapter 647 of the Acts of 1989, notes that fixed assets should be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to manage CSE's inventory system of record. During the course of our audit, we determined that the CSE did not report to the Office of the State Auditor any computer equipment that had been lost or stolen, contrary to Chapter 647.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that CSE strengthen its current practices to ensure compliance with policies and procedures documented in the OSC's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation.

We recommend that CSE perform an annual physical inventory and reconciliation of its IT resources to ensure that an accurate, complete, and valid inventory record of IT resources is in place. We recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical hardware, acquisition, and disposal records. To maintain proper internal control, the periodic reconciliation should be performed by staff who are not responsible for maintaining the inventory system of record. We also recommend that CSE refer to the policies and procedures outlined in the OSC "Internal Control Guide for Departments" to help achieve the goal of ensuring the integrity of the inventory record and enhancing knowledge of the IT infrastructure.

We recommend that the inventory responsibilities for recording, maintenance, disposition, and reconciliation of the inventory and configuration information be defined to provide appropriate segregation of duties and management review and oversight. We believe that it would benefit CSE to use a single inventory system to support inventory and IT configuration management requirements. We recommend that CSE management use the Internal Control Act, Chapter 647 of the Acts of 1989, as a guide for establishing inventory controls regarding the safeguarding of, accounting for, and reporting of IT-related resources. CSE should formalize a process for notifying the appropriate individual responsible for maintaining the IT system of record of any lost, stolen, or missing items.

With respect to IT configuration management, we recommend that the data fields in the IT inventory be expanded to include the cost, condition, and status of the IT resource. In addition, CSE should consider including data fields that record information related to hardware or software maintenance

and whether the IT resource is a core requirement for disaster recovery and business continuity planning. We also recommend that all IT resources be included on the inventory to support IT configuration management objectives. The recommended control procedures should provide increased assurance that all IT-related equipment is recorded on the inventory record in a complete, accurate, and timely manner to enable CSE to produce a complete record of all IT-related equipment on a perpetual basis. CSE's inventory records should reflect any changes to computer hardware items including location or status for both deployed equipment and items held in storage.

Auditee's Response:

> *Remedy will be the repository for maintaining the procurement lifecycle of an asset as well as the inventory. ZenWorks Asset & Compliance Management will be used to discover the assets as well as allow us to view software compliance. ZenWorks will discover any device that is connected to the network and has an IP address.*
>
> *Once a device is discovered by ZenWorks, ZenWorks can gather information on the device if it has the following information and or software. If the device has a Zen client installed it will report to ZenWorks the asset information regarding hardware and software. Other devices such as printers and network infrastructure equipment that have SNMP capabilities and are configured with the read community string active and the community string is configured in ZenWorks can have the asset information discovered as well. All other devices that are on the network will be discovered just as an IP address. This will automate the input of devices in the automated inventory eliminating duplication and errors drastically.*
>
> *The discovery and update process is configurable. DOR plans to integrate this into Remedy so a device is tied to a user or possibly a group in the case of a server or network infrastructure device. DOR is also discussing with the vendor the possibility of integrating ZenWorks and Remedy.*

Auditor's Reply:

We commend the actions initiated by CSE to improve fixed-asset inventory controls. We believe a single comprehensive inventory control system for all CSE fixed assets is an important ingredient for CSE's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding fixed assets and assist CSE in making IT infrastructure and configuration management decisions.

We believe that controls to ensure adequate accounting of fixed assets will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any

lost, stolen, or surplused equipment. In addition, these efforts should help minimize the risk of lost or stolen equipment and improve the identification of the status of equipment for configuration management purposes.

4. Questionable Car Rental Expenses for IT Contracted Employees

Our review disclosed that during fiscal years 2004 and 2005, CSE reimbursed IT-contracted employees $171,679 for rental cars and rental car insurance, and an indeterminate amount in associated gasoline and parking expenses. Our audit determined that, although CSE's policies and procedures require that "Other transportation options such as cabs and subway to and from the job site should be reviewed as a viable and less expensive means of transportation," none of the expense reports involving rental cars included a cost analysis showing that a rental car was more cost-effective than local ground transportation. In addition, CSE's policies and procedures state, "Contractors will be expected to share vehicles when appropriate, and will not be allowed a vehicle per individual." However, documentation generally was not available to show whether cars were used by one or multiple contract employees to drive from the hotel to work site, or used to visit one or multiple locations. Accordingly, it was not possible to determine whether a rental car was more cost-effective than other forms of transportation.

For selected months during fiscal years 2004 and 2005, we were able to glean enough information from the work site location and rental car use to determine local ground transportation should have been less costly. In these instances, considerable personal travel occurred in government funded rental cars. For example, we found that three contract employees worked at the data center and stayed at a hotel 4½ miles from the work site. Accordingly, the contracted employees' official travel miles in the rental car should have been approximately 45 miles during each week of work. However we found that:

- A typical monthly rental car receipt of one contract employee showed that the employee traveled 2,000 miles, which CSE approved for reimbursement.
- Another monthly rental car receipt for a contract employee showed that the employee traveled 1,964 miles, which CSE approved for reimbursement.
- The rental car receipt of the third contract employee showed that the employee traveled 131 miles and purchased $50 in gasoline (thereby averaging less than 5 miles per gallon for the vehicle), which CSE approved for reimbursement.

Although these contracted employees rented these vehicles with unlimited mileage, considerable personal travel occurred in government-funded rental cars. The unlimited mileage privilege is not a license to use the car at will, and allowing such use places the state at risk of costly lawsuits if the vehicle

were involved in an injury accident. Additionally, the Commonwealth paid the gasoline charges for the personal travel.

We reviewed supporting documentation for $10,119 in car rentals by contract employees during the month of March 2005 to determine whether a rental car was cost-effective compared to other forms of transportation. Our analysis determined that contracted employees were not sharing cars and CSE was allowing some contractors "a vehicle per individual." For example, our test indicated that at any one time there were 10 rental cars for 13 contracted employees. In addition, we contacted a local taxi company and determined the trip to the work site from the hotel would take an estimated 5-10 minutes and the estimated rate would be $10 per trip or $20 per day. The rental car cost CSE $250 for 7 days, or $35.71 per day. It should be noted that public transportation was available for each contractor at a cost of only $6 a day, as evidenced by one contract employee who was taking the commuter train to and from work daily. We determined that if all contracted employees had taken the available public transportation instead of renting cars, the cost to the Commonwealth would have been $1,893 for the period, a savings of $8,226 for the month of March 2005 alone.

In all incidents, because there were no cost analyses, the CSE had to rely on the word of the contract employees when approving reimbursement. A more appropriate action would have been to disallow the reimbursement until the contracted employee provided sufficient justification for renting the vehicle and the mileage incurred.

Recommendation:

We recommend that CSE review the reimbursements we have classified in this audit result to determine whether any of those amounts should be repaid to the Commonwealth. We recommend that CSE ensure that all senior management and contract employees be made aware of applicable policies and guidelines regarding the reimbursement of travel expenses. We also recommend that CSE review its procedures and perform cost/benefit analyses to support decisions to use rental cars and ensure that expenses reimbursed to contract employees are reasonable and in accordance with CSE policies and procedures.

Auditee's Response:

The Department agrees with the Auditor's finding and will review submitted expenses for compliance with expense guidelines and possible recovery. The Department will establish a workgroup to review current practice and to institute additional internal controls over the submission and approval of vendor expenses.

Auditor's Reply:

We are pleased that CSE will review the questionable car rental expenses for IT contracted employees to determine whether any amounts should be repaid to the Commonwealth. We agree that establishing a workgroup to review current policies and procedures in order to strengthen internal controls for the submission and approval of vendor travel expenses would be beneficial. We recommend, however; that CSE perform cost/benefit analyses to support decisions to use rental cars and ensure expenses reimbursed to contract employees are reasonable and in accordance with CSE policies and procedures.

GLOSSARY

Term	Definition
Accrual	The sum of child support payments that are due or overdue.
Administrative Process	A statutory system granting authority to an executive agency (instead of courts or judges) to determine child support legal obligations, including paternity establishment, order establishment, enforcement, and modifications.
Arrearage	The total unpaid child support obligation for past periods owed by a parent who is obligated to pay.
Assessment	Putting the child support case together to determine what child support services are appropriate (the first step in the child support enforcement process).
Case	A collection of people associated with a particular support order, court hearing, and/or request for Title IV-D services. A case typically includes a custodial parent, a dependent or dependents, and a non-custodial parent and/or putative father. In addition to names and identifying information about its members, a case includes information such as wage data, court order details, and payment history.
Child Support	Financial resources contributed by non-custodial parents to provide the necessities of living (food, shelter, clothing, medical support) to their children.
Child Support Enforcement Amendments (1984)	Required equal services for AFDC and non-AFDC families, mandatory practices, federal incentives, and improved interstate enforcement.
Child Support Recovery Act (1992)	Made it a federal crime to fail to pay past-due child support obligation for a child living in another state.
Complainant	Person who seeks to initiate court proceedings against another person. In a civil case, the complainant is the plaintiff; in a criminal case, the complainant is the state.
Court Order	A legally binding edict from a court of law by a magistrate, judge, or properly empowered administrative officer. A court order related to child support dictates issues such as how often, how much, or what kind of support a non-custodial parent (NCP) is to pay; how long he/she is to pay it; and whether an employer must withhold support from an NCP’s wages.
Custodial Parent (CP)	Parent who has primary care of the child(ren), which may include having legal custody of the child(ren).

CSE was the source of terms as presented within this glossary.

GLOSSARY

Term	Definition
Custody	Legal custody is a legally binding determination that establishes with whom a child should live. Physical custody is a physical possession of a child, regardless of the legal custody status. Joint custody occurs when two persons share legal and/or physical custody of the child. Split custody occurs when children from the same parents are in the legal, sole custody of different parents.
Default	The failure of a defendant to file an answer or response or appear in a civil case within the required time frame after having been properly served with a summons and complaint.
Default Judgment	A decision made by the court or administrative authority when the defendant fails to respond or appear.
Dependent Child	Any person who has not reached the age of emancipation or been legally declared emancipated.
Disbursement	The paying out of collected child support funds.
Enforcement	A means for obtaining payment of a child or medical support obligation. Enforcement methods include: • Income withholding • State and federal income tax refunds offset • License suspension • Liens against real and personal property
Family Support Act (1988)	Increased emphasis on enforcement remedies, simplified procedures for establishing paternity, and required states to automate procedures.
Garnishment	A legal proceeding whereby a person's property, money, or credit, in the possession of or under the control of a third-party person (garnishee) is withheld from the defendant and applied to the payment of the defendant's debt to the plaintiff.
Good Cause	A legal reason for which a Temporary Assistance for Needy Families recipient is excused from cooperating with the child support enforcement process. Includes cases involving rape, incest, and potential for harm to the custodial parent or child from the non-custodial parent.
Guidelines	A standard method for calculating child support obligations based on the income of the parent(s) and other factors as determined by state law. The Family Support Act of 1988 requires states to use guidelines as the rebuttably correct amount of support for each family.

GLOSSARY

Term	Definition
Income Tax Refund Offset	See Federal Income Tax Offset Program.
Lien	An encumbrance on any real or personal property. Real estate liens (mortgages) are usually filed where the property exists. Personal property liens are either filed statewide or in the county where the owner resides.
Non-Custodial Parent (NCP)	A legal/natural parent who resides outside the home and does not have primary custody of a dependent.
Obligation	The amount of money to be paid as support by the non-custodial parent on an ongoing basis and the manner by which it is to be paid.
Obligee	The person, jurisdiction, or political subdivision to whom a duty of support is owed. Also referred to as the custodial parent when money is owed to the parent who resides with the child.
Obligor	The person owing the duty of support. Also referred to as the non-custodial parent.
Office of Child Support Enforcement (OCSE)	The federal agency within the Administration for Children and Families in the U.S. Department of Health and Human Services that is responsible for the administration of the child support program. OCSE's mission is to assure that assistance in obtaining support (both financial and medical) is available to children through locating parents, establishing paternity and support obligations, and enforcing those obligations.
Payee	The person who, or entity that, receives money from a person paying child support. Used interchangeably with recipient or custodial parent in TANF cases.
Private Case	A support case in which there is no IV-A or IV-D involvement.
Public Assistance	Funds provided from the federal or state government to families in need of and eligible for support.
Social Services Amendments (1975)	Comprehensive child support legislation that enacted Title IV-D of the Social Security Act. Officially established the federal Office of Child Support Enforcement (OCSE).

GLOSSARY

Term	Definition
Stakeholders	Those individuals or organizations who have a legitimate interest in how our customers are served. Stakeholders include: • National or community-based organizations that serve the interests of our customers or partners. • Congressional and state legislators. • Federal, state, and local governments such as welfare, foster care, and Medicaid agencies. • Hospitals, birthing centers, and other places where paternity can be acknowledged. • Employers, taxpayers. • The general public.
Support Order	A legally binding edict from a court of law that dictates conditions of support that a non-custodial parent must pay. It can include how much is paid, how long it is paid, and whether an employer must withhold support from the non-custodial parent's wages. The order can be for child, medical, and/or spousal support.
Title IV-D	Part D of Title IV of the Social Security Act mandates and contains the statutory provisions for the child support enforcement program.
Wage Withholding	A procedure by which automatic deductions are made from wages or income to pay a debt such as child support. The Family Support Act of 1988 required immediate wage withholding for all support, current, and past due.