The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

SUZANNE M. BUMP, ESQ.
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2011-0142-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DEPARTMENT OF REVENUE'S CHILD SUPPORT ENFORCEMENT DIVISION

July 1, 2009 through August 19, 2010

OFFICIAL AUDIT REPORT

JANUARY 31, 2011

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

STATE HOUSE, BOSTON 02133

SUZANNE M. BUMP, ESQ.
AUDITOR

TEL (617) 727-2075
FAX (617) 727-2383

January 31, 2011

Dear Commissioner Bal,

Enclosed is an audit report for your review. This audit of the Department of Revenue covers the audit period of July 1, 2009 through August 19, 2010. This is one of a number of audits commenced and largely completed during the tenure of my predecessor, State Auditor A. Joseph DeNucci. Should you desire more information relative to this audit, please contact me.

I look forward to fostering a cooperative relationship between our respective offices. If my staff or I may be of assistance at any time, please do not hesitate to call upon us. I know we both share the goal of making government work better.

Sincerely,

Suzanne M. Bump, Esq.
Auditor of the Commonwealth

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 Title 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. An 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 authorizing provisions of Chapter 119A of the General Laws. The Office of the Deputy Commissioner directs the strategic planning for CSE and sets operational priorities for its approximately 700 employees.

The mission of CSE is to protect the economic well-being 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. Year-to-date as of May 31, 2010, CSE collected more than $537 million in child support for Massachusetts families and was supported by a budget of approximately $41 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 it 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.

The CSE information technology (IT) infrastructure used to support COMETS and administrative applications consists of local area networks (LANs) installed at the central, regional, and area offices linking over 600 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 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 general control evaluation of the appropriateness of program change procedures to determine whether adequate internal controls were in place to provide reasonable assurance that application program changes are authorized and documented, and that changes are developed, tested, and implemented in a secure environment. Included in our audit was an assessment of the adequacy and effectiveness of controls in place to protect the integrity and confidentiality of data within COMETS.

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 evaluation regarding program change control. We reviewed the appropriateness of program change procedures for the period of July 1, 2009 through August 19, 2010. Our audit scope included an assessment of the adequacy and effectiveness of controls in place to protect the integrity and confidentiality of data within the Commonwealth of Massachusetts Enforcement Tracking System (COMETS). The audit was conducted from July 6, 2010 through August 19, 2010.

Audit Objectives

Our primary audit objective was to determine whether the Division of Child Support Enforcement (CSE) IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that application program changes to CSE's business systems are authorized and documented, and that changes are developed, tested, and implemented in a secure environment. In this regard, we sought to determine whether adequate controls were in place to provide reasonable assurance that IT controls over program changes to application systems were in place and in effect to process all requests (including maintenance and patches) for changes to applications in a standardized and controlled manner. We sought to determine whether IT-related roles and responsibilities for program modification and maintenance were clearly defined, points of accountability were established, appropriate organizational controls were in place, and that appropriate change control and logical access policies and procedures were in place. 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 that provides IT governance over the management control process to minimize the risk of unauthorized disclosure, change, or deletion during the development and implementation of planned changes to application systems.

Audit Methodology

To determine our audit scope and objectives, we initially reviewed IT internal controls to obtain an understanding of CSE's mission and business objectives. Through pre-audit interviews with managers and staff and review of documentation, such as descriptions of the CSE organization and operations, we gained and documented an understanding of the primary business functions supported by CSE's IT systems.

To assess the adequacy of the planning, design, development, and testing of program changes to application systems, we compared the Information System Audit and Control Association's generally accepted standards for change management controls to documentation supplied by CSE for the change control process, including system change requests, project evaluations, risk assessments, program change approvals, resource allocations, testing processes, and program quality assurance. To determine whether requests for system changes were implemented in a structured manner, we reviewed CSE's policies in perspective of the procedures within the change application software used by CSE to define, document, prioritize, and report progress throughout the change control process. We reviewed documentation and evaluated CSE's change application software to determine whether appropriate controls were in place to ensure that emergency changes are approved, documented, justified, developed, tested, and moved to production in a timely manner.

With respect to logical access security, our audit included a review of logical access privileges of those programmers and developers authorized to access the network and associated IT systems. Through interviews, observation, and review of documentation, we sought to determine that only authorized programmers and developers were granted access to test and production source libraries. To determine whether the administration of logon ID's and passwords were properly carried out, we interviewed the Accounts Team Manager responsible for control practices regarding system security associated with access to test and production file servers. To determine whether controls in place were adequate to ensure that logical access privileges to IT systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application systems and related data files. Further, we determined whether all employees authorized to access IT systems were required to periodically change their passwords and, if so, the frequency of the changes.

AUDIT CONCLUSION

Our review of the Division of Child Support Enforcement (CSE) found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to program changes to application systems and logical access security. Our review also indicated that CSE had an adequate IT related internal control environment, including policies, procedures, practices, and organizational structure, to provide reasonable assurance that application program changes to CSE's business systems are properly authorized and documented. Regarding logical access security for program changes, we found there were strong controls in place to restrict access to only authorized users including programmers and developers that make modifications to CSE's application systems.

Based on our interviews with CSE management and review of CSE's change application software, we found that appropriate controls and procedures were in place to initiate, communicate, track, monitor, and approve modifications to programming code to meet specified approved objectives. We found that the initial work request is electronically entered into a change order problem log (COPL) database tool, which begins the process of changes to application systems. The request in turn moves to a shipping database where the developer, project manager, or project leader identifies the applications that need to be changed, the source code, and assigns duties and deployments. Consideration is also given by the approvers towards collateral impact to departments that are affected by the change request. Upon approval by management of the requested changes, the COPL electronically generates an email that is sent to all parties with an attachment that contains the script necessary to initiate the changes.

We found from our review that, upon receipt of the appropriate approvals, the configuration management department exports data from the COPL and populates CSE's project management software application with the appropriate information. The information in the project management application is then used to manage the change management process from inception to completion including quality assurance and subsequent movement to production.

Based on our review, we found that the change application software is used throughout the change management process to closely manage progress and ensure that requested changes are made in compliance with existing rules, regulations, and policies and procedures. In addition, we found that appropriate controls were in place to process emergency changes that include a review by the management team and assignment of a priority status in relation to existing change requests that are in the process of being implemented.

Concerning logical access security with regard to programmers and developers, we found that adequately documented policies and procedures were in place to restrict access to only authorized individuals within CSE's local area network and development servers. Our audit revealed that CSE had procedures in place that provide for password creation, deletion, logon, and password configuration requirements. In addition, we found that all new-hires or contractors sign the appropriate confidentiality agreements and that there is separation of duties by having the Inspectional Service Division conduct a Criminal Offender Record Information check and tax inquiry check.

We found that CSE has a secure process in place to approve and activate new user accounts for programmers and developers that require access for change management purposes to CSE's application systems. Upon receipt of appropriate approval for a new user account, user identification information is entered into a tracking application system that electronically assigns an incident number that is associated with a specific project and can be used to follow the progress of all developers associated with their respective change management project. We determined that CSE uses a tracking application system that manages all reporting and security lock-down of all employee and contractor changes of status including termination and transfers to other departments. Our review also indicated that CSE periodically monitors active user accounts to ensure that only authorized users are accessing CSE systems and that all user accounts are disabled for terminated or transferred employees or contractors.

Auditee's Response

> *The Department of Revenue strives to be an information security leader in the Commonwealth. Every effort is made to ensure that the information provided to us by our customer base is protected according to industry best practices and compliance requirements. The agency agrees with the audit results and conclusions.*

Auditor's Reply

We suggest that other Divisions within DOR benchmark their change control practices against those employed by the Division of Child Support Enforcement to ensure that generally accepted practices are in place on an enterprise-wide basis.