The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

No. 2010-1231-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE PROBATE AND FAMILY COURT DEPARTMENT BRISTOL COUNTY DIVISION

July 1, 2009 through March 24, 2010

OFFICIAL AUDIT REPORT

JUNE 14, 2010

TABLE OF CONTENTS

INTRODUCTION

The Probate and Family Court Department-Bristol County Division (the Court), is authorized by Chapter 211B, Section 1, of the Massachusetts General Laws. The Court services twenty cities and towns in Bristol County with a main office in the city of Fall River and courthouses in New Bedford and Fall River. The Court has jurisdiction over family-related matters such as divorce, child support, paternity establishment, family, elderly and disabled abuse protection, and adoption. In addition, the Court maintains exclusive jurisdiction over probate matters, such as wills, trusts, guardianships, and conservatorships. The Court consists of a First Justice, three Associate Justices, a Register of Probate, a Chief Probation Officer, and 65 employees.

The Administrative Office of the Trial Court (AOTC) provides management and fiscal oversight to the seven Trial Court departments, including the Probate and Family Court departments. The AOTC, which also overseas, the Office of the Jury Commissioner and the Office of the Commissioner of Probation, maintains the master inventory records for property and equipment for courts located throughout the Commonwealth. The AOTC's Information Technology Department located in Boston provides technical support to the individual courts. The AOTC also provides the courts with information technology (IT) resources, as well as IT policies guidelines and procedures. The AOTC administers the Court's IT infrastructure, including mission-critical applications that are installed on file servers located in Boston.

At the time of our audit, the Court's computer operations included 81 workstations. The Register of Probate's Office utilized 55 workstations, the Probation Department utilized 20 workstations, and six workstations are for public use. The Court also had switches and hub networking equipment that provided connectivity through T1 lines to the AOTC wide area network allowing access to the primary computer applications administered by the AOTC. The MassCourt application, which is the primary system used by the Court, is a comprehensive case management system that provides case entry, docketing, scheduling, case-related financial management, automated reports, notices and forms, and electronic storage of case documents available through the Trial Court Intranet. The MassCourt system allows the Trial Court to manage all case-related information and enable all departments and divisions of the Trial Court to share information and monitor and track cases as they proceed through the legal system. In addition, the Probation Department uses the Criminal Activity Record Information (CARI) system to access information on all cases involving guardianship or restraining orders, and also utilizes the Registry of Motor Vehicles (RMV) application system for identification purposes. The Court relies on the Commonwealth's Information Technology Division (ITD) for access to the Massachusetts Management and Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS). In addition the Court uses Microsoft Office for a variety of administrative functions.

The Office of the State Auditor's audit was limited to an examination of certain IT general controls over and within the Court's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Probate and Family Court Department-Bristol County Division. Our audit, which was conducted from January 11, 2010 through March 24, 2010, covered the period of July 1, 2009 through March 24, 2010. Our audit scope included an examination of IT-related general controls over system access security pertaining to user account management and password administration, inventory control over computer equipment, and on-site and off-site storage of backup copies of the applications residing on the Court's microcomputer workstations. In addition, we conducted a user satisfaction survey regarding the functionality and reliability of the mission-critical MassCourt application system.

Audit Objectives

Our primary objective was to determine whether selected IT-related controls were in place and in effect to support the Court's IT processing environment. In this regard, we sought to determine whether adequate policies and procedures, were in place to provide reasonable assurance that control objectives pertaining to user account management, inventory control of computer equipment and electronic backups of applications residing at the Court, would be achieved to support business functions.

Our system access security objective was to determine whether adequate controls were in place and in effect to provide reasonable assurance that only authorized users for the Court were granted access to the AOTC network and the MassCourt application. We evaluated whether activation and deactivation procedures were in place to ensure that only authorized individuals had access privileges to the Court's automated systems and IT resources. A further objective was to determine whether appropriate control practices were in effect regarding user IDs and passwords to the MassCourt application system accessed from the Court.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded and accounted for and safeguarded against unauthorized use, theft, or damage. In addition, we sought to determine whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647 reporting requirements.

We sought to determine whether adequate procedures for on-site and off-site storage of backup media for the applications residing on the Court's microcomputers were in place and in effect. We sought to determine whether these controls would provide reasonable assurance that critical and essential spreadsheets and documents could be regained within an acceptable period of time should a disaster render the Court's computerized functions inoperable or inaccessible.

We also sought to identify the level of satisfaction of Court management and staff regarding the functionality, reliability and integrity of the MassCourt application system.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of the Court's relevant operations and information technology control environment. To obtain an understanding of the internal control environment, we reviewed the Court's organizational structure and primary business functions and relevant policies and procedures. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding system access security, we examined the procedures used to authorize, activate, and deactivate access privileges for both the network and the MassCourt application. To determine whether only authorized employees were accessing the automated systems, we obtained system-generated user lists from AOTC for individuals granted access privileges to the network and the MassCourt application and compared the lists to an official Court personnel listing. In order to verify that all users were current employees, we obtained a system-generated user account list containing 65 network user accounts, 60 MassCourt user accounts, and 15 CARI and 15 RMV user accounts. We compared the user account lists to a current Court employee roster. To determine the adequacy of controls of user IDs and passwords we interviewed both Court and AOTC personnel regarding the frequency of password changes and reviewed control practices regarding logon ID and password composition and administration. We examined whether all individuals authorized to access system applications were required to change their passwords periodically and to determine the frequency of the changes

To determine whether adequate controls were in place and in effect to properly account for the Court's computer equipment, we reviewed inventory control policies and procedures. We obtained AOTC's inventory system of record, dated January 6, 2010, which consisted of 109 items. We determined whether the record contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. To determine whether the system of record for computer

equipment was current, accurate, complete and valid, we tested 100% of the computer equipment and determined whether there had been any equipment acquisitions or disposals during the audit period. We verified the location, as well as, the serial numbers and inventory tags of the computer equipment listed on the inventory record to the actual equipment on hand.

To determine whether the Court complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting AOTC's performance of an annual physical and reconciliation inventory of IT assets. We also reviewed the Court's process for complying with Commonwealth of Massachusetts regulations for disposal of surplus property. Finally, to determine whether the Court was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed for the existence of incident reports for missing or stolen IT-related equipment for the audit period, and verified whether all incidents were reported to the Office of the State Auditor.

We assessed whether the Court was generating backup copies of the applications, spreadsheets and documents located on the workstations located at the Court. In addition, we reviewed the process of the generation and storage of the backup copies of magnetic media on-site but did not review the off-site location.

To gain an understanding of the level of user satisfaction of the MassCourt application, we conducted user surveys with a cross section of nine management and staff members from the Register's Office, the Probation Department, and the Judge's Lobby. The results of the surveys were intended to provide feedback from users regarding system response time, application functionality, training, IT support, user comfort level, and overall satisfaction of the MassCourt application.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the 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 version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Our audit at Probate and Family Court Department-Bristol County Division found that controls in place provided reasonable assurance that IT-related control objectives would be met regarding inventory control of computer equipment and the generation of backup copies of applications and essential documents residing on the Court's workstations. In addition, our user survey of the MassCourt application revealed that users were generally satisfied with the functionality and reliability of the application. However, our audit revealed that in the area of access security, controls needed to be strengthened for password administration for the MassCourt application system.

Regarding system access security, we found that user management controls were in place and in effect for the application systems utilized by the Court and provided reasonable assurance that users were properly authorized to access the systems. Although we found that there were procedures in effect for the activation and deactivation of user access privileges, our tests of user account management of the MassCourt application revealed that of the 60 user accounts, 58 were current employees and two accounts were for former employees. Our audit revealed that these two accounts did not have network access, and through confirmation with AOTC, that the accounts had not been accessed since the employees' termination dates. In addition, these user accounts were promptly deactivated when brought to AOTC's attention. In regards to the test of network users, we found that all 65 users were current employees of the Court. In addition, our audit test confirmed that all user accounts to the CARI and RMV systems were employees of the Court.

Our audit revealed that policies and procedures needed to be implemented, presumably by AOTC, to ensure an appropriate frequency of password changes over the MassCourt application system. Our audit test revealed that a mandatory time frame had not been established for changing passwords and, as a result, passwords for system users had not been changed on a regular basis. In some cases MassCourt users at the Court had not changed their password since the implementation of the system in 2008. Furthermore, our audit also revealed that the requirements for password composition and length needed to be strengthened.

With respect to inventory control over computer equipment, we found that a complete and accurate list of computer equipment was being maintained. The inventory list, which assists Court management in identifying IT resources under its control, is maintained by the AOTC to help ensure that the official system of record for property and equipment is accurate and complete for IT resources allocated to the Court. We confirmed that the AOTC performed a physical inventory and reconciliation to address

accounting requirements promulgated by the Office of the State Comptroller. Our audit test of the 109 computer hardware items indicated that all items were located, properly accounted for, and tagged. However, we believe that including lease expense cost for all computer equipment deployed would enhance the computer equipment inventory record. In addition, we found that the Court had procedures in place to ensure compliance with reporting requirements of Chapter 647 of the Acts of 1989.

Regarding backup and storage of applications systems residing on workstations at the Court, we determined that control practices were in place and in effect to provide reasonable assurance that important documents and spreadsheets could be recovered at the Court in a timely manner should the workstations be inoperable for an extended period. Our audit disclosed that the AOTC uses an automated software product to perform nightly backups to AOTC's servers in Boston. Our review indicated that AOTC utilized a third-party vendor for it's off-site backup and storage of electronic media.

Regarding our survey of user satisfaction of the MassCourt system, we found that the users were generally satisfied with the system and that it had improved user productivity. We found that the system was capturing critical information, and users found the data to be reliable, complete and accurate. A common issue that users raised about the system was that the response time slowed at peak processing hours forcing the delays in processing Court documents. Users also expressed concerns over certain limited printing capabilities, and that the volume of file folders had dramatically increased due to a change in how the MassCourt system classifies information.

AUDIT RESULTS

User Account Management

Our audit revealed that the Court, in conjunction with AOTC management, needed to implement stronger policies and procedures to ensure an appropriate frequency of password changes over the MassCourt application systems and that the composition and length of the passwords needed to be strengthened. We found that although AOTC and the Court had access security procedures in place, such as the activation and deactivation of user accounts, control policies and procedures requiring users to change their passwords on a regular basis needed to be strengthened. We found that AOTC's internal controls stated that passwords and identification codes must be considered confidential information and department heads must ensure that passwords are changed periodically according to Trial Court standards.

Regarding our examination of password administration for the mission-critical MassCourt application system, we found that management had not established a mandatory timeframe for changing passwords. Our audit indicated that many users have maintained the same password since being initially trained on the system. Insufficient control practices for password administration controls over password administration places the Court at a high level of increased risk for unauthorized access to sensitive data residing on its mission-critical application. The failure to use generally accepted procedures for password composition and use places the Court at risk of unauthorized access to the MassCourt application by anyone having, or gaining access to the AOTC network. As a result, individuals could also gain a higher level of access privileges than they were initially authorized to have for this application system.

CobiT's control practices recommend that organizations have password policies that include "an appropriate and enforced frequency of password changes." In addition, computer industry standards advocate that policies and procedures for all aspects of system access security be documented and approved to provide a basis for IT systems and data. The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access.

Recommendation

We recommend that the AOTC develop written comprehensive policies and procedures to address password administration. The polices and procedures should include the length and composition of passwords (a minimum of eight alpha/numeric characters), frequency of password changes, establishment of audit trails, and procedures to be followed in the event of unauthorized access or access attempts are

detected. Further, we recommend that the AOTC management implement system changes or defaults that prompt users to change their passwords within an established timeframe.

Auditee's Response

Pursuant to the audit conclusions reached by your office, it appears that of the 60 user accounts associated with MassCourts, 2 of those users have since retired from their employment with the Trial Court. To rectify this discrepancy, I will be contacting the AOTC to immediately remove those 2 user accounts from the MassCourts system. Further, in response to your finding of insufficient control practices for passwords administration, I will work in conjunction with the AOTC to ensure that policies and procedures are implemented for the purpose of strengthening said controls. Specifically, I will advise the AOTC to set up and implement guidelines to ensure that password composition is strengthened and that mandatory time frames for changing passwords are implemented.

Auditor's Reply

We commend the Court's action for addressing the security concerns related to user account management. Further, we believe that by implementing and monitoring password administration policies and procedures the Court, in conjunction with AOTC, will enhance access security controls over its application systems.