Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued September 22, 2011

Plymouth Division of the Probate and Family Court Department

For the period July 1, 2008 through December 31, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Massachusetts Trial Court was created by Chapter 478 of the Acts of 1978, which reorganized the courts into seven Trial Court Departments: the Boston Municipal Court, the District Court, the Housing Court, the Juvenile Court, the Probate and Family Court, the Superior Court, and the Land Court. Chapter 217 of the Massachusetts General Laws authorizes the Probate and Family Court Department, which is established into 14 divisions, each having a specific territorial jurisdiction to preside over probate and family matters brought before it. The Plymouth Division of the Probate and Family Court Department (the Court) has jurisdiction over family-related matters such as divorce, support, paternity establishment, family and elderly abuse protection, disabled person abuse, protective custody, and adoption. In addition, the Court maintains exclusive jurisdiction over probate matters, such as wills, trusts, guardianships, and conservatorships. The Court, which has a primary location in the town of Plymouth and a satellite location in Brockton, serves 26 towns within Plymouth County and the City of Brockton.

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of information technology (IT) controls at the Court for the period July 1, 2008 through December 31, 2010 The scope of our audit included a general control examination of internal controls related to physical security, environmental protection, system access security control, inventory controls over computer equipment, disaster recovery and business continuity planning, and off-site storage of magnetic media. We also reviewed the Court's controls over the protection and storage of personally identifiable information.

Based on our review, we have determined that, except for those issues noted in the Audit Results section of the report, for the period July 1, 2008 through December 31, 2010, the Court maintained adequate internal controls for the areas tested.

Our test of computer equipment revealed that, contrary to the Administrative Office of the Trial Court (AOTC) Fiscal Systems Manual, the Court had not performed annual reconciliations of its inventory record. Moreover, we found discrepancies between the inventory record being maintained by the Court and the official system of record being maintained by AOTC. Specifically, we found that the Court had 119 computer desktops listed on its inventory record, whereas AOTC had only 102 computer desktops listed on its inventory for the Court. We found that the computer equipment inventory was not being monitored or reconciled due to a lack of communication of inventory responsibilities between the Court and AOTC.

INTRODUCTION

Background

The Massachusetts Trial Court was created by Chapter 478 of the Acts of 1978, which reorganized the courts into seven Trial Court Departments: the Boston Municipal Court, the District Court, the Housing Court, the Juvenile Court, the Probate and Family Court, the Superior Court, and the Land Court. Chapter 217 of the Massachusetts General Laws authorizes the Probate and Family Court Department, which is established into 14 divisions, each having a specific territorial jurisdiction to preside over probate and family matters brought before it. The Plymouth Division of the Probate and Family Court Department (the Court) has jurisdiction over family-related matters such as divorce, support, paternity establishment, family and elderly abuse protection, disabled person abuse, protective custody, and adoption. In addition, the Court maintains exclusive jurisdiction over probate matters, such as wills, trusts, guardianships, and conservatorships. The Court has a primary location in the town of Plymouth and a satellite location in Brockton, serves 26 towns within Plymouth County and the City of Brockton. The Court consists of a First Justice, three Associate Justices, a Register of Probate, a Chief Probation Officer, and a Chief Court Officer. At the time of our audit, the Court had 55 employees.

At the time of our audit, the Court's computer operations were supported by workstations configured in a local area network. The workstations are connected through T1 lines to the Administrative Office of the Trial Court (AOTC) wide area network (WAN), allowing access to AOTC's primary computer application systems. The primary application system used by the Court is MassCourt, 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 AOTC intranet. The system allows AOTC to manage all case-related information and enables all departments and divisions of AOTC, on a limited, controlled basis, 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 the Registry of Motor Vehicles (RMV) system for identification purposes. The Court relies on the Commonwealth's Information Technology Division (ITD) for access to the Massachusetts Management 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.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of information technology (IT) controls at the Plymouth Division of the Probate and Family Court Department. Our audit covered the period July 1, 2008 through December 31, 2010.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with 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) issued by the Information Systems Audit and Control Association, July 2007.

The scope of our audit included a general control examination of internal controls related to physical security, environmental protection, system access security control, inventory controls over computer equipment, disaster recovery and business continuity planning, and off-site storage of magnetic media. We also reviewed the Court's controls over the protection and storage of personally identifiable information. The primary objective of our audit was to determine whether IT-related controls were in place and in effect to support the Court's IT processing environment. In this regard, we determined whether the internal control environment, including policies, procedures, and practices, provided reasonable assurance that control objectives would be achieved to support business functions. We also determined whether adequate physical security and environmental protection controls were in place and in effect at both the main and satellite courthouses to prevent and detect unauthorized access to areas housing IT resources, damage, or loss of IT-related assets.

Our objective regarding system access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to the Court's applications systems and data files. We evaluated whether procedures were in place to prevent

unauthorized user access to automated systems and IT resources. In addition, we determined whether the data residing on the MassCourt application was sufficiently protected against unauthorized access, and whether the Court was actively monitoring password administration.

We determined whether adequate controls were in place and in effect to provide reasonable assurance that IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. In addition, we determined whether an annual physical inventory and reconciliation had been conducted.

Regarding system and network availability, we determined whether the Court, in conjunction with AOTC, had developed a disaster recovery and business continuity plan that would provide reasonable assurance that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render IT processing inoperable or inaccessible. Moreover, we determined whether adequate controls were in place to provide reasonable assurance that appropriate backup copies of application systems and data files would be available off-site to support disaster recovery and business continuity planning objectives.

Based on our review, we have determined that, except for the issues noted in the Audit Results section of the report, for the period July 1, 2008 through December 31, 2010, the Court maintained adequate internal controls for the areas tested.

AUDIT RESULTS

1. IMPROVEMENTS NEEDED IN INVENTORY CONTROLS OVER COMPUTER EQUIPMENT

We found that fixed-asset controls related to information technology (IT) needed to be strengthened to provide for the proper accounting of computer equipment maintained on the inventory system of record by the Administrative Office of the Trial Court (AOTC) and the Plymouth Probate and Family Court Division. Our audit revealed that both AOTC and the Court were responsible for maintaining a complete, valid, and current inventory record and reconciling the inventory on an annual basis; however, there was not a clear understanding of specific duties and responsibilities to ensure that the inventory records were accurate, valid, complete, and current. We found that even though the AOTC Fiscal System Manual requires that a reconciliation of inventory records be conducted on an annual basis, the Court last conducted an annual physical inventory and reconciliation on June 30, 2008.

We noted that although AOTC's master inventory record for the Court listed 102 computer desktops, the inventory record maintained by the Court listed 119 computer desktops. Our audit test of the Court's inventory revealed that all equipment listed was located at the Court's designated locations; however, the Court's inventory record contained 20 items not listed on the AOTC inventory record. In addition, other IT-related items physically located at the Court, such as switches, servers, hubs, routers, and printers, were not listed on either the Court's or the AOTC's inventory listing. Moreover, we found that although the AOTC inventory contained data fields pertaining to acquisition dates, purchase order and lease agreement information, historical cost, and equipment condition, AOTC did not input this critical information for any of these data elements. Accordingly, due to the lack of accurate listings and complete cost amounts on the inventory records, an accurate total value for the inventory could not be determined.

The weaknesses in inventory control were the result of a lack of a collaborative effort between AOTC and Court management as well as a failure to monitor assigned responsibilities regarding the accounting for and safeguarding of IT-related assets. The absence of an accurate inventory record may hinder the AOTC's ability to manage IT-related resources and to detect theft and unauthorized use of IT-related assets. Moreover, the lack of an up-to-date and accurate inventory hinders the Court's ability to assess its future technology and configuration management needs.

Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, 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 assign qualified individuals for that purpose, and 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.*

Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. Furthermore, the AOTC Fiscal Systems Manual requires each court to maintain a perpetual inventory, verify the inventory on an annual basis, and reconcile the record to the AOTC master record listing.

Recommendation

The Court should perform an immediate reconciliation of all IT-related assets and resubmit to AOTC a complete record of all IT-related items located at the Court. Further, the Court should maintain a perpetual inventory of computer equipment and ensure that AOTC records purchase order numbers, historical cost data, acquisition dates, and condition of equipment on the system of record. We also recommend that AOTC provide the Court with timely information regarding any changes to equipment deployment or removal so that an accurate perpetual inventory is maintained.

Auditee's Response

> *We are cognizant of the necessity of having accurate inventory records which are in reconciliation with the records of the Administrative Office of the Trial Court (AOTC) Information Technology Department (ITD). We shall immediately re-submit a complete record of all IT related equipment to AOTC ITD and work with that office to reconcile all essential IT inventory records of our two entities. In that effort we shall endeavor to include essential purchase data, identifying information and condition so that the records of both entities are current and in agreement.*

2. IMPROVEMENTS NEEDED IN CONTROLS OVER PASSWORD ADMINISTRATION

Our audit revealed that system access security controls over the Court's mission-critical MassCourt application needed to be strengthened to ensure that personal and confidential information residing on the application system (MassCourt) is adequately protected from

unauthorized access. Specifically, we found that although AOTC maintains a central register of account users, application users are not required to change their passwords beyond their initial logon to the system. In fact, we found that since the implementation of the MassCourt application in February 2005, users have never been prompted to change their passwords. In addition, initial access to the AOTC network requires only a generic password that cannot be changed by users. We found that although the Court, in conjunction with AOTC management, had limited policies pertaining to system access security, there is no requirement for users to change their passwords on a regular basis. The failure to change passwords on a regular basis for user accounts places the Court and AOTC at risk of unauthorized system access. In addition, we found that policies are not in place regarding password composition, length, restrictions on sharing, and user account monitoring. Without a comprehensive, formal set of password security policies and procedures in place, AOTC's automated systems and data are at risk of unauthorized access, modification, or loss.

The Information Systems Audit and Control Foundation's (ISACF) Control Objectives for Information and Related Technology (CobiT) guidelines for ensuring system security states that organizations should have password policies that include an appropriate and enforced frequency of password changes. Further, computer industry standards advocate that policies and procedures for all aspects of system access security be documented and approved to provide a basis for managing system security. These 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

The Court and AOTC should develop written policies and procedures to address password administration, including the length and composition of passwords, frequency of password changes, establishment of audit trails, and procedures to be followed in the event of unauthorized access attempts or unauthorized access. Further, we recommend that the Court and AOTC management implement system changes or defaults that will prompt users to change their passwords within an established timeframe.

Auditee's Response

We recognize the importance of maintaining an effective password management program. As you well know, this requires a coordination of our efforts with the AOTC ITD, which oversees the entire Trial Court IT operation. We shall work with the AOTC ITD to develop appropriate written policies and procedures to implement and refine practices that will address the audit recommendations in this sensitive security area.

3. BUSINESS CONTINUITY PLAN NEEDS TO BE DEVELOPED

Our audit revealed that the Court, in conjunction with AOTC, had not developed a documented disaster recovery and business continuity plan that would provide reasonable assurance that mission-critical data processing and business operations could be regained effectively and in a timely manner in the event of an emergency. In addition, the Court had not developed comprehensive, documented, and tested individual contingency plans to address the potential loss of automated processing. Without adequate contingency planning, including required user area plans, the Court is at risk of not being able to regain mission-critical business operations within an acceptable period of time. An extended loss of processing capabilities could adversely affect the Court's ability to perform its primary business functions and could result in significant delays in processing caseloads.

We found that there was no documentation available that clearly identified responsibilities associated with the development and execution of comprehensive, detailed user area procedures and contingency plans to address the loss of automated systems for an extended period of time. Although the Court was able to articulate the procedures needed to be performed under various disaster scenarios to regain business functions, none of these strategies has been formally documented or tested. For example, although Court management indicated that business could be conducted at either of its locations, this strategy has never been documented or tested. The Court needs to identify the nature and extent of judicial or business activities that could be conducted in the absence of AOTC-supported systems or in the event of damage or inaccessibility to the Court's facilities.

Court management informed us that under a disaster scenario in which the Court could not conduct business on a short-term basis, it could relocate to an alternate Court and be able to schedule hearings and use the MassCourt application for docketing and data input. These alternate processing sites could be used until another facility is selected or the original site is restored. It is our understanding that on a long-term basis, the AOTC's centralized Information

Technology Division could reconfigure a server at a facility or site to be determined based on the circumstances of a long-term or permanent move. However, since the overall plan and strategies have not been formally documented and approved, and the work-around plans have not been documented or tested, the Court may be at risk of not regaining mission-critical and essential business functions in a timely manner. Without a comprehensive, documented, and tested business continuity plan, including required user area plans, the Court would be hindered from performing essential business functions.

Recommendation

The Court, in conjunction with AOTC, should develop, fully document, and test disaster recovery and contingency plans, including detailed user area plans specific to the Court's operations. The Court should also document its strategy of conducting business at other court locations and perform an assessment of criticality and business impact at least annually, or upon major changes to Court operations or the IT environment. In addition, the Court, in conjunction with AOTC, should perform a risk analysis of the systems to gain a better understanding of associated risks and the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could render the IT infrastructure inoperative, the cost of recovering the systems, and the likelihood of threats and disaster scenarios and the potential frequency of occurrence. Moreover, the Court should obtain adequate assurance from entities that provide IT capabilities, or other essential services, that the IT or other services can be recovered within an acceptable time to support the Court's mission-critical business functions.

The business continuity and contingency plan, including user area plans, should document the Court's recovery and contingency strategies with respect to disruptions to business operations. The plan should contain all pertinent information, including clear assignment of key personnel and their roles and responsibilities, needed to efficiently resume business operations in a timely manner. Accordingly, we recommend that detailed business continuity user area plans be tested and periodically reviewed and updated, as needed, to ensure their viability and that the completed plans be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response

We understand the significance of developing a more formal written policy addressing continuity of operations in the event of any type of disaster. The court has its locations in Brockton and Plymouth which we feel provides us flexibility to adapt to most business interruption scenarios. We shall contact the AOTC and the AOTC ITD in order to develop a written coordinated business continuity and recovery plan in the event of any interruption of our normal operations. Responsibilities of the various entities involved in such an effort shall be clearly designated. At our court level, the responsibilities of all key personnel shall also be clearly set forth. Provisions shall be made to test the effectiveness of the plan and to distribute copies of the plan to all involved staff members.

.