The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DENUCCI
AUDITOR

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

No. 2009-1122-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE PLYMOUTH COUNTY SUPERIOR COURT

July 1, 2007 through October 30, 2009

OFFICIAL AUDIT REPORT

APRIL 9, 2010

TABLE OF CONTENTS

INTRODUCTION

The Plymouth County Superior Court was established under the authority of Chapter 211B, Section 1, of the Massachusetts General Laws, as amended. The Court has exclusive original jurisdiction in first-degree murder cases and for all other crimes, has jurisdiction over felony matters, and shares jurisdiction over crimes where other Trial Court Departments have concurrent jurisdiction. The Court also has jurisdiction in civil actions over $25,000 and in matters where equitable relief is sought. In addition, the Court has original jurisdiction in actions involving labor disputes where injunctive relief is sought and has exclusive authority to convene medical malpractice tribunals. The Court has offices in the City of Brockton and in the Town of Plymouth, both located in Plymouth County.

The Plymouth County Superior Court is divided into two functional offices, the Clerk's Office and the Probation Department. The Clerk's Office processes restraining orders, small claims, appeals, motor vehicle infractions, and maintains the Court's records, case dockets, and files. The Probation Department collects and disseminates important records to courts and other state agencies through investigations, community supervision of offenders/litigants, maintenance of crime statistics, mediations, service to victims, and the performance of other appropriate community service functions.

At the time of our audit, the IT operations at the Court's Brockton location were supported by 43 workstations that were configured through three host file servers and connected to the Administrative Office of the Trial Court's (AOTC) wide area network (WAN) that provides access to AOTC's servers and primary application systems. There were 18 workstations assigned to the Clerk's Office, 12 assigned to the Probation Department, five located in the judge's lobby, four in the courtrooms, two in the docket room, and two for public use. In addition, the Plymouth location's IT configuration consisted of 19 workstations, of which 14 were assigned to the Clerk's Office, four in the Probation Department, and one in the Judge's Lobby. As part of the judicial branch, the Court receives guidance and oversight from AOTC. AOTC's Information Systems Department, which is located in Boston and Worcester, provide information technology (IT) services and technical support to individual courts.

The primary application systems used by the Court are the ForecourtVision application, which is a Windows-based application system that uses client-server technology for electronically recording docket information, and the Warrant Management System, which is used to track warrants issued and warrant information from all courts. In addition, the Probation Department uses the Criminal Activity Record Information (CARI) system to track all dispositions from courts regarding criminal and juvenile offenses and restraining orders. The Probation Department uses a Quicken software package, in lieu of the Probation Receipts Accounting System, to account for all fines and fees processed through the Probation

Department. The Court uses the Massachusetts Management Accounting and Reporting System (MMARS) to track the revenues and expenditures during the fiscal year as well as the Human Resources Compensation Management System (HR/CMS) to track human resource information.

The Office of the State Auditor's examination was limited to a review 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 a follow-up audit of certain information technology-related controls at the Plymouth County Superior Court. Our audit, which was conducted from July 17, 2009 through October 30, 2009, covered the period of July 1, 2007 through October 30, 2009. The scope of the audit consisted of an evaluation of the status of prior audit results disclosed in our prior report, No. 2003-1122-4T, issued May 12, 2003 regarding IT-related policies and procedures, physical security, environmental protection, system access security, inventory control of computer equipment, and business continuity planning. In addition, we reviewed policies and procedures regarding the protection of personally identifiable information.

Audit Objectives

Our primary audit objective was to determine whether corrective action had been taken to strengthen IT-related internal controls for physical security and environmental protection over computer equipment, inventory control of computer equipment, and business continuity planning. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access or damage to, or loss of, IT-related assets and to provide general security controls for the protection of court staff and the general public. Our objective regarding system access security for user account management was to determine whether adequate controls were in place and in effect for the activation, maintenance, and deactivation of access privileges to ensure that only authorized personnel had access to the network from which additional application-specific access requirements must be met. We also reviewed application-specific access to the Warrant Management System and to the ForecourtVision application system utilized by the Court. We did not review specific access security to CARI, MMARS or HR/CMS.

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 determined whether an effective business continuity plan was in place that would provide reasonable assurance that mission-critical and essential operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable. We also sought to determine whether adequate policies and procedures were in place regarding the protection of personally identifiable information.

Audit Methodology

To evaluate whether corrective action was taken on the recommendations presented in our prior audit report, No. 2003-1122-4T, we performed pre-audit work that included a review of prior audit workpapers and gaining an understanding of the Court's current IT environment. We reviewed our prior recommendations regarding documented IT-related policies and procedures, physical security, environmental protection, system access security, fixed asset inventory, and business continuity planning. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected IT-related activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of the adequacy of IT-related policies and procedures, we interviewed Court management and staff to identify IT functions and responsibilities and evaluated the degree to which documented policies and procedures addressed those functions. We reviewed the IT-related policies and procedures to assess whether they provided guidance to Court staff.

To evaluate physical security, we interviewed senior management and security personnel, conducted physical inspections, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment as well as general security for the Brockton and Plymouth courthouse locations. We examined controls, such as office door locks, locked entrance and exit doors, windows security, presence of personnel at entry points, and whether the courthouse was equipped with an intrusion alarm. We reviewed management policies and procedures regarding the management of keys to obtain entry to offices inside the Court.

To determine whether adequate environmental controls were in place to properly safeguard areas housing computer equipment from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in place, we inspected the file server room to confirm the presence of appropriate dedicated air conditioning, heating, and ventilation systems. In addition, we reviewed environmental protection controls related to general housekeeping procedures in the file server room, as well as selected areas housing computer equipment. Audit evidence was obtained through interviews and observation.

Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the ForecourtVision and Warrant Management application systems that are accessed through workstations located throughout the Court. To determine whether only current Court

employees had authorized access, we obtained system-generated user lists from AOTC for the network and the ForecourtVision and Warrant Management application systems and compared the lists to the employee payroll roster. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to the Court personnel. 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. We reviewed control policies and practices regarding logon ID and password administration and evaluated user account authorization, password composition, appropriateness of documented policies and guidance provided to Court personnel, and frequency of password changes. We interviewed AOTC personnel to obtain an understanding of how user accounts are activated and deactivated.

To assess the adequacy of inventory control procedures for computer equipment, we conducted an examination of the Court's inventory of computer equipment to determine whether controls were in place and in effect to properly account for and safeguard computer equipment. We examined policies and procedures regarding the fixed-asset inventory to determine whether the Court was in compliance with the Office of the State Comptroller's and the AOTC's requirements regarding fixed-asset control. To confirm the existence of and assess the proper recording of computer equipment, we performed an inventory test of all 81 items of computer equipment listed on the AOTC master inventory record for Plymouth County Superior Court to confirm actual equipment location and data regarding information for identification tag numbers, location, description, and historical cost.

To assess the adequacy of business continuity planning, we determined whether any formal recovery or contingency planning had been performed to resume computer operations should the automated systems utilized by the Court be rendered inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We interviewed Court and AOTC personnel to determine whether backup copies of application system data files are generated on a scheduled basis for on-site and off-site storage.

We interviewed Court personnel and obtained documented policies regarding the protection of personally identifiable information. We reviewed guidelines for protecting personal information contained in court records and security practices in place at the Court.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices.

AUDIT CONCLUSION

Our review of the status of audit results from our prior audit report No. 2003-1122-4T, issued May 12, 2003, indicated that corrective action had been taken to strengthen controls regarding inventory control over computer equipment and user account management. Our audit indicated that Plymouth County Superior Court maintained an accurate and complete list of IT-related equipment that had been reconciled to the AOTC inventory system of record. During our review of user account management, nothing came to our attention to indicate any control weaknesses regarding the activation and deactivation of access privileges to selected automated systems utilized by the Court. However, our audit revealed that control practices needed to be implemented or strengthened for IT-related policies and procedures, physical security, environmental protection, and business continuity planning.

Our audit revealed that although the AOTC had developed certain policies and control guidelines for using technology, we found that there was a general absence of documented IT policies and procedures for maintaining documentation of authorized users, maintaining user area plans for continuity of operations, and changing passwords.

Regarding our examination of physical security, while we found adequate controls in place and in effect for the Court's Plymouth location, certain areas of physical security needed to be enhanced for the Brockton Courthouse. We found that all visitors entering the courthouse must pass through a metal detector and all packages must pass through an x-ray machine, and that only Court personnel have access to areas housing workstations and the file server where public access to these areas is prohibited. However, we found that controls over an emergency exit door needed to be strengthened to reduce a serious security risk.

Our review of environmental controls over areas housing IT resources revealed serious deficiencies throughout the Brockton Courthouse. We found the Courthouse was not equipped with smoke detectors or heat sensors. Our audit further revealed that neither emergency lighting nor a backup generator was being used in the case of a temporary loss of power.

With respect to inventory control over computer equipment, we found that an accurate and complete list of IT-related equipment was being maintained. The inventory list, which assists Court management in identifying IT resources under its control, is also provided to 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. Our tests indicated that hardware items were locatable, properly accounted for, and tagged. We found that the Court performed annual physical inventories and reconciliation to comply with AOTC guidelines

and to address accounting requirements promulgated by the Office of the State Comptroller. We found that the inventory record contained appropriate data fields including historical cost, condition, serial number, tag identification number, location, and purchase order number.

Regarding business continuity planning, the Court, in conjunction with AOTC, needs to further assess and develop, document, and test a comprehensive disaster recovery strategy to provide reasonable assurance that business operations could be regained in a timely manner should automated systems be rendered inoperable or compromised. Furthermore, although certain procedures are in place, the Court has not documented user area and contingency plans to help ensure the resumption of business operations and activities in the event of an extended loss of IT capabilities or a major disaster or emergency. Our audit also indicated that AOTC needs to provide instructions or plans to the Court to ensure continuity of IT and business operations should the applications used by the Court become inoperable or inaccessible.

AUDIT RESULTS

1. Prior Audit Results Resolved

a. Inventory Control over Computer Equipment

Our prior audit disclosed that an inventory of IT resources was not being maintained by either the Clerk's Office or the Probation Department. Although a list of IT hardware was obtained from AOTC, the Court did not maintain a copy of the list or perform an annual reconciliation to AOTC's inventory or to an inventory record maintained by the Court.

Our current audit found that the Court was maintaining an inventory of IT resources and had performed an annual physical inventory in compliance with requirements of the Office of the State Comptroller and AOTC guidelines, and that inventory reconciliations are performed by AOTC. In addition, AOTC uses IT configuration management tools to identify all IT equipment connected to the network. We found that the inventory system of record contained appropriate data fields including historical cost, location, condition, serial number, tag identification number, and purchase order number.

b. User Account Management

Our prior audit report revealed that procedures needed to be strengthened to ensure that access privileges to the automated systems utilized by the Court would be deactivated in a timely manner for those individuals no longer requiring access.

Our current audit tests of user account management revealed that controls were in place and in effect to provide reasonable assurance that only authorized users had access to application systems utilized by the court.

2. Prior Audit Results Partially Resolved

Our prior audit indicated that control practices should be strengthened by having documented management control practices and IT responsibilities regarding physical security, environmental protection, logical access security, business continuity planning, and inventory control of IT resources.

Our current audit indicated that although AOTC has partially developed limited guidelines for information technology, more detailed policies and procedures regarding physical security, environmental protection, system access security and disaster recovery, and business continuity should be documented and communicated to all court staff.

3. Prior Audit Results Unresolved

a. Physical Security and Environmental Protection

Our prior audit indicated that physical security and environmental protection controls needed to be strengthened. Since our prior report was issued in May 2003, the Plymouth County Superior Court extended its operations for civil cases at Plymouth District Court. The Plymouth District Court, which opened in August 2007, provides a state-of-the-art facility including strong physical security and environmental controls. However, our review of corrective actions at the Brockton Courthouse indicated that physical and environmental controls had not been improved and needed to be strengthened.

Our audit disclosed that although there was adequate security for the perimeter of the Brockton Courthouse, certain controls needed to be implemented or strengthened. The Courthouse is staffed with security personnel at the public entrance and is equipped with metal detection and X-ray machinery. We found that a list was maintained of authorized individuals who had been given keys to interior office areas. We found that access to the areas housing the microcomputer workstations were limited to only Court personnel, except for access to two terminals for which public access is provided. Our audit disclosed that the room through which all computer lines are routed to the AOTC file servers was locked and located in an area that is inaccessible to the general public. However, our audit revealed that an emergency exit door did not have an alarm sensor to alert Court staff should the door be opened. As a result, unauthorized entry could go undetected, placing personnel or the public at risk. In addition, we found that the Courthouse was not equipped with intrusion alarms and that windows in certain areas of the building could not be secured.

Regarding controls for environmental protection, we observed that there were serious deficiencies throughout the building. For instance, we found that there were no smoke detectors and heat sensors and the only fire detection equipment was located in two secured vaults. Furthermore, we found that the emergency backup generator for use in the event of a temporary loss of electric power was inoperable and located in an area that contained excess dust and dirt. The courthouse is owned and maintained by Plymouth County. According to Court management, budgetary constraints contributed to the difficulty in implementing physical security and environmental controls to safeguard IT equipment and Court staff.

Generally accepted computer industry standards advocate the need for sufficient physical security and environmental protection controls to provide reasonable assurance that damage to, or loss of, IT-related assets will be prevented and detected.

Recommendation

We acknowledge that although the courthouse facility is owned and maintained by Plymouth County, the Court, in conjunction with AOTC, should seek the means to improve physical security and environmental protection controls to provide a properly controlled operational environment and to safeguard Court staff and IT-related equipment. Management should consider the installation of smoke, heat, and fire detection devices throughout the Court.

Auditee's Response

The Clerk of Courts provided the following response:

> *A meeting was held with senior management, an attorney from the AOTC, the executive secretary of Plymouth County and we are in agreement with your findings regarding the corrective actions that need to be taken at the Brockton courthouse indicating that physical and environmental controls need to be strengthened. The following people were contacted the Plymouth County Commissioners, our Congressman and DECAM about funds for an alarm for emergency exit door, intrusion alarms and windows that could be secured, smoke detectors and a generator for use in the event of a temporary loss of electric power. This would allow us to practice generally accepted computer industry standards for sufficient physical security and environmental protection controls.*

Auditor's Reply

We acknowledge that the Court has initiated a meeting among senior management of the Court, AOTC, the Division of Capital Asset Management, and Plymouth County and that agreement has been reached regarding the need to take corrective action. We also acknowledge that an effort has been initiated to inform appropriate individuals of the need to obtain funding to enhance or implement appropriate controls.

b. Business Continuity Planning

Our prior audit report recommended that the Court, in conjunction with AOTC, assess the relative criticality of their automated processing, and develop and test appropriate user area plans to address business continuity. In addition, we recommended that an assessment of criticality and business impact be performed at least annually, or upon major changes to Court operations or the IT environment.

Our current audit revealed that the Court, in conjunction with AOTC, had not developed a documented 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 addition, the Court had not developed comprehensive, documented individual contingency plans to address the potential loss of automated processing. Without contingency planning, especially 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, Court management indicated that Court business could be conducted at either of its locations, but the strategy has never been documented or tested. The Court needs to identify the nature and extent of court or business activities that could be conducted in the absence of AOTC-supported systems and/or in the event of damage or inaccessibility to the Court's facilities.

Based on interviews with Court management, we were informed that under a disaster scenario in which the Court could not conduct business on a short-term basis at either the Brockton or Plymouth courthouses, the Court would be able to utilize the other location for scheduled hearings and use the ForecourtVision application for docketing and data input and the Warrant Management System to track warrants issued from all courts. 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 Department 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 Plymouth Superior Court may be at risk of not regaining mission-critical and essential business functions in a timely manner. Without a comprehensive, documented, and tested disaster recovery and contingency plan, including required user area plans, the Court would be hindered from performing essential business functions.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

The viability of the business continuity planning process requires continued 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 IT and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available. 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.

Generally accepted practices and industry standards for computer operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. Therefore, the Plymouth Superior Court should assess the extent to which it is dependent upon AOTC for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its own environment.

Recommendation

We recommend that the Court, in conjunction with the AOTC, develop, fully document, and test disaster recovery and contingency plans that include detailed user area plans specific to the Court's operations. We recommend that the Court 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. 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 various disaster scenarios. The recovery plan should contain all pertinent information, including clear assignment of key personnel and their roles and responsibilities, needed to efficiently recover mission-critical and essential operations within the respective time frames. We recommend that business continuity detailed user area plans be tested and periodically reviewed and updated, as needed, to ensure their viability. The completed plans should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response

The Clerk of Courts provided the following response:

> *We will work to develop a formal business continuity and contingency planning with the AOTC to address our risks and exposure. We will formalize our business plan to utilize either the Brockton or Plymouth facility in the case of a disaster.*

Auditor's Reply

We acknowledge the Court's intent to address business continuity planning. We will review this during future audits.