A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

NO. 2003-1135-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE EAST BOSTON DISTRICT COURT

JULY 1, 2002 THROUGH AUGUST 8, 2003

OFFICIAL AUDIT REPORT
APRIL 6, 2004

TABLE OF CONTENTS

INTRODUCTION

The East Boston District Court (EBDC) was established under the authority of Chapter 218, Section 1, of the Massachusetts General Laws, as amended. The Court has offices in the City of Boston in Suffolk County. The Court has original jurisdiction for crimes carrying a penalty of up to 30 months incarceration and original bail and cash receipt activity for criminal and civil matters. The Court also has jurisdiction in civil actions under $25,000 and in matters where equitable relief is sought. In addition, the Court has territorial original jurisdiction in actions involving the Sumner Tunnel, the Lieutenant William F. Callahan, Jr. Tunnel, and the adjacent Massachusetts Turnpike Authority property, toll plazas and approach roads.

Through the Court Reform Act, Chapter 478 of the Acts of 1978, the Administrative Office of the Trial Court (AOTC), previously entitled the Office of Chief Administrative Justice, was established to provide management and fiscal oversight to the seven trial court departments, including the Superior Court and the Office of the Commissioner of Probation. The AOTC's Information Technology (IT) Department is located in Boston and provides technical support to individual courts. The primary IT functions at the East Boston District Court were supported and maintained by the IT Department of the AOTC. The AOTC also provides the courts with IT resources, as well as guidelines for IT policies and procedures. The AOTC administers the Court's IT infrastructure, including mission-critical applications installed on AOTC's file servers located in Cambridge. In addition, at the time of our audit, the AOTC was in the process of establishing inventory records of IT equipment for the courts under its jurisdiction. At the Chief Justice's direction, the Fiscal Affairs Department has promulgated accounting policies and procedures that comprise the Trial Court Standard Accounting System.

The East Boston District Court is divided into two functional offices, the Clerk's Office and the Probation Department. The Clerk's Office handles 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 East Boston District Court were supported by microcomputer workstations, but were not configured through any on-site host file servers. Instead, the workstations were connected by lines to file servers in Cambridge and AOTC's wide area network (WAN). There were 16 workstations assigned to the Clerk's Office and 19 assigned to the Probation Department. The WAN allows connectivity to the IBM RS6000 server and the primary computer applications administered by the AOTC.

The primary application systems used by the Court residing on the file servers located at the AOTC Information Technology Department 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 (WMS), which is used to track warrants issued and warrant information from all courts. Additional applications installed on the AOTC mainframe used by the Court include the Domestic Abuse Registry, Operating Under the Influence (OUI) database system, and the Case Activity Tracking System (CATS) that tracks defendants on probation. 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 the Probation Receipts Accounting System software package to account for all fines and fees processed through this court. 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 and also a review of cash receipts activity.

SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From June 10, 2003 through August 8, 2003, we performed an audit of certain information technology (IT) related controls at the East Boston District Court for the period July 1, 2002 through August 8, 2003. Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security and environmental protection for selected areas housing IT resources, logical access security, business continuity planning, generation of on-site and off-site backup copies of computer media, storage and record retention of hardcopy files, and inventory control of IT resources. We also reviewed the cash receipts for the Probation Department for fiscal year 2003.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control framework, including policies, procedures, practices, and organizational structure provided reasonable assurance that control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection were in place and in effect to prevent unauthorized access or damage to, or loss of, computer equipment or IT-related assets. We sought to determine whether adequate controls were in place to prevent unauthorized access to systems and data available on the Court's workstations.

We sought to determine whether an effective business continuity plan had been implemented to provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period should a disaster render the computerized functions inoperable. Further, we determined whether adequate on-site and off-site backup media was being generated for any workstation-based applications and for the ForecourtVision, WMS and CARI systems. We determined whether hardcopy trial documentation was being backed-up and whether the Court was in compliance with record retention requirements. In addition, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's IT assets were

properly recorded and accounted for in the Court's records and safeguarded against unauthorized use, theft, or damage.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, performing a preliminary review, risk analysis and evaluation of certain IT-related internal controls, and interviewing senior management to discuss the Court's IT control environment. To obtain an understanding of the Court's activities and internal control environment, we reviewed the Court's mission statement, organizational structure, web site, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities as described in our audit scope. Upon completion of our pre-audit work, we finalized audit scope and audit objectives.

To determine whether IT-related policies and procedures were adequately documented, we interviewed Court management staff and requested documentation of IT general control areas pertaining to organization and management, physical security, environmental protection for selected areas housing IT resources, logical access security, and business continuity planning. We identified IT functions and compared existing documented policies and procedures to assess the extent to which they addressed IT functions. We then assessed the relevant IT-related internal controls through questionnaires and reviewed and analyzed available documentation of IT-related policies and procedures. Our work was focused on the Court's IT facilities and did not include a review of AOTC's management structure, IT operations, or facilities. We requested and reviewed AOTC's IT-related policies and procedures that had been distributed to the Court.

To evaluate physical security at the Court we interviewed senior management and security personnel, conducted walkthroughs and observed security devices. We requested a list of individuals to whom keys to the Court's offices and telecommunication closets had been distributed and through observation, documentation review, and selected tests, we determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as office door locks, visitor logs, motion detectors, and intrusion

alarms. Our examination of physical security controls included security over microcomputer workstations located throughout the Court.

To determine whether adequate environmental protection controls were in place and in effect within the Court to prevent damage to, or loss of, computer equipment or IT-related assets, we inspected the areas where the workstations were located, and interviewed Court employees and security staff. We also determined whether appropriate environmental protection controls were in place, such as general housekeeping, heat, water, and smoke detectors, uninterruptible power supply, and fire suppression measures.

To determine whether the Court's logical access security policies and procedures prevented unauthorized access to software applications and data files residing on AOTC file servers and mainframe computer and available through Court workstations, we discussed system security policies and procedures with the Office Manager and Chief Probation Officer who were the designated individuals responsible for system access security for the Court. We also reviewed procedures regarding the administration of logon IDs and passwords. Our tests of logical access security included a review of who was authorized to access various applications available through the Court's workstations. In addition, to determine whether adequate controls were in place to ensure that access privileges were granted to only authorized users, we reviewed procedures authorizing access to the automated systems. Moreover, we compared a list of users with authorized access to the Court's automated systems to a current Court payroll list to determine whether those individuals authorized to access the system were current employees. Our examination included a review of procedures regarding the deactivation of user access privileges.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been initiated to resume computer operations or business operations supported by technology should the Court not have access to the ForecourtVision, CARI, or the WMS application systems. With respect to business continuity planning, our discussions were limited to staff and management from the Court. Although we did not conduct a review of AOTC'S business continuity planning in conjunction with this audit, we inquired whether the Court had been provided a strategy from AOTC regarding recovery of AOTC-supported mainframe applications and data. In addition, we interviewed senior Court 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, tested business continuity plan was in place and in effect. Furthermore, to evaluate the adequacy of controls to protect data files through the backup of on-site and off-site magnetic media and hardcopy files, we interviewed Court and AOTC staff regarding the creation of backup copies of computer-related media, as well as hard copy files. Furthermore, we reviewed record retention requirements, policies and Massachusetts General Laws pertaining to hardcopy Court files and documentation, and interviewed Court staff regarding storage and disposition of these records.

To determine whether adequate controls were in place and in effect to properly safeguard and account for property and equipment, we reviewed inventory control procedures for computer equipment at the Court. We found that the AOTC was in the process of establishing inventory records of IT equipment and was responsible for promulgating policies and procedures for inventory control for all courts and for maintaining a central master inventory record for property and equipment. We reviewed related AOTC policies and procedures and obtained a listing of AOTC's inventory records for this Court. Our review and tests focused on inventory control procedures exercised by the Court and the integrity of AOTC's inventory record for the Court's IT resources. We tested 100% of 41 items of computer hardware from the inventory record provided by AOTC and examined the inventory record for identification tag number, location, description, condition and utilization.

We also examined cash receipt activity by examining overall internal controls, the timeliness of deposits, and the reconciliation process in effect. We determined the volume of cash receipt activity at the court for fiscal year 2003 and compared daily deposit slips to bank statements as well as the monthly cash receipts report.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume operations should operations supported through the AOTC's data center, such as the WMS and CARI systems, lose access or processing capabilities for an extended period. With respect to business continuity planning, we interviewed management from the Court as to whether a written, tested business continuity

plan was in place and in effect, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Although we did not review business continuity planning with AOTC staff, we inquired as to whether the Court had been provided a strategy from AOTC regarding recovery and processing of AOTC supported mainframe applications and data. In addition, to evaluate the adequacy of controls to protect data files through the generation of on-site and off-site storage of backup copies of magnetic media and hardcopy files, we interviewed Court staff regarding the creation of backup copies of computer-related media and hardcopy files.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry auditing practices. Audit criteria used in the audit included IT management control practices outlined in Control Objectives for Information and Related Technology (CobiT), as published by the Information Systems Audit and Control Association, July 2000. CobiT's control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices that provide a control framework for management, users, security practitioners, and auditors.

AUDIT CONCLUSION

Based on our audit at the East Boston District Court, we found that certain internal controls were in place for IT-related functions to provide reasonable assurance that control objectives would be met regarding physical security, environmental protection, and inventory control of IT resources used by the Court. However, we found that control practices needed to be implemented or strengthened for logical access security and IT-related business continuity planning at the Court. We found that policies and procedures relating to IT activities needed to be formally documented and that an appropriate business continuity strategy or contingency plans needed to be developed in conjunction with the Administrative Office of the Trial Court (AOTC).

Our examination of the Court's organization and management revealed that there was an established chain of command and adequate segregation of duties among Court employees. Our review of IT-related activities disclosed that the primary IT functions were supported and maintained by AOTC's IT Department. Although there was no established IT function at the Court, two employees served, in addition to maintaining their regular Court responsibilities, as the liaisons between the Court and AOTC regarding IT-related issues. Given that the AOTC had not defined IT-related areas of responsibility for the Court or communicated required IT policies and procedures, Court personnel were unaware of certain responsibilities and control practices with regard to IT-related activities. We found that there was a general absence of documented IT policies and procedures and IT control practices to address IT functions performed at the Court.

We determined that certain physical security controls were in place to safeguard IT-related resources. Upon entering the courthouse, all visitors entering through the main entrance are required to pass through a metal detector, and all packages must pass through an x-ray machine. Only Court staff occupy, or are in close proximity to, areas where the microcomputer workstations are located and those areas are restricted from public access. However, we found that controls over keys for all exterior doors at the East Boston courthouse needed to be strengthened since Court management was unable to provide a current list of holders of keys to exterior doors at the courthouse or provide evidence that

formal policies and monitoring procedures existed regarding key management. As a result, it could not be determined whether issued keys were assigned only to active employees, or if prior employees had returned their keys upon terminating employment with the Court. We also determined that controls regarding intrusion sensors needed to be strengthened.

Our review revealed that there were certain environmental protection controls in place, such as an emergency evacuation plan for the entire building, a fire alarm system connected to a fire department less than two miles away, an emergency shutoff valve for water lines for the entire building, air conditioning for areas housing microcomputer workstations, and fire extinguishers on each floor in the courthouse. However, we determined that environmental protection controls needed to be strengthened to provide appropriate safeguards with respect to installing an emergency lighting system. We also observed that there were no smoke detectors, and that heat sensors were located only in vaults.

Regarding the availability of automated systems, we found that the Court had not, on their own or in conjunction with the AOTC, documented a formal business recovery strategy or contingency plan for operations supported by mission-critical applications residing on AOTC 's file servers in Cambridge. In addition, we found that the Court, in conjunction with the AOTC, had not performed a criticality assessment of application systems and their associated risks. The policies and procedures relating to IT activities needed to be formally documented, and appropriate business continuity strategy or contingency plans needed to be developed in conjunction with the AOTC.

Since the Court's mission-critical applications were operating on the AOTC's file servers and mainframe computer in Cambridge, we did not perform tests of backup procedures for AOTC. These systems included the Warrant Management System and ForecourtVision application administered by the AOTC's Information Technology Department in Boston, and the CARI application system maintained by the Office of the Commissioner of Probation. Regarding the backup procedures for software residing on EBDC computers, the court had a formalized AOTC approved plan in effect.

We found that there were no backup procedures for many hardcopy standard forms and Court-related documentation. As a result, important documents could not be recovered if

they were destroyed, and added costs would be incurred to recreate standard forms. Furthermore, our review of record retention procedures indicated that court records stored in the Clerk's Office and the Probation Department were not being considered for archival storage. Importantly, the Court should address the risk of not being able to recover critical data contained in hardcopy documentation and the risk of incurring unnecessary data reconstruction costs.

Our audit disclosed that although certain access security controls provided reasonable assurance that authorized users could access only levels of information commensurate with each employee's job assignments, controls regarding access to AOTC applications available through Court workstations needed to be strengthened. Although sufficient procedures were in place to authorize and activate user access to automated systems, policies needed to be developed to ensure that access privileges no longer authorized or needed would be deactivated in a timely manner. Although the activation and deactivation of user accounts is managed by security personnel from outside the Court, appropriate access security controls need to be in effect at the Court. We found that controls for password administration did not exist at the East Boston District Court and there was no evidence that passwords had been changed for Court personnel.

Although certain inventory controls are centrally handled by AOTC, we found that the Court needed to strengthen its controls to provide reasonable assurance that IT resources would be properly recorded and accounted for. At the time of our audit, the Court did not maintain its own inventory record of IT resources. We found that AOTC had initiated a statewide inventory of IT resources and that an informal list of computer equipment for the Court had been provided during the audit. Although the inventory list identified computer hardware, cost data, location and tag numbers, it did not contain acquisition dates or installation dates, and the data in the cost category was blank in 36 out of 41 instances. Our limited audit tests indicated that the Court's IT equipment was properly tagged, and that equipment on hand was identified and properly recorded on the AOTC inventory list. We found that the Court did not perform an annual physical inventory as required by the Commonwealth of Massachusetts Trial Court's Internal Control Guidelines developed by the Administrative Office of Fiscal Affairs. Of the 41 items on the AOTC inventory record,

35 items were located, 6 items could not be verified at the EBDC, and there were eight items at the court that were not on the AOTC inventory record. We also determined that the court did not have a listing of software products.

Our audit disclosed that the cash receipts activity of the Probation Department was in compliance with existing laws and regulations governing cash receipts. We examined overall internal controls, the timeliness of deposits, and the reconciliation process in effect. We verified the volume of cash receipt activity at the court for fiscal year 2003, and examined a sample of cash receipts by comparing daily deposit slips to bank statements and the monthly cash receipts report.

AUDIT RESULTS

BUSINESS CONTINUITY PLANNING

We determined that business continuity requirements and plans needed to be formulated and documented. Our review of disaster recovery and business continuity planning indicated that the level of planning and documentation needed to be strengthened. At the time of our audit, the Court was unaware of any steps to be taken by AOTC to recover IT processing capabilities. AOTC had not provided the Court with a comprehensive business continuity plan regarding system availability should processing be lost in the event of a disaster. Our audit revealed that the Court had not, on their own or in conjunction with the AOTC, documented a formal business recovery strategy or contingency plan for mission-critical applications residing on AOTC's file servers in Cambridge. We found no evidence that formal planning had been performed to restore Court-based business operations in the event that automated systems were damaged or no longer accessible. In addition, we found that the Court, in conjunction with the AOTC, had not performed a criticality assessment of application systems and their associated risks. Regarding the recovery of business operations, the Court needs to develop, in conjunction with AOTC, an appropriate business continuity strategy to include identification of an alternate operational site, requirements and controls for on-site and off-site backup of hardcopy files, and the testing of recovery and contingency plans. The plans should be updated to reflect changes in business requirements, technology, personnel, and risks.

According to court management, backup procedures were in place for the mission-critical applications operating on the AOTC's file servers in Cambridge, which included the Warrant Management System and ForecourtVision application. The CARI application system has backup procedures administered by the AOTC's Information Technology Department in Boston. We found, however, there were no backup procedures for some of the Court's standard forms and for Court-related documentation available only in hardcopy form. As a result, critical standard forms having no electronic or backup copy would need to be recreated should the current forms be destroyed through a disaster. Importantly, the Court needs to assess the risk of being unable to recover the forms or completed documents within

an acceptable period of time, or of incurring unnecessary costs to recreate forms or reconstruct data.

Our review also disclosed that both the Clerk's Office and the Probation Department have closed court files that are maintained in standard hardcopy forms. These documents are not being stored in accordance with the Commonwealth's Record Retention Law, Massachusetts General Law (MGL) Chapter 66, Section 8 and Chapter 66A. We found files of resolved cases that were more than four years old, but were still stored in both of the offices cited above and not properly stored in accordance with established policies and procedures promulgated by the Office of the Secretary of State as well as the Administrative Office of the Trial Court. Specifically, the Court is not adhering to M.G.L. c. 221, sec. 27A permitting the destruction of records, as well as the disposal of records policy no. 17/76 established by the Secretary of the Commonwealth. In addition, we determined that the Court does not prepare or generate backup copy documents for unresolved court cases. In the event of a disaster, such as a fire, these files could be destroyed and rendered irretrievable should the Court require their accessibility in the future. Our observations indicated that adequate resources might not be available for generating backup copies of hardcopy standard forms and documents.

Recommendation

We recommend that the Court work with AOTC to develop or obtain IT-related policies and procedures appropriate to the Court's IT environment. The policies and procedures should outline controls and provide guidance for IT-related functions or activities partially or entirely performed at the Court.

The Court should work with AOTC to determine the extent to which business continuity plans (user area plans for the Court) and contingency plans need to be developed. The Court's recovery and contingency plans need to be coordinated with business continuity strategies to be executed by AOTC. We recommend that the development of business continuity plans be preceded by an assessment of the criticality and risk of IT operations and business impact should IT systems be rendered inoperable or inaccessible. This effort should assist the development of user area and contingency plans to help ensure resumption

of mission-critical and essential business operations within an acceptable time frame. The Court should also confirm that appropriate backup procedures are being followed and that secure on-site and off-site storage is being provided for backup copies of magnetic media and critical processing forms.

We recommend that the Court bring to AOTC's attention the risk of not having backup copies of critical Court-related documentation. We also recommend that the Court review its current program to store documents in the State Archives and to comply with the current record retention policy to the extent possible. We recommend that the Court, in conjunction with AOTC, develop a strategy to minimize the risk of lost or damaged hardcopy records by implementing a formal procedure for improving the controls for generating and storing backup copies of hardcopy files so as to be in compliance with record retention policies for archiving documents and to safeguard all of its critical hardcopy documents on an on-going basis.

Auditee's Response

Response received from the Clerk Magistrate:

> *I have received and reviewed the draft report on the examination of information technology-related controls in the Clerk's Office of the East Boston Division of the Boston Municipal Department.*
>
> *I agree with the recommendations made by the auditors and have implemented changes. With regards to keys to the front doors, the Presiding Justice of the Court had the locks changed, new keys made and a list of who has keys is in the possession of the Chief Court Officer.*
>
> *On March 5, 2004 two telephone calls were placed to AOTC.* [The AOTC has] *. . . reassured me, I would be receiving recommendations concerning a disaster recovery and business continuity plan which have been used in two other courts. I will review it and work with AOTC to implement the necessary procedures.*

Auditor's Reply

We acknowledge the Court's decision to implement appropriate controls regarding business continuity planning and to strengthen physical security.