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. 2004-1131-4T

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

July 1, 2002 through February 27, 2004

OFFICIAL AUDIT REPORT

JUNE 30, 2004

2004-1131-4T

TABLE OF CONTENTS

INTRODUCTION

The Boston Municipal Court (BMC) was established under the authority of Chapter 211B, Section 1, of the Massachusetts General Laws, as amended. The Court is located in Boston, Massachusetts. Criminal jurisdiction of the Boston Municipal Court includes most criminal offenses that do not require the imposition of a state prison sentence. The Court has jurisdiction on criminal litigation that carries a penalty of up to two and a half years incarceration upon conviction. If a prison sentence were mandated, the Court may conduct probable cause hearings to determine whether offenses will be bound over to the Superior Court. The Court has original jurisdiction over a number of serious felonies, concurrent with the Superior Court.

The BMC is divided into four functional offices, the Clerk Magistrate's Criminal Section, the Clerk Magistrate's Civil Section, the Probation Department, and the Judge's Lobby. The Clerk Magistrate's Criminal Section handles cases involving family abuse prevention, sanitary code, review of findings of the State Police Trial Board, residential nuisances, domestic abuse actions, failure to provide utilities, summary process, jury appeals, supplementary proceedings, civil motor vehicle infractions, default warrant assessment fee, and environmental fines. The Clerk Magistrate's Civil Section handles cases involving equitable jurisdiction in lead poisoning prevention, landlord interference with quiet enjoyment, mental health commitments, sanitary code, summary process, unemployment compensation appeals, small claims, jury appeals, contract and tort actions, cases remanded from the Superior Court, failure to provide utilities, supplementary proceedings, paternity and support actions, restraining orders, small claims, appeals, and motor vehicle litigation; 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, provides community supervision of offenders or litigants, maintains statistics on crime, mediations, welfare fraud, restitution for adults, service to victims, and performance of other appropriate community service functions. The Judge's Lobby is responsible for review of cases and administrative planning for cases.

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 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 application systems 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 time of our audit, the IT operations at the Court's offices were supported by 123 microcomputer workstations configured through one host file server and connected by a T1 line to file servers at AOTC 's wide area network and IT Department's data center in Cambridge. The AOTC, through its IT Department, provides individual courts with IT-related policies and procedures, IT resources, and technical support. There were 32 microcomputer workstations assigned to the Clerk Magistrate 's Criminal Section and 34 assigned to the Probation Department. There were also 32 workstations assigned to Clerk Magistrate's Civil Section and 25 workstations assigned to the Judge's Lobby. At the beginning of our audit, the primary application systems used by the Court residing on the file servers located at AOTC's IT Department were BASCOT for the Clerk Magistrate's Criminal Section and the ForecourtVision application for the Clerk Magistrate's Civil Section. Both sections of the Clerk Magistrate's Offic**e** use the Human Resources Compensation Management System (HR/CMS). At the time of the audit, BMC staff were beginning training for the Court View software application, which is a Windows-based application system that uses client-server technology for electronically recording docket information. The Clerk Magistrate's Criminal Section uses the Warrant Management System (WMS) to track warrant information from all courts, the Massachusetts Management Accounting and Reporting System (MMARS) to track the revenues and expenditures, and HR/CMS to track human resource information. As of November 1, 2003 the Court obtained the new application program Court View for the Clerk Magistrate's Criminal Section.

The Probation Department uses the Case Activity Tracking System (CATS), which is installed on the AOTC mainframe, to track defendants on probation. In addition, the Probation Department uses the Criminal Activity Record Information (CARI) system to record all dispositions from courts regarding criminal and juvenile offenses and restraining orders. The Probation Department also uses Probation Receipts Accounting System (PRA) to account for all fines and fees processed through the Probation Department at this Court. The Judge's Lobby uses the MMARS and the HR/CMS program applications.

The Office of the State Auditor's audit was an examination of certain IT general controls over and within the Court's IT environment and financial-related controls pertaining to cash receipt activity and bail fund maintenance.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From October 9, 2003 through February 27, 2004, we performed an audit of certain information technology (IT) related controls at the Boston Municipal Court for the period covering July 1, 2002 through February 27, 2004. 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 assessed the user satisfaction regarding the newly installed Court View application system for the Clerk Magistrate's Criminal Section. We also reviewed the audit results presented in our prior audit report regarding financial related controls for cash receipt activity and bail fund maintenance.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected activities 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 that provide reasonable assurance that only authorized users would have access to systems and data available through the Court's microcomputer workstations were in place. We also sought to determine whether adequate controls to prevent and detect unauthorized access to systems were in place.

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 systems housed at AOTC's Cambridge data center. 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 resources were properly recorded and

accounted for in the Court's inventory records and safeguarded against unauthorized use, theft, or damage. We also sought to determine whether users were satisfied with the newly-installed Court View application system, and whether our prior audit recommendations had been implemented concerning cash receipts activity and bail fund maintenance.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included gaining and recording an understanding of relevant court operations, interviewing senior management to discuss the Court's IT control environment, and performing a preliminary review, risk analysis and evaluation of certain IT-related internal controls. To gain 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 requested and reviewed AOTC' s IT-related policies and procedures that had been distributed to the Court. Upon completion of our pre-audit work, we determined audit scope and audit objectives. We assessed the strengths and weaknesses of the internal control system for selected IT activities as identified in our audit scope.

To determine whether IT-related policies and procedures were adequately documented, we interviewed Court management and staff and requested documentation of IT general control areas pertaining to IT organization and management, physical security, environmental protection for selected areas housing IT resources, logical access security, and business continuity planning. We identified 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 Boston Municipal Court's IT facilities and did not include a review of AOTC 's IT operations or facilities.

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 had been distributed and through observation, documentation review, and selected tests, we determined the adequacy of physical security controls over areas housing IT equipment. Our examination of physical security controls included security over the file server room wiring closets, and 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 workstations were located, including the file server room and wiring closets, 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 adequate internal controls were in effect to prevent or detect unauthorized access to application systems and data through the Court's microcomputer workstations, we discussed system security policies and procedures with the various court staff. The staff included the Clerk Magistrate's Criminal and Civil Sections and Chief Probation Officer and staff assigned to the Judge's Lobby, as well as individuals who were the designated liaisons 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 application systems available through the Court's workstations. We reviewed procedures authorizing access to the automated systems to determine whether adequate controls were in place to ensure that access privileges were granted only to authorized users. We compared a list of users with authorized access to the Court's application systems to current personnel records to determine whether those individuals authorized to access the system were current employees. In addition, our examination included a review of procedures regarding the activation and 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 BASCOT, ForecourtVision, Warrant Management System, CATS, CARI, PRA, HR/CMS system, MMARS or the newly-installed Court View application system. With respect to business continuity planning, our discussions were limited to management and staff from the Court. We interviewed senior Court management to determine 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 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 application systems and data. To evaluate the adequacy of controls to protect data files through generation and storage of backup copies of magnetic media and hardcopy files, we interviewed Court 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 the storage and disposition of these records.

To determine whether adequate controls were in place and in effect to properly safeguard and account for IT resources, we reviewed inventory control procedures for computer equipment at the Court. We reviewed AOTC's related 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 selected a judgmental sample of 170 IT-related items out of a population of 358 items of computer equipment and compared the information obtained from the inventory record provided by AOTC and the Court's own department inventory listings and examined the inventory record for identification tag number, location, description, condition, utilization and status. Of the total sample selected, we sought to verify the physical inventory at the Court by comparing 77 IT-related items from the AOTC inventory listing to the four department locations and by comparing 93 IT-related items from the Court's inventory listings to the four departments' locations.

To determine whether the Court employees were satisfied with and properly trained in the use of the Court View application, we completed informal assessments and interviewed staff members of the Clerk Magistrate's Criminal Section. Since the Court View application system had only been installed in the Clerk Magistrate's Criminal Section by the end of the audit, we were only able to interview the Clerk Magistrate's Criminal Section staff for this application. However, we were able to obtain and review the operating manual for this application during the course of the audit.

We also followed up on the prior audit result pertaining to cash receipts activity for the Clerk Magistrate's Criminal and Civil Sections and the Probation Department for the time period of July 1, 2002 through September 30, 2003. We assessed internal controls in effect and reviewed the implementation status of our prior audit recommendations. We also examined the timeliness of deposits of cash receipts and the status of the reconciliation process. We examined three different months for each section of the Court, thus testing nine of a possible fifteen months in our selected review period. We examined a total of $177,772 or 26% of all Clerk Magistrate Criminal Section cash receipts, and $304,802 or 20% of all Clerk Magistrate Civil Section cash receipts. We also examined $98,864, or 25% of all Probation Department cash receipts.

To determine whether corrective action had been taken to address the prior audit results regarding bail fund activity, we reviewed the adequacy of internal controls in effect and the implementation status of our prior audit recommendations. We also examined the forfeitures of bail, the notification of bail fund availability to sureties, and the status of abandoned property transmittals. We examined three different months for bail fund receipt for the Clerk Magistrate Criminal Section, thus testing three of a possible fifteen months in our selected review period. We examined a total of $415,700, or 21% of all Clerk Magistrate Criminal Section bail fund receipt activity.

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 Boston Municipal Court, we found that certain internal controls were in place for IT-related functions. However, we found that control practices needed to be implemented or strengthened for physical security, environmental protection, business continuity planning, logical access security and inventory control of IT resources 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 review of IT-related activities disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC. Although there was no established IT function at the Court, an AOTC employee served as an Implementation Manager and as the liaison between the court and AOTC regarding IT-related issues. Given that IT-related areas of responsibility had not been defined for the Court and that adequate IT policies and procedures were not in place, Court personnel were unaware of certain responsibilities and control practices with regard to IT-related activities.

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 must pass through a metal detector or display appropriate identification, and all packages must pass through an x-ray machine. Only Court staff occupy areas where the microcomputer workstations are located, and public access is prohibited to these areas. We found that controls could not be verified for all exterior doors at the courthouse, since the Court is a tenant of the Federal Government, and all door keys are maintained by the United States General Services Administration (GSA). However, we note that for all four BMC departments, the password to the key pad code locks to interior entrance doors to respective BMC sections had not been changed since May 2001. As a result, it could not be determined whether only active employees had access to departmental areas.

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, air conditioning for areas housing microcomputer workstations in the Clerk Magistrate's Office, and fire extinguishers on each floor in the courthouse. However, we determined that the existing HVAC units had not been repaired by the GSA, causing BMC to utilize its own air conditioning system, there was no BMC designee assigned to contact AOTC in case of emergency, there were no hand held fire extinguishers in the file server room, and the file server room was cluttered with boxes and cabling.

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 to address the loss of mission-critical application systems residing on AOTC's file servers in Cambridge. In addition, we found that the Court, in conjunction with the AOTC, had not assessed the criticality or performed a risk analysis of the application systems used by the Court. Regarding the recovery of business operations, the Court needs to develop, in conjunction with AOTC, an appropriate business continuity strategy to help ensure system availability and resumption of IT operations within an acceptable time should processing be rendered inoperable or inaccessible. The business continuity plan should include identification of an alternate operational site, requirements and controls for on-site and off-site backup of computer media and hardcopy files, and the testing of recovery and contingency plans.

Our audit disclosed that although certain logical access security procedures provided reasonable assurance that authorized users could access only levels of information commensurate with each employee's job assignments, controls regarding access to AOTC application systems available through the Court workstations needed to be strengthened. Although sufficient procedures were in place to authorize and activate user access to automated systems, procedures needed to be strengthened to ensure that access privileges no longer authorized or needed would be deactivated in a timely manner. We found that controls for password administration were informal in nature and that no record of password changes had been recorded for our review period. Although we determined that 69 users from the Criminal and Civil sections of the Clerk Magistrate's Office were authorized users, we found that six user accounts to the Probation Receipts Accounting system had not been deactivated for users no longer employed by the Court's Probation Department.

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. Although the AOTC has overall responsibility for maintaining a master inventory system of record for all fixed assets across the Trial Court system, the AOTC's 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. 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 lists identified computer hardware, the following deficiencies were noted:

- Inventory listings did not contain data regarding unit cost and acquisition or installation dates for all four departments.

- All four of the Court departments did not maintain up-to-date dollar amounts of inventory records that would support financial statements of AOTC concerning the Boston Municipal Court fixed asset inventory items.
- The court in all four department did not properly account for dispositions of fixed assets of hardware inventory items. It appears that the 36 items under consideration were old equipment that had been submitted to the AOTC.

Our substantive audit tests indicated that the Court's IT equipment was properly tagged, and that equipment on hand was identified and properly recorded on AOTC' s inventory list. The Court did not have adequate control mechanisms in place to help ensure a complete and accurate recording of the Court's IT resources in AOTC's inventory system of record. In this regard, a collaborative effort is needed on the part of the Court and AOTC to ensure that appropriate inventory control policies and procedures are in place and in effect for the accounting of IT resources.

Our review of user satisfaction was confined to a general understanding of how the new Court View software is operating within the Clerk Magistrate Criminal Section. This software program was implemented in the Clerk Magistrate Criminal Section of BMC's four departments on November 1, 2003, and was in its initial testing stage. The Court View application system was also implemented in the Clerk Magistrate Civil Section on February 2, 2004, near the end of our review period.

Our review of cash receipt activity for the Clerk-Magistrate Criminal and Civil Sections and the Probation Department determined that the Court was making timely deposits of its cash receipts and had addressed our prior recommendation by performing bank reconciliations on a monthly basis, was maintaining outstanding and bad check registers, and was adequately segregating cash receipts and cash disbursement functions by employee assignments.

Our review of bail fund maintenance for the Clerk Magistrate Criminal Section determined that the Court had implemented the prior audit recommendations by properly notifying appropriate sureties of bail fund availability within the prescribed time period after case resolution, and transmitting abandoned property and forfeited bails to the Office of the State Treasurer within the prescribed time period.

Our review of user satisfaction was confined to a general understanding of how the software application Court View is operating within the Clerk Magistrate's Criminal Section. This software program was implemented in the Clerk Magistrate's Criminal Section on November 1, 2003, and it is in its test stage. We note that at the time of our audit, Court personnel were being trained on Court View. At this time, the training program did not appear to be a formal training program. We note that the Court View application system was also implemented in the Clerk Magistrate's Civil Section on February 2, 2004, near the end of our review period. Although Court View was to be a forerunner to the MassCourts system, an accurate assessment of user satisfaction could not be performed due the short time that the system had been placed in production. At the time of our audit, the vendor installing the system was still

performing system tests and implementing changes to address certain system problems identified during testing.

AUDIT RESULTS

1. Business Continuity and Contingency Planning

Our review of disaster recovery and business continuity planning indicated that the level of planning and documentation needed to be strengthened. We determined that business continuity requirements and plans needed to be formulated and documented. At the time of our audit, the Court was unaware of any steps that AOTC would take to recover IT processing capabilities and had not been provided with a copy of any business continuity plans regarding AOTC's network and application system availability.

Our audit revealed that the Court had not, on their own or in conjunction with the AOTC, developed user area plans to recover critical operations or contingency plans for the newly-installed Court View system or other mission-critical applications residing on AOTC's file servers in Cambridge. There appeared to be little 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 or conducted an IT-related risk analysis. Regarding the recovery of business operations, the Court needed 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 computer media and hardcopy files, and the testing of recovery and contingency plans. The user area and contingency plans should be updated to reflect changes in business requirements, technology, personnel, and risks.

Based upon information obtained from other audits, we determined that procedures were in place for generating and storing backup copies of magnetic media for mission-critical application systems operating on AOTC' s file servers in Cambridge. In addition, the Court needs to assess the process for recovering hardcopy files and documents. The absence of imaging systems or other mechanisms to create backup copies places the Court at risk of not being able to recover the forms or completed documents within an acceptable period of time or incurring unnecessary costs to recreate forms or reconstruct data**.**

Recommendation:

The Court should work with AOTC to determine the extent to which business continuity plans 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 associated risks of IT operations and business impact should IT systems be rendered inoperable. This effort should

assist in the development of user area and contingency plans to help ensure resumption of mission-critical business operations within an acceptable time frame should automated processing be rendered inoperable or inaccessible.

We recommend that the court bring to AOTC 's attention the risk of not having backup copies of critical court-related documentation. The Court should evaluate the adequacy of procedures for generating and storing backup copies of magnetic media for the Court View system. 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, 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 in compliance with record retention policies for archiving documents, and to safeguard its critical hardcopy documents on an on-going basis.

Auditee's Response,

In addressing some of the audit's specific conclusions and findings, this office made the following adjustments:

The password to the key pad code lock on the interior doors was recently changed and will be changed again in the near future to ensure adequate internal controls.(P.8)

The audit found that no formal business recovery strategy or contingency plan existed to address the potential loss of mission-critical application systems. This office has begun to review several examples of Business Continuity and Contingency Plans in order to create a plan for this court. We will work closely with AOTC to formulate the most appropriate plan, which should include a provision to backup copies of critical court-related documentation and a component to minimize the risk of lost or damaged hardcopy records, consistent with record retention policies. (P.9, 12)

As the audit indicates, AOTC has the overall responsibility for maintaining a master inventory system of record for all fixed assets. However, this office has begun to expand its fixed inventory list to include a perpetual inventory list which will be updated annually. Future inventory listings should be in conjunction with AOTC documentation and should contain unit costs and installation dates. (P.9)

This office, in conjunction with AOTC, will establish adequate control mechanisms to ensure a complete and accurate recording of this office's IT resources, consistent with the AOTC inventory system of record. (P.10)

This office will account for dispositions of fixed assets of hardware inventory items. (P.10)

Auditor's Reply

We are pleased that the Court is implementing corrective action to strengthen IT-related controls. The review of several examples of business continuity and contingency plans is a good first step to identify topics to be covered in a plan. However, even after identifying elements of other plans which may meet the Court's needs, a risk and business impact assessment should be performed to identify risks, critical assets, and the impact of the loss of processing capabilities. The Court's business continuity and contingency plans need to support recovery strategies specific to regaining mission-critical and essential court functions. The plan, when approved, should be reviewed on an annual basis, or upon major changes to the IT environment or business requirements.

We believe that the corrective action taken to address inventory control will help ensure that IT resources will be properly accounted for and safeguarded.

PRIOR AUDIT RESULTS RESOLVED

1. Internal Control Issues

Our prior audit report noted that the Boston Municipal Court did not have adequate familiarity with its documented internal control system, the Trial Court's Fiscal Systems Manual, or Chapter 647 of the Acts of 1989.

The prior audit disclosed that the Court showed little or no familiarity with internal controls that would safeguard its assets, ensure the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.

Our follow-up review revealed that this prior audit result has been adequately addressed and the Court is now in compliance with the Fiscal Systems Manual and Chapter 647 of the Acts of 1989 with respect to depositing, recording, and reconciling cash receipts, segregation of duties, and fixed-asset management.

Specifically, we noted the following conditions:

(a) Bank accounts were reconciled during fiscal year 2003 and the first quarter of 2004. The court was performing monthly reconciliations of its cash receipt activity. By performing monthly bank reconciliations the court has reasonable assurance that bank and book balances are accurate and reliable. Furthermore, the Clerk Magistrate's Criminal and Civil Sections and the Probation Department were depositing cash receipt funds on a daily basis.

(b) The court departments examined had the internal control mechanism of an outstanding check register in place. We noted that outstanding checks were documented in the bank reconciliation process and followed up on in an expeditious manner in our review period.

(c) The court sections examined had the internal control mechanism of a bad check register in place. We noted that bad checks were documented in the bank reconciliation process and followed up in an expeditious manner for our review period. We also noted that the court, when appropriate, would file a criminal application for complaint to ensure the proper resolution of bad checks.

(d) The court departments administering cash receipts had adequate segregation of duties in effect so that transaction functions pertaining to cash receipts and cash disbursements activity were divided among assigned personnel. We noted that only selected employees could receive funds, while only other selected employees could disburse funds. All disbursements required two authorized signatures.

Therefore, we note that our prior audit recommendations in this area have been implemented.

2. Control and Accountability over Bail Fund Activities

The Clerk Magistrate's Criminal Section is responsible for the accounting of bail, which is an amount of money paid to the court by a defendant or a third-party surety that allows a defendant to be freed after arrest, but helps ensure the defendant's appearance in court. Our prior report revealed inadequacies over controls and accountability of bail activities in the following three areas:

(a) Our prior report noted that the Clerk Magistrate's Criminal Section had not performed any reconciliations of bail funds for a two-year period. Our current audit revealed the court was performing all appropriate reconciliations of bail funds for fiscal year 2003 and the first quarter of fiscal year 2004. The Court was also maintaining a record of its cash position, as its financial records reflected a balance of $626,305 on July 1, 2002 and a balance of $713,369 at September 30, 2003.

(b) Our prior report noted that the Clerk Magistrate's Criminal Section had not notified appropriate sureties of bail fund availability for a two-year period. Our current audit determined that the court properly notified sureties of the availability of bail funds as required by Section 35.5 of the Trial Court's Fiscal Systems Manual. Also, the Court conducted an annual review of the bail book for resolved cases over one year old and notified the surety by letter that the bail funds were available to the surety. Our testing confirmed that proper notification of bail fund availability to sureties and return of bail after case resolution to sureties was in effect for our review period.

(c) Our prior report noted that the court was not remitting abandoned property to the Office of the State Treasurer as required by Massachusetts General Law Chapter 200, Section 4. We determined from our current review that the Court during fiscal year 2003 and the first quarter of fiscal year 2004 was transmitting abandoned property to the State Treasurer as required. The Court implemented the prior OSA recommendation by preparing detailed monthly trial balances of bail funds and annually reviewing the bail book to ensure that sureties are notified of bail fund availability. Also, the Court implemented our prior audit recommendation by remitting bail funds unclaimed for three years or more to the State Treasurer as abandoned property, as required by law.

Furthermore, the Clerk Magistrate's Criminal Section was depositing bail receipt funds on a daily basis. Therefore, we note that our prior audit recommendations in this area have been implemented.