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. 2004-1191-4T

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

July 1, 2002 through June 21, 2004

OFFICIAL AUDIT REPORT
DECEMBER 27, 2004

2004-1191-4T

TABLE OF CONTENTS

INTRODUCTION

The Taunton District Court (TDC) is organized under Chapter 211B, Section 1, and Chapter 218, Section 1 of the Massachusetts General Laws. The Court's organization and management structure consists of the Judge's Lobby, Clerk-Magistrate's Office, Probation Department, and a Chief Court Officer responsible for security over the Courthouse. The Court has jurisdiction for all criminal and most civil matters for the city of Taunton, and the towns of Berkley, Dighton, Easton, Raynham, Rehoboth, and Seekonk. The Court is located at 15 Court Street, Taunton, with additional office space for the Probation Department at 18 Broadway Street, Taunton referred to as the Probation's annex. During the period from July 1, 2002 to June 21, 2004, the Court processed revenues of approximately $1,328,735 from various designated Commonwealth victim/witness protection grants, surcharges, indigent defense counsel fees, drug analysis fees, and other various fees. In addition, the Probation Department received $1,328,000 from monetary obligations imposed by the Court, which included drug analysis assessments, child support, and driving under the influence of liquor fees.

From an information technology (IT) perspective, the Administrative Office of the Trial Court (AOTC) supports the mission and business objectives of the District Courts by managing an IT infrastructure that includes operational support of mission-critical application systems for the courts. In addition, the AOTC provides IT services, technical support, and internal control guidelines to the individual courts. The AOTC's Internal Audit Department and the Administrative Office of the District Court periodically review various processes and functions within the District Courts to help ensure compliance with applicable policies and procedures as well as providing oversight.

At the time of our audit, the Taunton District Court's computer operations were supported by 47 microcomputer workstations, of which 28 were in the Probation Department and 19 in the Clerk-Magistrate's Office. The Court's workstations are connected to a Verizon Frame Relay circuit that has two PVCs (permanent virtual circuits). One PVC connects to a T3 line that is routed through the Brooke Courthouse and then connected to the AOTC Cambridge data center through a wireless relay. The other PVC connects to a T3 line directly into the AOTC Cambridge data center wide area network (WAN). All servers and services, including Internet access, email, and primary applications, including the Warrant Management System (WMS) and Basic Court Operations Tool (BasCOT), which the Court started to use near the completion of our audit, are operated and maintained by the AOTC Cambridge data center. The WAN allows the

Probation Department connectivity to the Criminal Activity Record Information (CARI) and the Probation Receipts Accounting (PRA) systems. In addition, the Court utilizes the Massachusetts Management Accounting and Reporting System (MMARS) as well as the Human Resources Compensation Management System (HR/CMS) maintained by the Office of the State Comptroller. Further, the Probation Department used an application called OPMAN (Operations Management System), which is a window-based program for case management tracking. The application system is used to identify case information such as date, probation officer assignment, and case status such as default.

The Office of the State Auditor's examination focused on a review of certain IT-related general controls over the Court's computer operations and a review of the status of prior audit results related to bail funds.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an audit of selected information technology (IT) general controls at the Taunton District Court (TDC) from January 29, 2004 through June 21, 2004. The audit covered the period of July 1, 2002 through June 21, 2004. Our audit scope included an examination of IT-related controls pertaining to documented IT policies and procedures for selected control areas, physical security and environmental protection for areas housing IT resources, system access security, inventory control over IT-related assets, business continuity planning, generation of copies of magnetic media for off-site storage for the Probation Department's Operations Management System (OPMAN), and the backup and storage of hardcopy files pertaining to cases and standard court forms. Our audit also included a review of the status of prior audit results brought forward in our audit report, No. 2000-5076-3, issued August 14, 2001.

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 documented policies and procedures, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets and hardcopy files. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to the Court's automated systems. Furthermore, we sought to determine whether the Court, in conjunction with the AOTC, was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. Furthermore, we sought to determine whether the Court had adequate area user plans that would provide reasonable assurance that mission-critical and essential IT-related operations and the Probation Department's OPMAN micro-computer-based application could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. In

conjunction with reviewing the business continuity strategy, we determined whether adequate provisions for off-site backup of computer media were in effect at the Probation Department for the OPMAN application to assist in recovery efforts. We also determined whether provisions were in effect for recovering hardcopy documents and whether the Court could retrieve the information from a copy should the original hardcopy document be damaged or lost.

We also sought to update the audit results that pertained to TDC that were presented in the Independent State Auditor's Report (2000-5076-3) on the "Financial and Management Controls Over the Collecting, Accounting, and Reporting of Bail Funds at the Sixty-Nine District Courts of the Commonwealth of Massachusetts."

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, interviewing senior court personnel, and performing a preliminary review and evaluation of stated controls for selected IT-related internal controls. To obtain an understanding of the internal control environment, we reviewed the Court's organizational structure and enabling legislation and performed an IT-related risk analysis to assess the strengths and weaknesses of the IT control environment. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To evaluate the IT internal control environment, we assessed the extent to which TDC had documented formal IT-related internal control policies and procedures in place to govern IT-related responsibilities relevant to the Court. We interviewed senior management and reviewed and analyzed IT-related documentation. We reviewed documented internal controls for selected IT activities identified in our audit scope and audit objectives. We requested and received AOTC's formal IT-related internal control guidelines that included policies and procedures contained in the Trial Court's Fiscal Systems Manual. We also downloaded policies and procedures memos that were available on the AOTC's website. Our audit work was focused on the Court's IT activities and did not include a review of AOTC's IT operations or facilities.

To evaluate physical security, we interviewed management and security personnel, requested written policies and procedures, and performed walkthroughs of the Courthouse, the Probation Department's annex, and the computer network and storage room. We also determined who had the responsibility of providing perimeter and access security at the Courthouse as well as determined the level of security in place at the annex. We examined the existence of controls, such as the keypad system, key lock system, and intrusion alarms for areas housing IT resources

and hardcopy files. To evaluate physical security regarding the procedures used in obtaining a key or combination access to the Courthouse and the annex, we completed a questionnaire and interviewed Court personnel. We obtained a list of personnel to whom keys had been distributed and compared the list of key holders to an employment listing for the TDC to verify that all key holders were current employees of the Court.

To determine the adequacy of environmental protection controls, we performed a walk-through of the communication closet in the Courthouse's annex, storage room in the Courthouse, and areas housing microcomputer workstations to identify environmental protection requirements and evaluate environmental control provisions. We determined the adequacy of environmental controls over areas housing IT equipment through observation and completion of detailed questionnaires. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting; water detection; and temperature and humidity controls. To determine the conditions of the wiring for the computer network room, we observed and examined the wiring for general housekeeping and the security and stability of installation.

To assess the adequacy of business continuity planning, we determined whether the Court had user area plans to assist them in resuming operations should the WMS, PRA, or CARI systems be inoperable or inaccessible for an extended period. We also requested information regarding the Court's plan for recovering the Probation Department's OPMAN application. We interviewed management from the Court to determine whether a written, tested business continuity and disaster recovery plan was in place and in effect; whether or not the criticality of application systems had been assessed; and whether risks and exposures to computer operations had been evaluated. For the OPMAN application, we determined through interviews, procedures for generating backup copies of computer-related media for this application and then storing them in an off-site location.

Our test of system access security included a review of procedures to authorize, activate and deactivate access privileges to the systems used by the Court, but residing on the AOTC file servers. To determine whether only authorized employees could access the automated systems, we analyzed a list of current users for individuals authorized to access WMS, CARI, and PRA and compared them to current TDC personnel records. We performed the test by cross-referencing WMS, CARI, and PRA users from the user listing provided by AOTC to the current TDC personnel list to determine whether only current TDC employees had access to the automated systems. We reviewed control practices regarding logon ID and password

administration by evaluating the extent of documented policies and guidance provided to TDC personnel. In addition, we determined whether all employees authorized to access the automated systems were required to periodically change their passwords and assessed the frequency of password changes.

To determine whether adequate controls were in place and in effect to properly account for the Court's IT resources, we reviewed inventory control policies and procedures for property and equipment. We requested and received a copy of the AOTC's inventory system of record for the Court's IT resources. We considered the AOTC's master inventory as the official system of record for TDC, because the AOTC was responsible for maintaining fixed-asset inventory records for all courts. We reviewed the current system of record to determine whether it contained the appropriate data fields to identify, describe, value, and indicate location and condition of the IT resources. To determine whether the system of record, dated February 9, 2004, was current, accurate, complete and valid, we chose a random sample of 27 out of 124 Probation Department and Clerk Magistrate IT resources. For each item selected, we verified that the piece of equipment was locatable and that the identifying information regarding the item was properly reflected on the system of record. We also compared the IT-related system of record to the Court's inventory listings, maintained by both the Probation Department and Clerk Magistrate, and made note of any discrepancies.

To follow up on audit issues from our prior audit report, No. 2000-5076-3, and to gain and record an understanding of the issues, we reviewed the statewide report's audit results. To determine if appropriate corrective action had been taken to implement the prior audit recommendations, we reviewed the actions taken regarding the recommendations made in our audit report, we updated the results for existing conditions, and performed tests regarding the accounting and disposition of bail fund activity for the period of July 1, 2003 through April 30, 2004.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology, as issued by the Information Systems Audit and Control Association, July 2000, and the Commonwealth of Massachusetts Trial Court Fiscal System Manual.

AUDIT CONCLUSION

Based on our audit, adequate IT-related controls were not in place to provide reasonable assurance that control objectives would be met for system access security, physical security at the Courthouse, environmental protection at both the Courthouse and Probation's annex, and inventory control of IT-related resources at the Court. Although we found controls over physical security at the Probation's annex to be adequate, policies and procedures were not documented for this control area. We determined that the Probation Department had mechanisms for backing up the OPMAN system to assist in recovery efforts for this application. However, the Court did not have user area plans to ensure continuity of system availability for mission-critical and essential applications provided by AOTC. In addition, the Court did not have a recovery strategy for hard copy files stored in various locations at the Court.

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 department due to the nature and limited extent of the IT environment at the Court, an employee served as the informal liaison to AOTC regarding IT activities at the Court. Although the AOTC had limited IT-related policies and procedures, we found that certain controls over the use of IT-related resources at the Court needed to be strengthened, documented, and communicated to Court personnel to ensure that IT control objectives would be met. With respect to planned technology implementation, we also found that the Court had not been using the Basic Court Operations Tool (BasCOT) system, which is an application system used for tracking civil and small claim cases and available to other District Courts. Near the end of our audit, three Court employees had received the necessary training, and had begun to use the BasCOT system for tracking civil and small claim cases at the Court.

With respect to physical security, although we found certain physical security controls in place at the Courthouse and the Probation's annex, physical security controls and related documentation could be strengthened. We found that the Court needed to document policies and procedures related to physical security controls and to strengthen controls over the maintenance of keys for the Courthouse. In addition, we found that the Court needed to strengthen the physical access to the storeroom that contains computer network equipment and hard copy documents.

We determined that physical security over IT equipment was specifically assigned to designated individuals. All visitors were required to pass through a security checkpoint upon

entering the Courthouse. In addition, only authorized Courthouse staff occupied areas where microcomputer workstations and computer network equipment were located. Although surveillance cameras were in use, the Court needed to better monitor and document activity on a more consistent basis. We observed that the Courthouse had a security alarm that is activated and deactivated by a keypad control and the Chief Court Officer changes the keypad code on a regular basis.

Regarding key management at the Courthouse, we found that employees who were no longer employed by the Court were not required to turn in their access keys. The Court did not maintain an up-to-date list of authorized office key holders employed at the Courthouse because the Court did not have an established process to maintain a current list of key holders and to retrieve keys from terminated employees. In addition, the Court needed to strengthen physical security controls for the storeroom housing both IT network equipment and hardcopy files. For example, the Court did not maintain a list of individuals who should have access to the area. Our observations indicated the Court did not monitor access to the storeroom even though the area was rarely secured and public access to the area was available. As a result, there was inadequate assurance that IT equipment and hardcopy documents would be protected from unauthorized access, theft, or destruction.

Although physical security controls in place over the Probation's annex provided reasonable assurance that unauthorized access to IT resources would be prevented or detected, controls would be strengthened by documenting polices to help ensure compliance with physical security control procedures. We found that the Probation Department, which was located on the second floor of the annex, had closed circuit surveillance cameras and an alarm system. The area housing computer network equipment in the annex was not visible from the street or from adjacent corridors. The Probation Department maintains an access list of all probation staff that have physical keys and key pad codes. Keys for the Courthouse offices and communication closet housing IT equipment could not be duplicated. The Probation Department has installed motion detectors in locations that do not contain a security camera. These motion detectors are connected to the intrusion alarm system, which consists of a keypad control. In addition, we observed that all visitors were escorted to and from the second floor's entrance, which is protected by locked doors.

With respect to environmental protection controls at the Courthouse, our audit disclosed that controls needed to be strengthened. We found that the computer network room was located in the Courthouse's cellar and did not have proper environmental protection controls, such as heat

and humidity controls and water detection equipment. Computer network room wires and cables were not properly secured,and the general housekeeping and security of the wiring was inadequate. In addition, the equipment was tenuously located on man-made platforms supported by buckets on top of a cement slab placed on a dirt floor. We also found that the areas in which microcomputer workstations were located were overcrowded. We observed as many as six employees working in a small area that was originally designed for two people. We discussed this with management who indicated that this was not under their control, since the staff was required to work in this confined area to accommodate the Court's activities.

Regarding the Probation's annex, we found that certain environmental protection controls were in place. We found that both the computer network closet and the offices housing the microcomputer workstations had adequate general housekeeping procedures, smoke and heat detectors were installed, emergency lighting was available, and temperature and humidity levels were monitored and controlled by a computerized climate control system. However, at the time of our audit the annex did not have fire extinguishers or water sprinklers.

At the time of our audit, the Court was unaware of the general adequacy of any business continuity plans or strategies to be exercised by AOTC and did not have user area plans to address the loss of automated processing should IT systems be inoperable. 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 Court, in conjunction with AOTC, should address the risks of not being able to rely upon the continued availability of AOTC-based systems, or the loss of critical IT resources at the Court, including hardcopy court records pertaining to dockets and complaints, and to develop, in conjunction with AOTC, appropriate continuity or contingency plans to address business operations. Although we determined that the Court had implemented procedures for generating backup copies for the OPMAN application and storing the backup copies in a secure off-site location, the Court did not have a formal business continuity plan or an alternate processing site for resumption and use of this application in the event of a disaster.

Our review of access security controls indicated that the Court needed to strengthen access security controls to ensure timely notification for terminating active user accounts for the WMS application for users no longer requiring access to the application. Our review of system access security controls revealed that adequate control practices were in place to provide reasonable assurance that only authorized users were initially granted access privileges to the applications residing on the AOTC's file servers. Although we found the Court had provided timely

notification to deactivate access privileges for the CARI and PRA application systems, WMS access administrative procedures needed to be strengthened to ensure timely change or deactivation of user privileges for individuals no longer requiring access to this system. Our test, comparing an AOTC user list for the WMS application to a current list of Court employees, revealed that at the time of our audit, 18 out of the 61WMS users were no longer employed at the Court.

Regarding password administration, we found that Court personnel were not aware of AOTC guidelines concerning requirements for password construction and changing passwords in a timely basis. The Court had little guidance concerning password administration since there were only limited written policies and procedures contained in the AOTC's "Internal Control Guidelines, section 2.3.1" that outline parameters for password administration. In addition, during our audit, the AOTC issued "Information Technology Policy #1" on August 13, 2003, which formalized certain policies regarding IT-related security for all Court employees. However, we believe that due to the limited aspect of the technology policy and the confidential nature of the information residing on the Court's application systems, policies and procedures for password and user account administration should be strengthened by formalizing a process for terminating user accounts and then communicating to appropriate Court personnel any changes in policies and procedures for password administration.

Our review of inventory control of IT-related equipment revealed that controls needed to be strengthened to provide reasonable assurance that the Court's IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. The Court, which maintains inventory lists of IT resources for the Probation Department and the Clerk Magistrate's Office, respectively, had not conducted an annual physical inventory or reconciled inventory information to AOTC's system of record. Although the AOTC is responsible for maintaining a master inventory listing for all courts under its jurisdiction, the individual courts are expected to maintain an inventory record for local control. At the time of our audit, although the Court did provide an inventory record of hardware items, the lists were not an accurate and complete record for all IT-related items.

Our audit tests revealed that the AOTC's master inventory and the Court's inventory lists of IT resources were not in agreement and needed to be reconciled. We determined that the list received from AOTC, dated February 9, 2004, of IT asset inventory items, contained 124 items pertaining to 50 items located in the Clerk Magistrate's Office and 74 items located in the Probation Department. We found that 11 items that appeared on the TDC inventory list were not

on the AOTC inventory and nine items on the AOTC list were not included on the TDC lists. We determined that AOTC and the Court's inventory listings lacked essential information, such as historical cost, acquisition dates, and status of equipment in use. In addition, our review of equipment found that six items were not properly tagged.

We reviewed the audit results presented in our prior statewide audit report, No. 2000-5076-3, issued August 14, 2001. The prior audit report contained seven audit issues concerning bail funds, six of which we found to be resolved during our current audit period (see Appendix A, Page 24). We performed tests to evaluate the degree of corrective actions taken to address our prior audit recommendations. Our review of 59 case files out of 248 cases revealed that docket sheets, recognizance forms, and judge's releases were found in each of the case files tested. We also found that bail funds were properly documented on docket sheets for the same 59 case files tested. Between July 2002 and April 2004, we determined from our review of the Court's bail assignment process and cash journals that TDC was no longer assigning bail to probation officers in order to resolve unpaid court ordered assessments. However, we found that the Court was still not transferring out-of-jurisdiction bails to the appropriate Court and not depositing bails received into a separate bank account.

AUDIT RESULTS

1. Physical Security and Environmental Protection

With respect to physical security, although we found adequate physical security controls in place at the Probation's annex, we found that physical security controls at the Courthouse needed to be strengthened. We found that the Court needed to document policies and procedures related to physical security controls and to strengthen controls over the maintenance of keys for the Courthouse.

Our audit disclosed that the Court had certain physical security controls in place to safeguard IT-related resources. We found that all visitors entering the Courthouse through the main entrance must pass through a metal detector, and all packages must pass through an x-ray machine. We also determined that the Courthouse windows on the lower level and street floor were protected by diamond screen mesh to prevent ingress and egress to the Courthouse, and that the Court officers were required to file incident reports with the Security Department of the Trial Court. We determined that the back door of the Courthouse has a keypad, which has a code that is periodically changed. We found that the Courthouse has a surveillance camera on the back door that is in use during business hours, providing a videotape of individuals entering and exiting the Courthouse. However, we found that surveillance camera protection and intrusion alarm controls needed to be strengthened.

Regarding key management at the Courthouse, we found that key management controls needed to be strengthened. We found that neither the Chief Court Officer nor the Clerk Magistrate could provide a current and up-to-date list of key holders to the interior and exterior doors at the Courthouse. Since the Court did not have a process for retrieving keys from terminated employees, we could not determine whether individuals no longer employed at the Court had returned the keys that had been previously assigned to them. Furthermore, we found that an undetermined number of County employees had been assigned keys to the Courthouse and the Courthouse keys could be duplicated for interior and exterior doors. In addition, we found that the storeroom area housing network communication devices and case files was not properly secured, and was in a section of the Courthouse basement readily accessible to the public. Further, the Court did not maintain a storeroom access log.

Although we found that the Probation's annex had numerous physical security controls in place, the Probation Department did not have documented polices to ensure compliance with physical security controls procedures. The annex had close circuit surveillance equipment,

intrusion detection, and an ADT alarm system and restricted access to areas housing hubs, routers, and microcomputer workstations. The Probation Department has installed motion detectors in locations that do not contain a security camera. These motion detectors are connected to the intrusion alarm system, which consists of a keypad control. In addition, none of the Probation Department employees are required to sign a form prior to the issuance and return of keys. However, policies and procedures regarding physical security for the annex needed to be formalized and documented.

Our review revealed that there were certain environmental protection controls in place at the annex, such as an emergency evacuation plan for the entire building, air conditioning for areas housing microcomputer workstations, smoke and fire detection devices, fire extinguishers on each floor, procedures for conducting fire drills, and emergency shut off valves for all water lines. However, regarding the environmental protection, we found that there were no documented policies and the procedures at the Courthouse. We also found that the areas housing workstations were located in overcrowded offices. The area housing the network computer equipment and hardcopy records was located in a very cluttered area of the basement of the Courthouse and lacked adequate ventilation and smoke, water, temperature, air quality, and humidity detectors. The area was also exposed to foot traffic and the equipment was precariously located on a man-made platform supported by buckets on top of a cement slab on a dirt floor.

Regarding the annex, we found proper environmental protection regarding emergency lighting, and the maintenance of an air conditioning and air filtration system. The area housing network computer equipment was not exposed to water pipes and general housekeeping conditions were adequate. However, there were no documented policies and procedures for environmental protection and the annex lacked a fire alarm system; emergency evacuation plan; fire, smoke or heat detectors; fire suppression devices; and emergency water shut off valves.

Generally accepted computer industry practices indicate that appropriate physical security and environmental protection controls need to be in place to ensure that the information technology assets are operating in a safe and secure processing environment. IT-related assets should be protected and properly safeguarded against loss or damage due to heat, humidity, water, or fire. Appropriate physical security and environmental protection controls also serve to protect employees or other persons from undue harm. The Court should adopt appropriate physical security and environmental protection policies and procedures requiring that IT-related assets be protected from unauthorized access, use, damage, or theft.

Recommendation:

We recommend that the Court, in conjunction with the AOTC and the County Commissioner's Office, develop and maintain policies and procedures for physical security and environmental protection for all areas housing IT resources and communications equipment. In addition, we recommend that policies and procedures be developed regarding the issuance and administration and return of keys to Courthouse areas and that an accurate, up-to-date master key list be maintained to strengthen accountability and physical security and help ensure that only authorized access to the building is permitted. In addition, we recommend that the Court develop, document, and implement a process to retrieve keys from terminated employees and require completion of a standard form that will ensure that all access keys are returned when an employee is terminated. Furthermore, we recommend that the Court, in conjunction with the County Commissioners Office, review and document all county employees who have been issued a key to the Courthouse and include them on the master key list. We also recommend that the area housing network communication devices and hardcopy case files in the Courthouse be locked and the Court maintain a storeroom access log to assure only authorized entry. We recommend that all exterior doors be alarmed at the Courthouse. Furthermore, we recommend that the surveillance camera at the Courthouse be engaged during non-business hours, and the videotapes be subsequently reviewed.

Regarding environmental controls, the Court should evaluate the overcrowded conditions and communicate with both the County Commissioners' Office and AOTC the need for additional office space. We also recommend that the Court consider the installation of heat and smoke detectors; intrusion alarms on unalarmed exterior doors and windows; and temperature and air quality controls in the area housing the network computer equipment, as well as areas housing hardcopy records. In addition, we recommend that the Court communicate with AOTC regarding the relocation of the network computer equipment, currently housed in the basement of the Courthouse, to be relocated to a less cluttered and more environmentally sound area with properly secured wiring. Furthermore, we recommend that the Court consider the installation of emergency lighting where appropriate.

Regarding the Probation Department's annex, the Court should develop an emergency evacuation plan and install fire, smoke, and heat detectors, as well as a fire alarm system, fire extinguishers or water sprinklers.

Auditee's Response, Probation Department

We agree with the audit documenting the fact that the Probation Department's annex lacks certain fire detection and suppression systems, and note that these devices were not required in either the original or subsequent lease agreements entered into by the Administrative Office of the Trial Court and the Division of Capital Asset Management. Since the conclusion of the audit period, the landlord has provided fire extinguishers at several locations. The Probation annex does have emergency lighting and exit signage, and all employees and interns are aware of egress routes.

Auditee's Response, Clerk-Magistrate's Office:

The door to the cellar storeroom is now locked at all times and all Court Personnel must use a key to gain entry.

Auditor's Reply:

We agree that certain security procedures and personnel are in place, but certain controls for physical security and environmental protection should be implemented or improved for areas housing IT resources and equipment. We acknowledge that the Court has taken steps to enhance physical security and environmental protection. We recommend that the Court notify in writing the parties responsible for facility management of the rented offices as well as those parties at AOTC regarding funding for improving physical and environmental controls at the Court. Improvements in physical security and environmental protection would enable the Court to reduce the risk of damage to property, equipment and records from vandalism, fire, excessive heat or humidity, or water damage. The Court should institute, at a minimum and with limited cost, a key management policy, requiring that all employees who leave the employment of the Court return any and all keys to the Court facility.

2. System Access Security

Our audit revealed that system access security over the application systems used by the Court needed to be strengthened. Our review of access security controls indicated the Court needed to strengthen controls to ensure timely notification for terminating active user accounts for the WMS application for users no longer requiring access to the application since they are no longer employed by the Court. In addition, minimal documented policies and procedures regarding access security controls existed at the Court, and password administration control procedures needed to be strengthened to ensure that user accounts no longer required or authorized were deactivated in a timely manner.

At the time of the audit, we found there was no formal process, or standard electronic form, for notifying the AOTC of changes in employment status or terminations that would require user account access privileges to be changed or deactivated. We found that access privileges to the WMS application were not being deactivated in a timely manner when a Court employee was transferred or terminated employment from the Taunton District Court. Our test, comparing an AOTC user list for the WMS application to a current list of Court employees, revealed that at the time of our audit, 18 out of the 61WMS users were no longer employed at the Court.

We determined that because management had not established a mandatory timeframe for changing passwords, passwords had not been changed on a regular or frequent basis for the AOTC-supported applications. For application systems available through Court workstations, we found that passwords had not been changed in some cases for periods ranging from one to three years. Furthermore, access security functions were not being used to prompt users to change their passwords for access to the WMS applications. We found that password composition, length, and frequency of change needed to be reevaluated, formally documented, and communicated to all users. Generally accepted access security procedures and password syntax rules require that passwords be comprised of at least eight alpha/numeric characters, not be easy to guess, be of sufficient length, and be changed periodically. In addition, authorization and authentication mechanisms should be reviewed and maintained to support security administration.

Access to computer systems, program applications, and data files should be authorized on a need-to-know, need-to-perform, and need-to-protect basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact the individual's level of authorization. Appropriate notification procedures should be in place to ensure that access privileges are modified in a timely manner when changes occur in job responsibilities or employment status.

The failure to fully document and implement appropriate system access security policies and procedures may place critical systems and data files at risk to unauthorized access, modification, deletion, or loss of confidentiality. Given the nature of the Court's activities and operations and the sensitivity of information captured, stored and processed by the computer systems, access security to IT resources and systems is a critical IT-related function. Access security and user accounts should be reviewed on a relatively frequent basis.

The Commonwealth of Massachusetts' Internal Control Guide for Departments, promulgated by the Office of the State Comptroller, states in part, " . . . an employee's password should be

changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility." In addition, computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for security administration and proper protection of information assets. The policies and procedures should address authorization for system users, establishing and activating user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt, or unauthorized access. Lastly, appropriate mechanisms need to be in place to provide assurance that security policies and procedures are in effect to ensure that only authorized users have access to automated systems and on-line data files.

Recommendation:

We recommend that the Court, in conjunction with AOTC, document and formalize policies and procedures regarding access security controls. We also recommend that the Court, in conjunction with AOTC, establish a formal process, or standard electronic form to notify AOTC's Help Desk or security staff of changes in the status of TDC employment or employee responsibilities that requires timely deactivation or changes to user privileges. In addition, we recommend that policies and procedures regarding deactivation of access privileges be extended to address other changes in employee status that would impact and provide access, such as leaves of absence and job transfers.

We recommend that the Court work in conjunction with AOTC to develop and implement formal procedures for creating, assigning, monitoring, and deleting of passwords, and that the frequency of password changes regarding all Court applications be established and communicated to all users. We recommend that access procedures and password syntax rules be established or enhanced to include password composition, rules of use, password confidentiality, password length, frequency of changing passwords, responsibility for safeguarding passwords, authorization procedures, and timely notification in changes in employment or authorization status.

Auditee's Response, Probation Department

> *We agree with the auditor's finding that password syntax rules have not been formalized. CARI passwords emanate from the Office of the Commissioner of Probation (OCP) and periodically new passwords are assigned. PRA passwords originate locally, and there is a documented history that employees*

are required to change their password every six months. Employees who fail to do so are prevented from accessing the system. Syntax rules are being developed and we will request OCP to issue new CARI passwords concurrent when PRA passwords are changed.

Auditee's Response, Clerk-Magistrate's Office:

Active user accounts for the WMS have been updated. Guidelines concerning requirements for password construction and changing passwords in a timely basis will be followed.

Auditor's Reply:

While we note that system access security controls are primarily administered through AOTC and the Office of the Commissioner of Probation, Court management originally assigns user privileges and access security profiles to their staff. As such, the individual court exercises an important role in implementing access security procedures. In addition, because changes in employee status or responsibilities originate at the individual court, each court needs to take the steps necessary to ensure that only appropriate and authorized access is maintained. In that light, procedures, including notification to AOTC and the Office of the Commissioner of Probation, need to be followed so that required changes in access privileges to automated systems are addressed in a timely manner. We also suggest that the Court, in conjunction with AOTC and the Office of the Commissioner of Probation, document and ensure the presence of adequate access security controls. We recommend that detailed security reviews be performed to ensure all users have appropriate levels of access.

3. Business Continuity Planning

Our audit revealed that the Court, in conjunction with the AOTC, had not collaborated to develop a formal business continuity strategy, including user area plans, that would provide reasonable assurance that critical business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. Furthermore, the Court, in conjunction with AOTC, had not assessed the relative criticality of the automated systems supporting Court operations and identified the extent of potential risks and exposures to business operations. Although the AOTC generated backup copies of magnetic media for the business functions processed through AOTC's file servers, our audit revealed that the Court, in conjunction with AOTC, had not developed user area contingency plans to address a potential loss of automated processing. Without adequate disaster recovery and contingency planning, including required user area plans; the Court was at risk of not being able to perform

certain functions should the automated systems be disrupted or lost. A loss of processing capabilities could result in significant delays in processing caseloads. The environmental protection issues forwarded in our earlier audit finding, place even more emphasis on the Court's need to develop a detailed business continuity plan should mission-critical applications become unavailable for an extended period of time.

Without comprehensive, formal, and tested user area and contingency strategies, the Court's ability to access information related to the WMS operating on the AOTC's file servers, the CARI system operated by the Commissioner of Probation, as well as access to its in-house OPMAN application would be impeded. Without access to these application systems, the Court would be hindered from obtaining information regarding outstanding warrant information and unable to access all trial court dispositions regarding criminal cases. The absence of a comprehensive recovery strategy could seriously affect the Court's ability to regain critical and important data processing 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 policies and procedures to be followed, detailing the logical order for restoring operations either at the original site or at an alternate-processing site, and appropriate user area plans outlining recovery or contingency steps. The user area plans should be coordinated with overall enterprise-based business continuity plans. The Court, in conjunction with the AOTC, should also perform a risk analysis of the systems and identify the impact of lost or reduced processing capabilities.

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 entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

Recommendation:

In conjunction with the AOTC, the TDC should implement procedures to provide reasonable assurance that the criticality of automated systems is evaluated, business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the automated systems, and appropriate business continuity plans are developed for automated systems. Based on the results of the assessment, the Court should proceed with the development of a written

business continuity plan for its critical and essential functions. If feasible, the Court, at a minimum, should develop user area plans should mission-critical applications be unavailable.

The business continuity plan should document the Court's recovery strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. We further recommend that the business continuity plan be tested, then periodically reviewed and updated, as needed, to ensure that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response, Probation Department

> *We recognize the need for a business continuity plan and note that such a plan will require significant input from the Administrative Office of the Trial Court and the Office of the Commissioner of Probation. While no formal plan currently exists, the Probation Department has utilized the resources of another court to print checks. The Taunton Police Department has also provided this office access to their system to print records of criminal offenders when the Court server was disabled.*

Auditee's Response, Clerk-Magistrate's Office:

> *Although the auditee agreed with our audit recommendations, they chose not to respond in writing to this issue.*

Auditor's Reply:

We believe that the Court will be able to develop appropriate user area plans in concert with AOTC's IT Department. Efforts in this area will help ensure adequate system availability and provide reasonable assurance that critical data processing operations could be regained effectively and in a timely manner.

4. Inventory Control of IT Resources

At the time of our audit, we found that IT-related fixed-asset controls needed to be strengthened to provide for the proper accounting of the Court's inventory record. Our audit review of the AOTC master inventory record for hardware items and the TDC inventory of IT resources indicated that the inventory listings were not in agreement and needed to be reconciled. Although our audit revealed that IT-related equipment at the Court had vendor serial numbers and in most cases state asset tag numbers, our audit test revealed that the inventory record was not

accurate and complete and lacked essential fields of information such as historical cost, acquisition dates and status of equipment.

AOTC is responsible for maintaining the Court's IT-related fixed asset inventory records and 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's master record listing. Although the Court provided a record for its IT-related items, we could not determine when the Court performed an annual physical inventory or reconciled its inventory records to AOTC's system of record.

Our examination of the February 9, 2004 inventory record of the Taunton District Court provided by AOTC, consisting of 124 IT-related items for the Clerk Magistrate's Office and the Probation Department, revealed that there was incomplete data, such as historical cost, acquisition dates, and status of IT resources. Our test of the AOTC master inventory record disclosed that nine IT-related items were not included on the Court's in-house lists, and that 11 from a total of 126 items on the Court's in-house inventory lists were not found on the AOTC master inventory record. Also, our physical inspection of the Court's microcomputer workstations revealed that six items were not properly tagged. In addition, due to the lack of cost amounts on the inventory records, an accurate total value for the inventory could not be determined. Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained to properly account for all IT-related assets and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

The AOTC's "Internal Control Guidelines" state that, "All assets with a value over $100 must be inventoried on an annual basis and submitted to the AOTC, Fiscal Affairs Department." The Court should, in conjunction with AOTC, develop written procedures, maintain a perpetual inventory record, and perform an annual physical inventory and reconciliation of the Court's property and equipment to the AOTC's inventory record. During the course of our audit, AOTC issued a memorandum, on May 28, 2004, to all courts requiring each department within each court to establish a separate, reconciled fiscal-year-end fixed assets inventory and report to AOTC by October 1, 2004. The inventory is to include equipment type, status of equipment (disposition, surplus or obsolesce), tag number, location, manufacturer, model, cost, date of invoice and installation. From an IT configuration management perspective, all IT resources should be inventoried with appropriate information on the location and the status recorded.

Generally accepted industry standards and sound management practices dictate that adequate controls be implemented to account for and safeguard property and equipment. Although the Court's management indicated that they were unaware of Chapter 647 of the Acts of l989, it states, in part, that "…the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts."

Shortcomings in inventory control were the result of a lack of management attention and proper assignment of inventory control responsibilities. The absence of an accurate inventory record may hinder the Court's ability to manage IT-related resources and to detect theft and unauthorized use of IT-related assets. The lack of an up to date and accurate inventory hinders the Court's ability to assess its future technology and configuration management needs.

Recommendation:

The Court, in conjunction with AOTC, should enhance controls over its record-keeping to provide for maintenance of a perpetual hardware inventory record. We recommend that the perpetual inventory include historical cost data, acquisition dates, and tag numbers for all equipment. Based on the results of the review, the Court, in conjunction with the AOTC, should implement formal policies and procedures to include compliance with all state reporting requirements for fixed assets. Additionally, the Court should include practices regarding the maintenance of a perpetual inventory, and perform an annual physical inventory and reconciliation of all physical assets.

We believe that the Court should comply with the policies and procedures documented in the AOTC "Internal Control Guidelines" pertaining to inventory control. Specifically, the Court should maintain a perpetual inventory that is periodically reconciled to the physical assets and records of purchased and surplus or lost equipment. To maintain proper internal control, a staff person who is not responsible for maintaining the inventory record of property and equipment should perform the periodic reconciliation. Further, the inventory record once reconciled should be used as the basis for documenting the Commonwealth's required asset-management reports.

We recommend that the Court enter all property and equipment into the fixed-asset inventory record at the date of acquisition or date of installation. The Court should work, in conjunction with the AOTC, to ensure that the inventory records are current, accurate, and complete. In

addition, we recommend that the Court's management be aware of Chapter 647 of the Acts of l989.

Auditee's Response, Probation Department

> *The Probation Department periodically reconciles furniture and equipment allocated to the office, however historical cost data has not always been provided at the time of receipt or installation. We recognize the need to work locally as a Court, in conjunction with the Administrative Office of the Trial Court, to ensure that an annual physical inventory and reconciliation of physical assets is instituted.*

Auditee's Response, Clerk-Magistrate's Office:

> *A physical inventory list of the Clerk's office equipment was taken and submitted to the Judge's Lobby on September 9, 2004 and will be updated yearly. Inventory of the Clerk's Office IT resources was completed and forwarded on October 29, 2003 to John Beaton.*

Auditor's Reply:

We are pleased that the Court is taking steps to strengthen the integrity of the fixed-asset inventory record. We believe that once the Court's inventory has been reconciled and updated to the AOTC's master list, the Court should maintain a perpetual inventory record that is reconciled periodically with AOTC's master inventory record. We will examine the progress made to the fixed-asset inventory record during our follow-up audit.

APPENDIX A
PRIOR AUDIT RESULTS

Summary and Disposition of Prior Audit Results from
The Office of the State Auditor's Report:
Audit Report No. 2000-5049-3

Issue (Prior Conditions and Prior Recommendations)	Current Status (what they have done to correct)	Disposition
1. Inadequate Internal Controls in Notifying Owners of Unclaimed Bails and Forwarding Forfeited and Abandoned Bails to the State Treasurer: Recommendation: Immediately process and forward all forfeited bail funds to the State Treasurer; review cases identified as unclaimed for three years from completion date and remit bail to the State Treasurer, in accordance with Chapter 200A, Section 6, of the General Laws; ensure that sureties are notified of any bail remaining unclaimed one year after the date of the resolution of each case by sending out certified letters to the sureties; and perform monthly reviews of bail records to ensure future compliance with state laws and regulations governing bail. Additionally, we recommended that AOTC continue to provide oversight and direction to the Divisions relative to forfeited, abandoned, and unclaimed bail matters.	The Court currently processes and forwards all forfeited bail funds to the State Treasurer; reviews cases identified as unclaimed for three years from completion date and remits bail to the State Treasurer in accordance with Chapter 200A, Section 6, of the General Laws. The Court has established procedures to ensure that sureties are notified of any bail remaining unclaimed one year after the date of the resolution of each case by sending out certified letters to the sureties, and the Court performs monthly reviews of bail records to ensure future compliance with state laws and regulations governing bail.	Resolved

2. Bail Funds Were Not Forfeited Following Defendant Defaults: Recommendation: Immediately forfeit the bail that applies and transmit these funds to the State Treasurer. All District Court Divisions should review the status of bails on hand to determine whether other bails qualify for forfeiture. In the future, Divisions should promptly forfeit bails at the time of a defendant's default. In the event that a defendant subsequently provides a reasonable explanation for his/her actions, the Division can request a refund from the State Treasurer for the bail earlier transmitted.	Currently, the Court does forfeit all applicable, forfeited and defendant default bails and transmits the funds to the State Treasurer. The Court also reviews the status of bails on hand to determine whether the bails qualify for forfeiture and then promptly forfeits the bails at the time of a defendant's default.	Resolved
3. Inappropriate Processing of Out-of-Jurisdiction Bails: Recommendation: The Court should not accept out-of-jurisdiction bails after hours from its Bail Magistrates and should adhere to the Fiscal Systems Manual's policies and procedures governing bail processing.	The Court is still accepting out-of-jurisdiction bails after hours from its Bail Magistrates and is not adhering to the Fiscal Systems Manual's policies and procedures governing bail processing.	Unresolved
4. Inadequate Maintenance of Case Papers (The docket sheet and recognizance form were missing from the case papers, and personnel could not locate entire case files): Recommendation: Taunton should continue looking for the missing case files in order to determine the status and appropriate disposition of the bails. In the future, the Divisions should ensure that an adequate tracking system is in place to monitor the removal and return of case papers. Furthermore, AOTC should ensure that a determination is made and full accounting performed for the 32 unaccounted for case papers.	The Court has currently established an adequate tracking system that is in place to monitor the removal and return of case files. We also found that all materials related to individual case files were located in the proper file.	Resolved
5. Improper Validation of Bail Receipts:	The Court now validates all docket sheets for all cash bails received, in	Resolved

Recommendation: The Taunton Division should validate the docket sheet for all cash bails received, in accordance with Section 9.3 of the Fiscal Systems Manual. If the Taunton Division cannot validate docket sheets, then the Division should request AOTC's guidance on the matter.	accordance with Section 9.3 of the Fiscal Systems Manual.	
6. Bail Assignment Process Results in the Inefficient Use of Court Resources: (District Court justices commonly assign bail to probation officers in order to resolve unpaid court ordered assessments (e.g., fines, court costs, victim witness fees): Recommendation: The Trial Court should continue moving forward with developing a standard bail assignment process and develop a central system that can be implemented at court locations throughout the Commonwealth. Such a system would improve efficiency within the Clerk-Magistrate's and Probation Offices, allowing Division personnel to address other important court matters.	The Court currently makes all checks out to the defendant. To resolve unpaid fees, the staff escorts the defendant with the check over to the Probation Department and has the defendant endorse the check.	Resolved
7. Divisions Have Not Maintained a Bail Receipt File or Documented Bail Release Authorizations: Recommendation: These Divisions should take steps to ensure that all policies and procedures established by AOTC are implemented in a timely manner. Moreover, if a Division believes a section of the Fiscal Systems Manual is redundant or unnecessary, then the Division should request relief from AOTC.	The Court now maintains a bail receipt file and has implemented a process for tracking bail release authorizations.	Resolved

APPENDIX B

Additional Comment from Kevan J. Cunningham

First Justice

Nov.22, 2004

Perhaps most importantly, as you are aware, we are Trial Court of the Commonwealth employees in a Bristol County building of almost two hundred years of age. We are one of the ten busiest Courts in the Commonwealth with the worst physical plant of all Courts. We are not handicap accessible, we do not have a lockup facility to handle the often violent defendants brought to us and just within the last several years we have finally left the age of the scrivener and entered the world of the computer. We struggle with our caseload with at best three judges spread over two Courts. We deserve more help, but due to the limitations of our building, we do not receive that help.

There are some situation beyond our control such as the location and storage of our computer systems. We have no place other than a dirt floored basement to house our system nor do we have air conditioning anywhere in our building, let alone for our "IT" resources.

The good news, I hope, is that we are moving at some point in the future to a facility where we will be able to address the concerns raised in the audit. I have already discussed those mutual concerns with Richard L'Heroux of AOTC, the individual in charge of the Cohannet School project, and I assure you your audit will serve as a foundation for our policies and procedures in our new Court. On behalf of the Court, I thank you for your time, effort and recommendations presented to us in this audit report.