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

A. JOSEPH DeNUCCI
AUDITOR

AUDIT NO. 2004-1147-4T

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

July 1, 2002 through February 23, 2004

OFFICIAL AUDIT REPORT

JUNE 10, 2004

TABLE OF CONTENTS

INTRODUCTION

The Waltham District Court (WDC) is organized under Chapter 211B and Chapter 218, Section 1 of the Massachusetts General Laws. The Court's organization and management structure consists of the Judge's Lobby, the Clerk Magistrate's Office and the Probation Department. The Court hears a wide range of criminal, civil, housing, juvenile, mental health, and other types of cases for the City of Waltham and the towns of Watertown and Weston. The Waltham District Court received $1,522,574 of state funds and processed revenue of $878,625 from sources such as cash bail receipts, fines, fees, and penalties for fiscal year 2003.

Chapter 478 of the Acts of 1978 reorganized the courts into seven Trial Court departments, including the District Court. A central administrative office, known as the Administrative Office of the Trial Court, (AOTC) was created at that time supervised by the Chief Justice for Administration and Management responsible for the overall management of the Trial Court. From an information technology (IT) perspective, the AOTC supports the mission and business objectives of the District Courts by administering the IT infrastructure, including mission-critical application systems installed on the file servers and mainframes located at the AOTC's Information Technology Department in Cambridge. In addition, the AOTC provides IT services and technical support to individual courts and maintains master inventory records for the courts under its jurisdiction.

The District Court's criminal jurisdiction extends to all felonies punishable by a sentence of up to five years, and many other specific felonies with greater potential penalties; all misdemeanors; and all violations of city and town ordinances and by-laws. In felonies not within the District Court's final jurisdiction, the District Court conducts probable cause hearings to determine whether a defendant should be bound over to Superior Court. District Court magistrates conduct hearings to issue criminal complaints and arrest warrants, and to determine whether there is probable cause to detain persons arrested without a warrant. Both judges and magistrates issue criminal and administrative search warrants. In civil matters, District Court judges sitting in Middlesex County conduct both jury-waived trials and determine any matter in which the likelihood of recovery does not exceed $25,000. In all counties, the District Court adjudicates small claims involving up to $2,000 (initially tried by a magistrate, with a defense right of appeal either to a judge or a jury). Fifteen of the District Court judges serve on the Appellate Division, which is an appellate tribunal of three-judge panels that is organized in three geographical districts to review questions of law that arise in civil cases.

The District Court's civil jurisdiction also includes many specialized proceedings: inquests; summary process (evictions); supplementary process (to enforce money judgments); and abuse prevention

restraining orders. Some District Court divisions in Middlesex County (including WDC) exercise limited jurisdiction in juvenile cases (delinquency, child abuse or neglect, and children in need of services). Many Middlesex County District Court divisions (as well as WDC) exercise jurisdiction in mental health matters including involuntary civil commitments and medication orders; supervision of criminal defendants committed for mental observation or deemed incompetent to stand trial or after an insanity acquittal; appeals from certain administrative agencies involving, for example, firearms licenses or unemployment compensation; civil motor vehicle infractions (tried initially to a magistrate, with right of appeal to a judge); and equitable injunctions exercising general equity jurisdiction.

At the time of our audit, the Waltham District Court's computer operations were supported by 21 microcomputer workstations, of which 13 were in the Clerk Magistrate's Office, six in the Probation Department, and two in the Judge's Lobby and court rooms. In addition, one laptop computer was located in the Judge's Lobby. The workstations were connected by a router and two switches to the AOTC's wide area network (WAN) through an IBM Netfinity file server located at the AOTC data center in Cambridge. The Court utilizes the Warrant Management System (WMS) and the Basic Court Operation Tools (BasCOT) which are maintained by the AOTC, and the Probation Receipt Accounting System (PRA) and Criminal Activity Record Information System (CARI), maintained by the Office of the Commissioner of Probation. In addition, the Court utilizes the Human Resources Compensation Management System (HR/CMS) payroll system maintained by the State Comptroller's Office.

The Clerk Magistrate's Office uses WMS to track warrants issued from all courts under the jurisdiction of the AOTC. The Probation Department uses the CARI system to access information on all dispositions from courts regarding criminal offenses and restraining orders, and the PRA system to account for fines and fees.

The Office of the State Auditor's examination focused on a review of certain IT-related general controls over the Court's computer operations.

SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) related audit at the Waltham District Court (WDC) from October 23, 2003 through February 24, 2004. The audit covered the period of July 1, 2002 through February 23, 2004.

The scope of our audit included an evaluation of IT-related controls pertaining to IT organization and management, physical security, environmental protection, logical access security, inventory control over IT-related assets, disaster recovery and business continuity planning, and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control framework, including policies, procedures, practices, and organizational structure provided reasonable assurance that 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. Our objective regarding logical access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to automated systems available through the Court's workstations. Further, we sought to determine whether the WDC, 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. In addition, we determined whether the Court, in conjunction with AOTC, had a business continuity strategy, including user area plans in place to assist them in regaining business operations supported by technology within an acceptable period should a disaster render computerized functions inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether adequate off-site storage of back up media was in effect to assist recovery efforts.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior court personnel. To obtain an understanding of the internal control environment, we reviewed the Court's organizational structure and primary business functions. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities, and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation, and assessed relevant IT-related internal controls. Our work was limited to personnel who performed IT-related functions and a review of AOTC's IT-related policies and procedures. Our audit did not encompass a review of AOTC's centrally-controlled IT facilities.

To evaluate physical security, we interviewed management and security personnel, conducted walk-throughs, observed security devices, and reviewed procedures to document and address security violations and/or incidents. We requested a list of key holders to the courthouse offices and verified whether those individuals were current employees. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined the existence of controls, such as office door locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees of the Court and that these areas were restricted to only Court personnel. In addition, we reviewed the Court's emergency evacuation plan.

To determine the adequacy of environmental controls, we interviewed the Director of Facilities Management and observed areas housing computer equipment. We also conducted walk-throughs and evaluated controls in selected areas in order to assess the sufficiency of documented control-related policies and procedures. We examined the areas housing IT equipment at the Court to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression measures; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures. We confirmed the existence and functionality of the main and local controls of the heating, ventilation, and air conditioning system (HVAC) and reviewed the operating instructions for the fire alarm system. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of logical access security included a review of procedures used to authorize, activate, and deactivate access privileges to the AOTC file servers through the microcomputer workstations located at

the Court. Since the Court does not administer activation and deactivation of user accounts, we relied upon our understanding as obtained on audit work performed for audit number 2002-1106-4T of AOTC's procedures for performing these functions. To determine whether only authorized employees were accessing the automated systems, we obtained user lists from AOTC and the Office of the Commissioner of Probation for individuals granted access privileges to the automated systems used by the Court and compared the lists to the Court's current payroll listing of employees obtained through HR/CMS. We reviewed control practices regarding logon ID and password administration and evaluated the extent of documented policies and guidance provided to the WDC personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for IT-resources located at the Court, we reviewed inventory control policies and procedures and requested a copy of the Court's inventory of IT resources and AOTC's system of record for the Court's IT resources. Even though we did request the Court's inventory control records for IT-related assets, we considered the AOTC's master inventory as the official system of record because the AOTC was responsible for maintaining fixed asset inventory records and promulgating related policies and procedures for all courts. We traced 100% of the IT-related items on the AOTC master inventory listing to the items on the floor. We further reconciled the inventory record to the equipment by serial number, tag number, location, and description of the item. We also determined whether the Court maintained an inventory record of IT resources that could be reconciled to the AOTC's inventory system of record and was being updated when necessary upon changes in equipment or its location.

To assess the adequacy of business continuity planning, we evaluated the extent to which the Court had user area plans that could be activated in conjunction with AOTC's disaster recovery plans to resume IT operations should mission-critical and essential application systems be rendered inoperable or inaccessible. We determined whether the Court was aware of AOTC's business continuity plans and efforts to resume IT operations should the application or communication systems be rendered inoperable. We interviewed senior management at the Court to determine whether the Court had determined, in conjunction with AOTC, the criticality of application systems, and the associated risks and exposures to computer operations. In addition, we determined through interviews with our Office's audit staff conducting an IT audit at the AOTC, whether AOTC was storing backup copies of computer-related media in an off-site location.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) 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 (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Our audit disclosed that although the Court, in conjunction with AOTC, had internal controls in place over physical security, environmental protection, and off-site storage of backup computer media, certain controls pertaining to IT organization and management, IT-related inventory, logical access security, and business continuity planning needed to be strengthened.

Our audit revealed that physical security controls throughout the Court provided reasonable assurance that WDC's IT-resources would be adequately protected. We found that security to the entrance of the courthouse was adequate as all visitors were required to pass through a metal detector and a hand-held magnetometer inspection when entering the Court. In addition, all packages were required to be scanned through an X-ray machine. We observed that the WDC employed remote cameras and intrusion alarms throughout the courthouse. Our observations of the Court's telecommunication area, which contains equipment that enables access to the mission-critical application systems utilized by the Court, indicated that access was limited to only authorized personnel. The room which houses the server and the Verizon T-1 lines is kept locked at all times, with only four employees authorized to access it. Our review confirmed that Court management maintained a list of individuals having keys for office areas throughout the courthouse, and that the individuals listed were current employees. However, we determined that physical security controls needed to be strengthened by creating and maintaining a key register detailing the dates that keys were assigned and the areas of access, along with the individual's name, and that procedures needed to be documented regarding the distribution, safekeeping, and return of keys.

Our audit revealed that adequate environmental protection controls were in place and operating within the Court's offices and the area housing the telecommunication equipment with respect to general housekeeping, heating, ventilation, and air conditioning, emergency lighting; and smoke and heat detectors. The fire alarm system was connected to the local fire department, and hand-held fire extinguishers (inspected annually) were located in strategic areas throughout the building. We found that the Court had an emergency evacuation plan in place, and that the operating instructions for the fire alarm system, which included a floor plan for the six zones, were clearly delineated and adequate. An uninterruptible power supply (UPS) was installed and regular battery status assessments were made to protect against power failures and fluctuations.

Our review of logical access security controls revealed that adequate control practices were in place to provide reasonable assurance that only authorized users were granted access privileges to the applications residing on the AOTC's file servers operating through the Court's workstations. Our audit revealed that although access privileges for individuals no longer employed by the Court had been removed by AOTC, controls were not in place to ensure that AOTC is notified in a timely and standard

manner that user account privileges need to be modified or deactivated. However, we found that Court personnel were not required to change their passwords, and there was little indication that password administration was being monitored. There were limited written policies and procedures contained in the AOTC's "Internal Control Guidelines section 2.3.1" that outline parameters for password administration. AOTC issued Information Technology Policy #1 on August 13, 2003, which formalizes certain policies regarding IT-related security policies and procedures for all court employees. Due to the confidential nature of the information residing on the application systems used by the Court, policies and procedures for password administration should be strengthened and communicated to appropriate court personnel to ensure that appropriate passwords are used, safeguarded, not shared, and changed on a regular basis. Court management should ensure that the levels of access to certain application systems are appropriate for the individual's job classification and responsibilities. We recommend that passwords for all systems be changed at least every sixty days and monitored for compliance.

Our review of the Court's organization and management over IT-related activities disclosed that the primary IT functions were supported and maintained by the AOTC's IT Department. Although job descriptions for staff existed at the Court, they did not include reference to IT-related responsibilities. Our examination of the Court's organization and management revealed that there was an established chain of command. Due to the nature and limited extent of the IT environment at the Court, there was no established IT department. However, two employees served, in addition to maintaining their regular Court responsibilities, as the liaisons between the Court and AOTC regarding IT-related issues. Given that AOTC had not defined IT-related areas of responsibility for the Court or communicated required IT policies and procedures, Court personnel were unaware of generally accepted control practices and did not have clear operational standards and guidance for performing IT related tasks and activities.

Our review 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. Although certain inventory controls are centrally handled by AOTC, the Court needed to strengthen its controls to provide reasonable assurance that IT resources would be properly recorded and accounted for. At the time of our audit, the Court did not maintain its own inventory record of IT resources, and the Court had not conducted an annual physical inventory or reconciled its 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 we began our audit, the Court could not provide a current and complete record for all IT-related items.

At the time of our audit, the Court did not have business continuity, or user plans, to address the loss of automated processing should IT systems be inoperable. The Court was also unaware of the general

adequacy of any business continuity plans or strategies to be exercised by AOTC. 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 needs to address the risks of not being able to rely upon the continued availability of AOTC-based systems, access to AOTC systems, or the loss of critical IT resources at the Court, and to develop, in conjunction with AOTC, appropriate continuity or contingency plans.

AUDIT RESULTS

1. IT Organization and Management

Although our audit revealed that the Court had certain IT-related general controls in place, overall IT organization and management controls needed to be strengthened in order to provide the Court with an appropriately-documented internal control framework for IT functions and activity. The Court would benefit by having a comprehensive set of written IT policies and procedures in place to ensure that IT-related controls would be exercised and that control objectives would be met. Since IT operations are limited to accessing information and transaction processing and are supported by a centralized IT Department within AOTC, the extent of required policies and procedures for IT-related functions should be focused on system users and be evaluated and prepared in conjunction with AOTC. While there may be limitations in allocating staff resources to document IT-related policies and procedures, overall control practices would be strengthened by documenting policies and procedures regarding physical security, environmental protection, business continuity planning, system access security and password management, and inventory control of IT resources. In addition, it would be beneficial for the Court to be able to access documented procedures covering IT planning, risk assessment, risk management, data management, virus protection, physical and logical access security, business continuity planning, and monitoring and reporting of IT activities.

Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff, serve as a good basis for evaluation, and enhance communication among personnel to improve operating effectiveness and efficiency. Documented roles and responsibilities and associated policies and procedures enable trained personnel to develop a broader understanding of their duties and improve their level of competence.

In the absence of formal policies, standards and procedures, employees may rely on individual interpretation of what is required to be performed or how to best manage and control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result, and important control practices may not be adequately addressed. Furthermore, the absence of documented policies and procedures undermines management’s ability to monitor and evaluate IT related functions and activities of operations and application systems. In addition to generally accepted control practices, documented and approved internal control procedures are required of all state agencies under Chapter 647 of the Acts of 1989.

Recommendation:

We recommend that the Court, in conjunction with AOTC, begin documenting its IT-related policies and procedures to provide sufficient, formal guidance for IT-related tasks and activities. Control practices would be strengthened by written IT- related policies and procedures regarding physical security, business continuity planning, environmental protection, hardware and software inventory, access security and password administration and procedures to address IT job descriptions for IT functions performed at the Court. Documented procedures would help ensure that important operational and control objectives would be met.

Auditee's Response:

The Auditee agreed with our audit recommendations, but chose not to respond in writing.

Auditor's Reply:

Documented controls, policies, and procedures provide a framework to guide and direct staff in the discharge of their responsibilities. The nature and extent of the documented control procedures also needs to accommodate staff experience, competency and knowledge. Development of documented policies and procedures should be done in conjunction with AOTC's implementation of the new MassCourts application.

2. 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 for IT resources. The Waltham District Court could not provide us with a current IT-related fixed asset inventory listing. The WDC did not maintain a perpetual inventory system that included conducting an annual physical inventory and reconciling the listing to the actual equipment on hand and to AOTC's master inventory record. Although the AOTC has overall responsibility for maintaining a master inventory file for all fixed assets across the Trial Court, 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.

Our examination of the inventory record of the Waltham District Court provided by AOTC, consisting of 63 IT-related items, reflected the resources at the Waltham District Court with the exception of one laptop computer, but revealed that there was incomplete data, such as historical cost, acquisition dates, purchase order numbers, receiving records, and surplus and lost equipment. We traced all of the IT related items, except for the laptop computer, from the AOTC master inventory record to the items on the floor. We further reconciled the inventory record to the equipment by serial number, tag number, location, and description of the item.

Although we found that all 63 IT-related items on the AOTC master inventory could be physically located and verified, the inventory list did not include a laptop computer and due to the lack of cost amounts on the inventory records, an accurate total value for the Court's IT inventory could not be determined. Because of the extent of the deficiencies in the system of record and the general absence of inventory control practices in effect, we did not perform tests of inventory against records of procurement.

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 Court, in conjunction with AOTC, must initiate assurance mechanisms to help ensure that inventory systems of record can be properly maintained, safeguarded and available when needed.

The AOTC's "Internal Control Guidelines" states, "All assets with a value over $100 must be inventoried on an annual basis and submitted to the AOTC, Fiscal Affairs Department." The Court, in conjunction with AOTC, should 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. From an IT configuration management perspective, all IT resources should be inventoried with information recorded, such as to their status and location.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989, 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."

The lack of adequate inventory control was the result of insufficient 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 the status and location of equipment. The Court

should implement control practices regarding the maintenance of the perpetual inventory and perform an annual reconciliation of all physical assets to the AOTC inventory system of record.

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, staff person(s) not responsible for maintaining the inventory record of property and equipment, should perform the periodic reconciliation.

Auditee's Response:

The Auditee agreed with our audit recommendations, but chose not to respond in writing.

Auditor's Reply:

We will review the corrective actions taken to improve your inventory controls by reconciling your records to AOTC's at the time of our next audit.

3. Business Continuity and Contingency 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 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.

Without comprehensive, formal, and tested user area and contingency strategies, the Court's ability to access information related to the WMS and BasCOT operating on the AOTC's file servers, and the CARI and PRA systems operated by the Commissioner of Probation would be impeded. Without access to these application systems, the Court would be hindered from obtaining information regarding outstanding warrant information, or unable to confirm that fines, fees, and penalties were being collected by the Probation Department. Furthermore, the Court would be 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 success of the business continuity planning process requires management commitment and management and system user involvement to help ensure that there is a clear understanding of IT processing requirements, that appropriate IT and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available. The Court, in conjunction with the AOTC, should 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.

We believe that AOTC and Court management have not emphasized the importance of developing business continuity and contingency plans along with user area plans to address the loss of automated systems for an extended period of time.

Recommendation:

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

The business continuity plan, or user area plan, should document the Court's recovery and contingency 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 recommend that business continuity and user area plans be tested and periodically reviewed and updated, as needed, to ensure their viability. The

completed plans should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response:

The Auditee agreed with our audit recommendations, but chose not to respond in writing.

Auditor's Reply:

We believe that the Court will be able to strengthen its business continuity plan by developing appropriate user area plans in concert with AOTC's IT Department. Efforts on the part of AOTC and the court 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.

Appendix
Summary of Internal Control Practices
Waltham District Court
as of February 23, 2004

Pg. Ref.	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
6	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, computer rooms, microcomputer workstations, and court records in hardcopy form so that loss or damage is prevented.	Control over access to offices, computer rooms, file servers, microcomputer workstations, laptop computers, designated facilities manager, intrusion devices, locked doors, foot patrols.	In Effect	Certain Controls	Adequate, for authorized personnel listings.
6	Environmental Protection	Provide reasonable assurance that IT-related resources are adequately protected from loss or damage.	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures.	In Effect	Certain Controls	Adequate, for emergency and evacuation procedures.

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Appendix
Summary of Internal Control Practices
Waltham District Court
as of February 23, 2004

Pg. Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
6-7	System Access Security	Provide reasonable assurance that only authorized users are granted system access to automated systems.	Passwords required to access automated systems, changes of passwords required; formal rules for password formation and use; formal procedures for authorization, activation, and deactivation of logon IDs and passwords.	Insufficient, Informal procedures in place	No	Inadequate
7 10-12 Audit Results	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record, and reported on, when appropriate, to oversight entity.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed, software inventory maintained.	Insufficient	No	Inadequate
7-8 12-14 Audit Results	Business Continuity Planning	Provide reasonable assurance that essential mission-critical functions can be resumed in a timely manner should file servers and microcomputer workstations be rendered inoperable.	Current, formal, tested business continuity plan; periodic review and modification of plan; plan implemented, distributed, and staff trained in its use.	Insufficient	No	Inadequate
7 9-10 Audit Results	Organization and Management	To ensure that adequate organizational and management controls are in effect over IT activities to ensure that such activities are managed effectively and efficiently. To review the documentation of organizational controls over and within the IT environment.	Document a comprehensive set of written policies and procedures for IT-related control functions; effective evaluations and training; enhance communication of staff; IT- related job descriptions: clear lines of command.	Insufficient	Certain Controls	Inadequate

Appendix
Summary of Internal Control Practices
Waltham District Court
as of February 23, 2004

Pg. Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
5,12	On-site storage	Provide reasonable assurance that backup of magnetic media are available should automated systems be rendered inoperable	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage area are adequate; storage area is in a separate on-site location	In Effect	Certain Controls	Inadequate
5,8,12	Off-site storage	Provide reasonable assurance that critical and important media are available should automated systems be rendered inoperable	Same as above. Storage area in a separate location	In Effect	Yes, AOTC	Adequate