

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200



A. JOSEPH DeNUCCI

AUDITOR

No. 2002-1106-4T

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

July 1, 2001 through July 21, 2003

OFFICIAL AUDIT
REPORT
JUNE 22, 2004

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	4
AUDIT CONCLUSION	11
Auditee's Response	18
Auditor's Reply	19
AUDIT RESULTS	20
1. IT Organization and Management	20
2. System Access Security	48
3. Inventory Control and IT Configuration Management	59
4. Disaster Recovery and Business Continuity Planning	65
APPENDIX	
A Full Text of Auditee Response	72
B Auditor's Reply	78

INTRODUCTION

The Massachusetts Trial Court was created under Chapter 478 of the Acts of 1978. The 1978 statute reorganized the courts into seven Trial Court Departments: the Boston Municipal Court, the District Court, the Housing Court, the Juvenile Court, the Probate and Family Court, the Superior Court, and the Land Court. The Act established the responsibility for the administration of each court under the charge of Administrative Justices.

The 1978 statute also created a central administrative office managed by a Chief Administrative Justice, who was also responsible for the overall management of the Trial Court. The statute delegated responsibility to the central office, now called the Administrative Office of the Trial Court (AOTC), with developing a wide range of centralized functions and standards for the benefit of the entire Trial Court system. These functions included the development of a budget for the Trial Court, central accounting and procurement systems, and personnel policies, procedures and standards for judges and staff who were formerly employed by the counties.

In 1992, the Massachusetts Legislature enacted a second court reorganization bill, Chapter 379 of the Acts of 1992. The structure of the Trial Court remained the same encompassing the same seven departments, each with a Chief Justice rather than an Administrative Justice, and the central office headed by a judge to be known as the Chief Justice for Administration and Management. The current duties and responsibilities of the Chief Justice for Administration and Management are to provide oversight for the Trial Court, including responsibility for management and security of facilities, centralized control and oversight for maintenance of fixed asset system of record, and the purchase, distribution, and support of IT resources.

The Massachusetts Trial Court, which falls under the general superintendence of the Supreme Judicial Court, has oversight responsibility through the central Administrative Office of the seven court departments, the Office of the Jury Commissioner, and the Office of the Commissioner of Probation. There are three hundred and sixty-two authorized judicial positions in the Trial Court. Trial judges sit in more than one hundred and thirty locations across the state and the Trial Court employs more than 6,500 people. AOTC's primary objective is to enhance the administration of justice in the Commonwealth. The AOTC's organizational structure consists of nine departments: Court Capital Projects, Court Facilities, Fiscal, Information Technology, Judicial Institute, Legal, Human Resources, Planning and Development, and Security.

The AOTC and the Trial Court are supported by the information technology services provided by AOTC's Information Technology (IT) Department. The mission statement for the Information

Technology Department of AOTC is to pro-actively support the data processing and information system needs of the Trial Court through the use of information technology.

At the time of the audit, the IT Department had responsibility for the selection, deployment, implementation and support of computer systems and networks used by the Trial Court. The IT Department falls under the supervision of the Chief Justice for Administration and Management. The IT Department's staff are located at two sites: Two Center Plaza, which housed 25 staff including senior management and fiscal staff providing general guidance and budget support, local area network (LAN) and database administrative staff, clerical staff and a help desk function; and the Cambridge data center, where seven staff were located to provide computer operations for the various application systems, and to perform back up functions. In addition, there were three technical field staff that support Trial Court locations throughout the state. Additionally there was a Project Management Office (PMO) consisting of three management and 17 support staff. The PMO had the responsibility to manage the implementation of the new MassCourts application system that will integrate case management throughout the Trial Court.

At the time of our audit, the AOTC's computer operations included over 5,000 workstations located at the AOTC office and court facilities throughout the state. Data communication between the AOTC and the court facilities was supported by various local area networks at individual courts and a wide area network (WAN) to which AOTC and the courts were connected. The local area networks and the wide area network had the characteristics of star topology and ring topology. The mainframe computers, the IBM AIX RS/6000 SP and the UNISYS ClearPath, at the Cambridge data center support, store, backup and restore data residing on various Windows and Linux file servers located at different courts through T-1 and T-3 lines. The AOTC network provides access to court computing activities that include e-mail, case management, warrant information, court activity records, payment information, account history, and Internet access.

At the time of the audit, there were a number of application systems providing support to the courts' business operations. The Basic Court Operation Tools (BasCOT) is used for civil and criminal case management by Land Courts, Probate and Family Courts, the Boston Municipal Court, and the District Courts. The FORECOURT application system is used for case management by the Superior Courts. The Court Activity Records Information (CARI), is used by probation departments throughout the Trial Court to track all dispositions from courts regarding criminal and juvenile offenses, restraining orders, and the sex offender registry. Many of the trial courts also use a jury selection software package called JURY for tracking jurors. Probation departments throughout the Trial Court also use the Probation Receipt Accounting (PRA) application to process and track receipts and disbursements under the supervision of the Office of the Commissioner of Probation. The Probate and Family Courts, the District

Courts, and the Superior Courts use the Warrant Management System (WMS) to track outstanding warrant information. The Juvenile Courts also use an application called JURIS, which tracks juvenile subjects from the time a complaint or petition is filed against or on behalf of the individual through probation of the individual, maintains all pertinent docket and probation information, updates information as it is entered, and is maintained on the Data General system. The AOTC also utilizes several software packages, including WordPerfect for word processing and Excel for spreadsheets. Access to the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources/Compensation Management System (HR/CMS) is limited to authorized AOTC personnel.

In 1992, the Massachusetts State Legislature also charged the Judicial Branch of government with developing a technology plan for automating the Massachusetts Trial Court. Funded by a capital bond, the plan called for a comprehensive, integrated automation of the Trial Court. In response, the AOTC established a dedicated Project Management Office that was funded by the capital bond to select a vendor to provide an integrated court system. The new integrated system, known as the MassCourts application system (referred to as the Project), will support the main case management processes specifically performed by the Trial Court departments and offices. During the course of our audit, the PMO selection committee selected a vendor, MAXIMUS Inc., for this project. The project will be implemented over a three-year period.

Subsequent to the audit period and completion of our fieldwork, the Honorable Robert A. Mulligan was appointed to the position of Chief Justice for Administration and Management. Our report and recommendations are intended to assist the new administration in formulating a comprehensive IT governance framework.

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over the AOTC's IT Department's information technology operations and the framework for IT internal control at AOTC and the Trial Court.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) general controls audit of IT functions and activities at the Administrative Office of the Trial Court (AOTC), from July 1, 2002 to July 21, 2003 covering the period July 1, 2001 through July 21, 2003. The scope of our audit included an examination of control practices and procedures related to IT organization and management, system access security, physical security and environmental protection over and within the administrative offices and the Cambridge data center, hardware inventory including procedures for IT infrastructure planning, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media. During our audit, we also gained and recorded an understanding of the MassCourts Project and management techniques being used for the project's implementation.

Audit Objectives

Our primary audit objectives were to determine whether the IT-related control environment provided reasonable assurance that control objectives would be met to support business functions of the AOTC and the Trial Court and to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. More specifically, we sought to determine whether IT organizational and management controls were in effect over information technology activities to ensure such activities would be managed effectively and efficiently and the IT policies and procedures were adequately documented. In conjunction with our review of the control environment and IT organization and management, we determined whether AOTC had established a sufficient IT planning framework to generate and implement: long-range strategic and short-range tactical plans to help fulfill the AOTC's mission and goals; written and approved policies and procedures regarding the proper accounting for, authorized access to, and safeguarding of its IT-related assets; procedures for IT infrastructure planning; and a sufficient IT organizational structure and steering committee to oversee and monitor AOTC's information technology functions and activities. We also sought to determine whether an internal audit function and quality assurance standards existed to ensure adequate monitoring and evaluation procedures were in place for IT-related activities.

We sought to evaluate whether adequate controls were in place to safeguard information against unauthorized use, disclosure, modification and damage, or loss of the data files and software residing on the AOTC's automated systems, and further whether adequate physical security was in place to restrict access to AOTC's LAN file servers and microcomputer workstations to prevent loss of, or damage to,

computer equipment or IT-related media. We also sought to determine whether adequate environmental protection controls were in place over IT resources at the AOTC Center Plaza offices and at the area housing AOTC's file servers located at the Cambridge data center to prevent and detect damage to equipment and data or other IT-related media.

Our objective with respect to the AOTC's hardware inventory was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT resources were properly accounted for in an inventory record and safeguarded against unauthorized use, theft, or damage and whether appropriate data was being recorded to support configuration management decisions.

Regarding system availability, we determined whether controls were in place to provide reasonable assurance, through a business continuity plan and access to backup copies of system and data files, that required IT processing could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether adequate on-site and off-site storage of backup media was in effect to assist recovery efforts.

Finally, we sought to gain an understanding of the MassCourts Project and to determine whether adequate management controls were in place to support the implementation and future operation of the MassCourts system and to provide reasonable assurance that project objectives would be met.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of enabling legislation and relevant operations, including the IT infrastructure and in-house software applications, reviewing documentation and interviewing management and staff regarding AOTC's mission, operations, and IT organization and management.

To determine the appropriateness of documented IT controls, we reviewed relevant Commonwealth statutes, policies, procedures, and IT industry standards regarding IT security and internal control. We interviewed the AOTC's Acting Chief Information Officer, the MassCourts IT Project Executive and Project Manager, other AOTC staff at Center Plaza and the Cambridge Data center to obtain an understanding of the AOTC's operations, the IT systems infrastructure, the IT control environment and the organizational structure of the IT Department and the Project Management Office. To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we evaluated the degree to which the AOTC had documented, authorized, and approved IT-related control policies and procedures. To assess the adequacy of general controls regarding IT-related operations, we interviewed AOTC IT Department staff, observed operations, and performed selected audit tests.

Regarding our examination of organization and management, we interviewed IT Department senior management, completed questionnaires, analyzed and reviewed the organizational structure and reporting lines of the AOTC IT Department; requested documented IT policies and procedures; and reviewed and analyzed the existing IT-related policies, standards, procedures and strategic plans to determine their adequacy. We also determined whether AOTC's IT-related job descriptions were up-to-date and assessed the IT Department's organizational structure for unity of command, span of management and points of accountability. To determine whether the IT-related job descriptions and specifications were up-to-date and reflected current responsibilities and technology knowledge requirements, we obtained a current list of the personnel employed by the IT Department and compared the list to the IT Department organizational chart and the employee's IT-related responsibilities. To determine whether an IT-related steering committee was in place and operating for the purpose of providing adequate oversight of IT functions and processes across AOTC and the Trial Court, we interviewed senior management and IT staff. We obtained a further understanding through interviews of user department management and staff during ongoing IT audits being conducted at the Trial Court by our Office. In addition, we requested minutes of steering committee meetings.

We reviewed the adequacy of operational and management controls, including documentation of the AOTC IT Department's mission, the adequacy of monitoring and evaluation procedures for IT-related functions and activities, and the extent of management supervision. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented and were monitored for compliance. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe and comply with statutes, regulations, and generally accepted control objectives for IT operations and security. We also reviewed the extent of IT-related contracts with third-party service providers.

To determine whether IT-related assets were adequately safeguarded from damage or loss, we reviewed physical security over IT resources through observation and interviews with the IT Department staff at Center Plaza and the Cambridge data center. We reviewed physical security over IT resources at the central office through observation and by evaluating controls for gaining access to the Center Plaza offices. We determined whether procedures were in place and effect to help prevent unauthorized persons from gaining access to the data center and whether authorized personnel were specifically instructed in physical security operational standards and procedures. We reviewed potential risk factors regarding physical security through inspection of the data center and interviews with the management and staff responsible for the data center. Through observation, we evaluated whether doors to the data center were locked at all times, that a list of persons authorized to be in the data center was posted within the data center, and that a log was being maintained of those not on the list who were permitted access to the

data center. To determine whether vendor agreements were in place to cover hardware maintenance and respond to hardware failures, we interviewed data center and AOTC's Fiscal Department staff and reviewed the appropriate contracts.

We also reviewed environmental protection over IT resources through observation and interviews with the IT Department staff. To determine the adequacy of environmental protection, we conducted a walk-through of the Cambridge data center, interviewed the facilities manager, and assessed the sufficiency of environmental protection-related policies and procedures for the data center and the on-site storage area for backup copies of computer media. During the audit, we determined and verified the existence of certain environmental protection controls, such as heat, water, smoke detectors; fire suppression measures; general housekeeping; and uninterruptible power supplies for the Cambridge data center's file servers and mainframe computers.

To assess the adequacy of controls to provide continued operations and system availability, we assessed the degree to which disaster recovery and business continuity plans were required and documented for the AOTC and whether steps had been taken to implement recovery and contingency plans to regain mission-critical application systems and important operations should IT systems be rendered inoperable or inaccessible. In addition, we interviewed the IT Department staff to determine whether a written, tested business continuity plan was in place, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We also determined whether an alternate processing site had been designated to be used in the event that the Cambridge data center was damaged or inaccessible. We determined whether an alternate processing site would be available, such as a hot site provided through a contract with a third party, to allow the AOTC to recover its IT functions in a timely manner. Further, we interviewed data center staff to determine whether the staff had been trained in their recovery and security responsibilities in the event of an emergency or disaster.

We reviewed AOTC's backup procedures and assessed the degree to which copies of backup media were stored in secure on-site and off-site locations through interviews with the IT Department staff and an inspection of the on-site and off-site storage facilities. As part of our review of the adequacy of generation and storage of backup copies of magnetic media, we assessed relevant policies and procedures and the adequacy of physical security and environmental protection controls for on-site and off-site storage of magnetic media. We reviewed the adequacy and completeness of current backup procedures in place. We also inspected the on-site daily backup copies of computer media to determine the provisions for storage, frequency of backup, and adequacy of controls in place to protect the backup media. Further, we interviewed IT Department personnel to determine whether they were being formally trained in the procedures of performing backups and were aware of on-site and off-site storage procedures

and the steps required to safeguard the backup media. We further sought to determine whether designated data center personnel were cognizant of, and trained in, procedures to restore systems via backup media that would be required under disaster or emergency circumstances. Also, we examined the off-site storage facility of the third-party vendor to determine whether the area housing the backup computer media had adequate physical security and environmental protection controls. We analyzed the physical access security for the off-site storage facility in order to determine whether the backup copies of computer media were secured from unauthorized access, accidental or purposeful damage, unauthorized examination, removal, or disclosure of confidential information.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated application systems. To determine whether AOTC's control practices regarding system access security adequately prevented unauthorized access to the automated systems, we initially sought to obtain policies and procedures regarding system access and data security and reviewed the appropriateness of stated controls. To determine whether system access security controls were in place to provide reasonable assurance that only personnel authorized to use the AOTC's network and microcomputer systems were able to gain access to programs and data files, we requested documented policies related to access security and evaluated procedures for logon user ID and password administration. Regarding password administration, we reviewed controls for authorization and activation and deactivation of user IDs and passwords, and requirements for the appropriate length, composition and frequency of change of passwords. We determined the frequency with which all staff authorized to access the automated systems were required to change their passwords.

To determine whether user ID and password security was being properly maintained, we interviewed the security administrator and other IT Department personnel. To determine whether access privileges were provided to only authorized users, we reviewed procedures for granting system access and compared a system-generated list of current E-Mail, BasCOT, FORECOURT, and WMS users to an AOTC generated list of current employees and conducted interviews. We determined whether procedures were in place to provide reasonable assurance that the AOTC's security administrator would be notified in a timely manner of changes in personnel status (e.g., employment terminations, job transfers, or leaves of absence) that would impact access privileges and possibly require deactivation of access privileges to the network or automated systems. To determine whether there were adequate controls in place to prevent unauthorized entry to desktop computers and the Court's E-Mail system, we conducted limited penetration tests.

To determine whether adequate controls were in place and in effect to properly account for AOTC's IT resources, we reviewed inventory control procedures for hardware and software. We obtained and reviewed the hardware inventory system of record as maintained by the IT Department. To determine

whether the AOTC's hardware inventory system of record was current, accurate, and valid, we compared a selected sample of hardware inventory items listed on the computer hardware inventory record to the actual computer hardware on hand. We reviewed the AOTC's IT inventory record at the beginning of our audit to determine whether the inventory record contained appropriate data fields, such as identification, description, historical cost, location and condition of the items and whether the AOTC had conducted an annual physical inventory of IT-related assets. Due to a lack of financial data on the inventory record, we obtained and analyzed court expenditures for hardware purchases for fiscal year 1997 through fiscal year 2002 to estimate the value of the AOTC's and the Trial Court's hardware which we estimated to be valued over \$17,000,000. We conducted data analysis of the inventory record that listed computer hardware for the IT Department and individual courts. We judgmentally sampled 195 items out of a total population of 21,027 hardware items listed on AOTC's system of record at AOTC and tested all 78 hardware items listed as assigned to the Hampshire Probate and Family Court. We evaluated the adequacy of inventory controls through these tests and observations by assessing the integrity of the inventory record, determining whether computer hardware was properly tagged, and whether the serial numbers attached to the item were properly recorded on the inventory list. Inventory tests were conducted at the AOTC offices at Two Center Plaza, the Cambridge data center, and the Hampshire Probate and Family Court. We also determined whether adequate controls were in place to provide reasonable assurance that computer software would be properly accounted for by interviewing IT Department staff and reviewing the inventory record.

To gain an understanding of the MassCourts Project and to determine whether adequate management controls were in place to provide reasonable assurance that project objectives would be met, we interviewed the MassCourts IT Project Executive, the Project Manager and other staff working on the project. We also reviewed the request for proposal, the formal contract, and other project documents related to the planning and status of the project, including staff resources, deliverables and tasks breakdown.

Our review was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. The audit criteria used for our control examinations were based on applicable legal requirements, control objectives and generally accepted IT control practices. In addition to generally accepted controls, audit criteria were drawn from CobiT for management control practices. CobiT (Control Objectives for Information and Related Technology), is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners, IT functions, users, and auditors.

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 IT organization and management, system access security, IT-related inventory control and configuration management, and disaster recovery and business continuity planning. Adequate controls and assurance mechanisms were not in place to provide AOTC with reasonable assurance that control objectives would be met regarding the integrity, security, efficiency, and availability of IT processing activities, and the safeguarding and accounting of IT resources, including data files, programs, documentation and computer equipment across the Trial Court. AOTC must develop and implement a comprehensive IT governance and control framework and assurance mechanisms to ensure that IT control objectives will be met.

The AOTC needs to implement a cohesive organizational structure within which the IT Department, Program Management Office, and IT-related positions within the courts are linked together with clear points of accountability. Second, management direction needs to be well documented in terms of IT strategic and tactical plans, coupled together with IT policies, standards, and management directives that are supplemented by project plans, budgets, and performance measurement. Third, increased management efforts must be made regarding the security of systems, IT configuration management, and business continuity planning. Unless appropriate IT governance principles can be implemented on an enterprise-based perspective, the Trial Court places successful and timely implementation of the MassCourts Project at continued risk.

Although certain controls were in place, IT strategic and tactical planning and IT-related organization and management controls needed to be strengthened to adequately define a well-communicated direction and ensure that appropriate IT policies and procedures, points of accountability, segregation of duties, and monitoring and evaluation would be in effect. Adequate controls were not in effect to provide reasonable assurance that only authorized parties could gain access to court systems, that IT resources were properly accounted for and safeguarded, and that automated systems and electronic data availability could be regained should IT systems become inoperable or inaccessible.

Although the audit's focus at the request of the AOTC was the IT Department and not the Program Management Office (PMO) or the MassCourts Project, we acknowledge that senior AOTC management were aware that IT operational and control deficiencies needed to be addressed within the IT Department and across the courts. However, until control deficiencies have been adequately addressed, strategic planning and court initiatives under the umbrella of the MassCourts Project must incorporate appropriate risk analysis and additional control measures to offset existing control and operational risks.

Regarding strategic planning, we acknowledge that the PMO had a documented strategic plan for the MassCourts Project. At the time that we were briefed on the plan, it appeared to be well organized and detailed. However, there was little indication that the IT Department had either provided substantive input to the MassCourts Project plan or had an IT strategic plan for their own areas of responsibility. There was no evidence that there had been clear directives for the IT Department to develop documented IT strategic and tactical plans for IT projects and initiatives. Effective strategic planning should direct the AOTC's actions and incorporate performance measurement as a management tool. The lack of a comprehensive long-range IT Department strategic plan increases the risk that critical future system development or IT-related acquisitions may not achieve management's business objectives or meet user expectations and that time and budget over-runs could result. We found that the AOTC needed to implement a comprehensive planning process to address the acquisition, deployment, and management of IT resources, including outsourced IT services.

With respect to enterprise-based management, the IT strategic planning process should be extended to address all IT-related functions across the courts and include all departments and personnel responsible for providing IT services. IT strategic planning should be aligned with overall strategic planning for the Trial Court's business objectives. The scope and detail of the IT strategic plan should be comprehensive enough to support tactical planning activities. And, in addition to the metrics that would be applied to individual initiatives, functions and projects, the strategic planning process should incorporate mechanisms to measure the use of resources and resulting performance. The implementation and maintenance of sound IT-related project management techniques combined with IT related tactical plans that support strategic initiatives would enhance the AOTC's efforts to manage, control and benefit from IT functions and systems. Implementation of these planning mechanisms is a critical success factor for the successful implementation and rollout of the MassCourts application system across the Trial Court.

We found that policies and procedures necessary to guide IT functions and activities needed to be clearly defined and formally documented. The nature and extent of documented IT policies and procedures found in place were insufficient to adequately direct IT activities and provide reasonable assurance that IT control objectives would be met within the IT Department and across the enterprise. In addition, our audit indicated that two of the critical success factors to having a viable system of internal control were generally absent. First, appropriate mechanisms were not in place to ensure a clear understanding of risks and vulnerabilities. At the time of our review, AOTC management had not adopted a comprehensive risk assessment approach to identify IT risks and control vulnerabilities. Management's ability to mitigate risk within the Trial Court's IT environment and adequately address internal control was significantly inhibited by not conducting IT-related risk assessments and by not having a risk management function. The process of risk assessment assists management in identifying

risk and the associated impact to the organization. Second, mechanisms were not in place to provide assurance that controls were working as intended and that control objectives would be met. At the time of our audit, there was an almost complete lack of monitoring and evaluation of control practices within the IT environment.

The failure to have tactical plans, established policies and procedures, and generally accepted control practices placed the integrity, security and availability of IT-generated information and systems at risk. We found that the AOTC IT management agreed with the need to develop documented IT-related control practices and they have, subsequent to our discussions with senior management, started to address these concerns.

At the time of our audit, we found weaknesses in organizational structure and management control over IT functions. Our audit revealed that a court-wide IT organizational structure had not been established with well-defined and communicated roles and responsibilities. In addition, the absence of clear points of accountability placed at risk AOTC's ability to ensure that IT-related tasks and activities were properly addressed, and to facilitate a comprehensive IT strategy for effective direction and adequate control of IT functions throughout the Trial Court. We also found that an adequate level of oversight had not been established and maintained by senior management to ensure that IT functions and activities were adequately controlled. Although the PMO was subject to management oversight, neither the IT Department nor personnel performing IT-related functions within the courts were subject to oversight from an IT steering committee. The absence of a steering committee to set IT direction, review and approve IT policies and procedures, and evaluate IT performance placed the IT Department at risk to misdirect its efforts. In addition, there was inadequate segregation of duties regarding the help desk staff performing access security functions.

Regarding resource management, AOTC should ensure that job descriptions and assigned responsibilities for personnel performing IT-related duties in conjunction with their respective jobs and positions clearly delineate IT-related responsibilities being performed. Reporting mechanisms should be established to permit IT management to regularly verify that personnel performing specific IT-related tasks throughout the AOTC and the Trial Court are following standards and accepted practices, and that personnel are qualified on the basis of appropriate education, training and/or experience. Senior management should also implement a division of roles and responsibilities that should exclude the possibility for a single individual to subvert a critical process and should clearly segregate security functions from operational and support activities.

While reviewing IT human resource management activities, we noted that performance evaluations were not performed in the IT Department or for IT liaison personnel within the Trial Court. Control over the IT process of managing human resources must consider the business requirement of acquiring and

maintaining a motivated and competent workforce and maximizing personnel performance through sound, fair and clear personnel management practices to recruit, train, evaluate, compensate, promote and dismiss staff.

In regards to quality assurance, the AOTC had not established adequate monitoring and evaluation policies, procedures and functions to ensure that business and internal control objectives for IT processes and activities would be met. The IT Department did not have a quality assurance mechanism to review and monitor IT functions and activities against established standards and criteria. A quality management program should be established with an appropriate approach regarding quality assurance that covers both general and project-specific quality assurance activities. During our audit period, we noted that the AOTC had not used their Internal Audit Department to review or examine IT operations and functions within the Trial Court. We recommend that AOTC's Internal Audit develop the capability to conduct general IT control and application system audits and be realigned within the organizational structure to ensure adequate independence and reporting to a higher level of management.

We believe that adequate IT-related controls were in place over physical security and environmental protection at the AOTC's Center Plaza offices and the Cambridge data center to ensure that IT resources were adequately safeguarded and protected. Adequate controls were also in place for the Cambridge data center's generation and on-site and off-site storage of backup media. The latter is a necessary step toward providing business continuity capabilities for assisting recovery efforts should IT systems be rendered inoperable or inaccessible.

Regarding system access, our audit disclosed that the AOTC had not established adequate system access security controls over its IT systems to prevent or detect unauthorized access or use. First, we noted that access security to automated systems was being performed by staff from the IT Department's help desk, rather than by a properly segregated security function. Second, appropriate policies and procedures were not in place to provide a control foundation for access security. Although there were limited controls for initiating user access, documented policies and procedures were not in place to provide adequate assurance that only authorized individuals would have access to automated systems and related data files. During our review of system access, our penetration testing revealed that one could gain access to files, e-mail, and potentially to systems through desktop computers without using a user ID or password. Further, although there was limited monitoring of system access, it appeared to be more focused on network traffic and availability, rather than confirming that only appropriate access privileges were being granted. At the time of our audit, the IT Department could not produce a comprehensive list of user accounts indicating the systems and related access privileges for each user.

We found that controls needed to be strengthened to ensure that user IDs and passwords would be active for only authorized personnel and that appropriate password standards would be followed.

Security access privileges should be deactivated in a timely manner for users no longer needing or authorized access to automated systems or on-line data. At the time of our audit, we found that the AOTC help desk staff and acting security administrator were not being consistently notified in a timely manner by department heads or the AOTC's Human Resources Department of changes in employment status of users having access to automated systems throughout the Trial Court. Our testing of access privileges to WMS, BasCOT, FORECOURT and e-mail revealed that access privileges had not been deactivated for hundreds of individuals no longer employed by the AOTC or the Trial Court. Also regarding password administration, passwords for court employees were often not changed for years, and passwords for certain applications consisted of as little as one character.

The absence of adequate controls over system access security placed critical and confidential information at risk. Without proper access restrictions, the Trial Court's system data and programs were placed at risk of unauthorized access or use, which could have led to modifications, deletions, or disclosure of critical or confidential data. An access security framework should be established which includes security policies and standards; risk and vulnerability assessment; a detailed security plan; an independent security function; mechanisms for authorization and authentication; centralized user account management; password standards; security awareness and training; security assessment; incident reporting; and monitoring and evaluation. AOTC should also identify requirements for a working relationship and points of accountability for those responsible for physical and logical access security to automated systems and supporting technology. As the Trial Court moves toward web-enabled application systems and processing, access security functions also need to include intrusion detection and prevention, application security, hardening of systems, and strong access security administration.

Our audit disclosed that adequate controls were not in effect to provide reasonable assurance that AOTC's inventory system of record of IT resources within AOTC and across the Trial Court had a sufficient level of integrity. We found that AOTC's master list of IT inventory, which was being updated and reconciled during our audit, was not complete or accurate. The problem of accounting for IT resources was compounded by not having individual courts either maintain their own inventory lists to be reconciled to the AOTC master list, or use the AOTC master list as their primary source of inventory information. We found that AOTC was not following their own established fixed-asset inventory guidelines, effective July 1, 1998, in that IT resources with a value of \$100 or more were not being accounted for in the fixed-asset inventory and that an annual physical inventory and reconciliation of IT resources was not being conducted. We determined that the established procedures for fixed-asset control were not consistently monitored and evaluated for compliance to safeguard and properly account for IT-related assets. As a result, AOTC could not provide reasonable assurance that its system of record for IT-related resources, with an approximate value of \$17 million, could be relied upon.

From a fixed-asset inventory perspective, IT resources were included on two inventory lists, one maintained by the Fiscal Affairs Department and the other by the IT Department. We found the IT Department's list appeared to be more complete for tracking IT equipment that pertained to installations in separate courts. However, the IT Department's separate inventory system of record of IT resources, which included only computer hardware, had not been properly maintained or updated and was missing in many instances essential information regarding historical cost, date of purchase, installation date, tag number, and status.

Although AOTC's IT Department was responsible for acquisition, installation, and accounting for IT resources, inventory records and procedures did not provide adequate assurance that all IT-related assets were properly listed and identified. We view that the accounting of all property and equipment should be a centralized function administered by the Fiscal Affairs Department responsible for maintaining the official system of record. During our audit, the AOTC had initiated a physical inventory of IT-related hardware to establish an inventory for the AOTC and throughout the Trial Court. By the end of our audit, the physical inventory of IT resources had not been completed for all court locations, nor reconciled with individual courts and procurement and surplus property records. Without sufficient inventory controls over IT-related assets, the potential for misuse, loss, or theft of hardware items increases, and configuration management decisions, especially in light of the implementation of the new MassCourts application system, may be hindered. Inventory control procedures are necessary to ensure that the AOTC's system of record properly accounts for IT resources and supports IT configuration management within the Trial Court.

Our audit indicated that significant improvements in business continuity planning were warranted to ensure that automated systems could be recovered or that appropriate contingency plans could be initiated should IT systems be rendered inoperable or inaccessible. Although the AOTC had taken limited measures to address disaster recovery and business continuity planning, our audit disclosed that these efforts were not comprehensive or sufficiently documented. We note that an enterprise-based business continuity and contingency strategy for the Cambridge data center and across the Trial Court had not been developed. Additionally, criticality and risk assessments of application systems, supporting technology, and processing environments had not been performed to assist business continuity planning. We also note that primary or original hardcopy files, which are maintained at most court locations, would be irretrievable if lost or damaged. Although backup copies of magnetic media were readily available, an alternate processing site for the Cambridge data center had not been designated. As a result, should a disaster occur, the restoration of automated systems within an acceptable period of time would be jeopardized. Without sufficient business continuity planning, an extended loss of AOTC's computer

operations could hinder access to processing capabilities and electronic information needed to perform essential Trial Court functions.

The AOTC and the Trial Court should perform a criticality assessment of all application systems and a thorough risk analysis of the systems and the IT environment. In conjunction with their user community, the AOTC should develop, document, and test disaster recovery and business continuity strategies and contingency plans for the Trial Court. The IT Department needs to identify a viable alternate processing site to help ensure the resumption of IT operations within an acceptable time period. We further recommend that the business continuity plans be periodically reviewed, updated and tested to the extent possible to ensure their viability and the accuracy and completeness of required information.

Our limited review of the MassCourts Project indicated that certain project management controls appeared to be in place. However, the success of the MassCourts Project will remain at risk unless an appropriate framework of controls for IT governance is established, including management commitment and appropriate assurance mechanisms across all IT functions within the IT Department and the Trial Court.

Subsequent to the completion of our audit, the IT Department has come under new leadership through the appointment of an IT Director. In addition, a change in administration occurred through the appointment of a new Chief Justice of the Administrative Office of the Trial Court. Our meetings with senior management before and after the change in administration indicated a strong commitment to addressing issues being brought forward in the audit. Our observations are that senior management under the new administration has increased the level of collaboration among all departments at AOTC to improve IT management and strengthen internal control. Continued efforts to monitor and evaluate internal control must be made to address IT control objectives and ensure the successful implementation of the MassCourts Project.

Auditee's Response

Auditee Response from Robert A. Mulligan,
Chief Justice for Administration and Management

For the past several years the Administrative Office of the Trial Court has been moving towards developing and implementing an integrated, comprehensive computer system for the entire Trial Court known as MassCourts. The retirement of the prior Director of Information Technology Department presented a unique opportunity to reexamine the structure and function of that Department. To that end, the AOTC requested that the State Auditor conduct an "IT Audit" of the Trial Court's IT Department. It was hoped that such an audit would provide a working blue-print for the improvements that would be necessary to be sure that the correct structure, policies, and procedures were present to maintain and to operate MassCourts as soon as it was in place.

The Audit Report that you have provided fulfills those expectations. Thank you for the comprehensive and complete assessment of the IT Department. The recommendations and suggestions that are contained within that document provide the needed framework that will enable further progress to be made. This Office will move to implement those recommendations as quickly and as fully as resources allow. To begin with, the "CobiT Standards" will be adopted as applicable and appropriate to the work of the Trial Court and they will provide the baseline for all future endeavors. We greatly appreciate that your office has provided us with an electronic version of the CobiT standards to serve as a framework for this policy development initiative.

As the report notes, the audit covers the period between July 1, 2001 to July 21, 2003. Since the conclusion of the audit, there has been a change in the administration in the Trial Court as well as a change in the leadership of the IT Department. The report acknowledges that improvements have been made during the audit period, and we believe that considerable progress has continued after the end of the formal audit period. For example, as the Audit Report noted, "senior management under the new administration [of the Trial Court] has increased the level of collaboration among all departments at AOTC to improve IT management and strengthen internal control." Further, there has been a recognition of the need for formal written IT related policies and several of those policies have already been developed and implemented. More will be promulgated in the near future.

We have begun to address System Access and Security issues. The Audit Report noted, "a strong effort [has been] made to identify and document all user accounts that needed to be deactivated." In fact, formal communications between the Human Resources Department and the IT Department has resulted in the regular deactivating of IT access for former employees of the Trial Court. The need for a formal and accurate inventory control system has been recognized. The IT Department has begun to actively pursue different options for an effective Disaster Recovery program.

I am attaching a document which identifies some specific recent improvements that have occurred as recommended in the audit report. These efforts, however, are not complete and much more remains to be done. The Administrative Office of the Trial Court will continue to work collaboratively with your Department in order to put in place the appropriate standards and controls for the Trial Court in its efforts to serve all the citizens of this Commonwealth.

Thank you again for providing us with such a thoughtful blueprint to guide our efforts to improve the IT environment.

Auditor's Reply

We are pleased that our audit report and recommendations have provided guidance for AOTC to develop and implement a comprehensive and appropriate enterprise-based IT control framework and a blueprint for reform for IT activities, functions and operations throughout the Trial Court. While we commend the AOTC for the corrective actions that were initiated during and following our audit, the issues described in the report's audit results section existed during the course of the audit and that the corrective actions implemented have not fully addressed all of our audit recommendations. While we recognize the difficulties in implementing all the control recommendations, corrective efforts will help ensure adequate integrity, security and availability of IT operations, application systems and data throughout AOTC and the Trial Court.

In addition to including the auditee's response after the conclusion section of our report, we have incorporated AOTC's comments on individual findings within the text of the report's audit results section, as well as providing the full text of those responses in Appendix A.

AUDIT RESULTS

1. IT Organization and Management

Although the IT Department had certain controls in place, the overall framework of controls pertaining to the department and the IT environment that it serves lacked adequate policy and standards, risk assessment, planning and direction, and monitoring to ensure that control objectives would be addressed regarding the integrity, security, and availability of systems and the management of IT resources. Management control practices needed to be strengthened to provide more comprehensive guidance through documented policies and procedures, a cohesive organizational structure with more clearly established points of accountability, and monitoring and evaluation mechanisms to provide reasonable assurance that control objectives would be met.

We did find that the IT Department's control environment was positive regarding physical security and environmental protection of IT resources under their charge. Adequate physical and environmental controls were found in place over the IT Department's data center and AOTC's office areas housing IT resources. In addition, appropriate management control practices appeared to be in place for the generation and storage of back-up copies of magnetic media at the IT Department's data center. Also from a management perspective, nothing came to our attention to indicate material issues on computer or network operations. However, appropriate guidance from the IT Department on IT configuration management and security was not apparent at several courts where we had conducted IT audits over the past year. In addition, within the IT Department and at the courts that had been audited, there were no risk assessments performed on the IT environment to identify risks and vulnerabilities. Further, the individual courts did not have documented IT policies and procedures to guide the IT functions they performed.

While the IT Department had a defined organizational structure and established IT operational procedures and provided operational support for automated systems, the department lacked adequate strategic and tactical planning, documented policies, and mechanisms to provide assurance that controls were working as intended. There was little coordinated effort with the Project Management Office (PMO) leaving the IT Department to be generally unaware of the specifics of the PMO's MassCourts Project.

Auditee's Response of Recent Improvement and Corrective Action Taken

The Information Technology (IT) Department Director and/or his designee attend all Project Office (PO) meetings. Support desk personnel have attended some training and are utilized on-site the day of any implementation to further learn and provide user support. Information Technology staff have also been readily available for any PO inquiry or support.

Overall, IT organization and management controls needed to be strengthened to provide the AOTC and the courts with a well-documented internal control framework for IT functions and activities. We found that management practices and controls at the time of the audit did not provide a sufficient foundation to meet IT governance objectives. Implementation of an IT governance framework would have helped ensure that IT strategies and initiatives were in line with overall organizational strategies, that an appropriate framework of controls was in effect over IT, and that IT resources were properly accounted for, safeguarded, and used in an effective, efficient and responsible manner. From an enterprise-based perspective, the AOTC and the Trial Court lacked an adequately defined and cohesive organizational structure of cross-entity reporting lines and clear points of accountability for IT functions and activities performed throughout the courts.

Auditee's Response of Recent Improvement and Corrective Action Taken

Various policies have been published, addressing the areas of management control and resource utilization. The need for any further policies is being investigated and those policies will be developed when identified.

a. Information Technology Strategic Planning

The results of our audit indicated that the IT Department had not developed comprehensive strategic or tactical plans to address IT functions within the department or across the courts. We observed that the IT Department had a rudimentary IT-related short-term plan, but that it lacked sufficient detail regarding assignments, priorities, milestones, or performance metrics. Our observation of the PMO's strategic plan was that it appeared to be well organized and detailed. However, from an enterprise-based perspective, there was no overall IT strategic plan covering all IT functions and projects. We found that management control practices needed to be strengthened to ensure that IT strategic planning for the IT Department be sufficiently defined and aligned with overall IT strategies to support the Trial Court's operations and business objectives.

Auditee's Response of Recent Improvement and Corrective Action Taken

Policies have been developed addressing IT service delivery and the users expectations of that, to include service levels. The need for any further policies is being investigated and they will be developed when identified.

Although the IT Department had developed a mission statement outlining its overall purpose and key duties, the statement needed to be enhanced to adequately identify the department's role in supporting enterprise-based management of IT across all courts. The latter would include establishing appropriate IT-related policies and guidelines, setting strategic direction for IT functions and configuration management, and providing oversight of IT activities.

Auditee's Response of Recent Improvement and Corrective Action Taken

Several policies have been developed that address the management of IT across all courts and several other initiatives are actively being pursued which will further address this area.

As the primary IT provider within the Trial Court, the IT Department performed important functions ranging from Help Desk support to operating application systems and managing network security. The result of not having the IT Department subject to an IT strategic planning process was the absence of a documented strategic plan and tactical plans for the department's functions. While it is understandable that the key focus regarding technology was the efforts of the PMO, the management of the IT Department was somewhat handicapped by not being subject to a strategic planning process and relevant project management techniques. It was apparent based on our interviews and observations that there were no clear directives for the IT Department to develop a documented IT strategic plan, or detailed tactical plans. The absence of an IT steering committee over the IT Department may have contributed to the lack of IT strategic and tactical plans not being identified and highlighted to senior management.

Strategic planning is an essential process to assist an organization in setting direction and appropriate courses of action to meet its mission and business objectives. The more that IT strategic planning can be integrated in the Trial Court's overall strategic planning process, the more likely that the management and use of IT resources will become a key enabler of operational processes to support the Trial Court's business objectives. A comprehensive strategic planning process should incorporate a formal, organizational-tailored approach to developing and managing automated application systems, whether the systems are acquired or internally developed. The planning process should also address IT configuration management for all IT resources, including the computer systems and networks supporting the application systems. Effective IT strategic planning should help direct the AOTC's and the IT Department's actions and incorporate milestone and performance measurements to be used as effective management tools. Performance measures provide management with qualitative and metric-based feedback against which the progress of strategic initiatives and IT operations can be evaluated. The IT Department would benefit from having performance metrics gradually applied to its functions and service areas.

An IT strategic plan should include the following components:

- Statement of organizational mission and primary business objectives identifying the linkage of the IT strategic plan to the overall enterprise strategic plan(s).
- Summary of the organizational strategic plan goals and strategies enabled by IT and supported by IT functions.
- Statement of critical success factors for IT and the IT Department. Statement of IT requirements to adequately support the enterprise's business objectives. It is important that the IT strategic plan reflects and supports long and short-term plans.
- Statement on how each IT goal and strategy will support organizational goals and strategies.

- Detailed information on the organization's current IT infrastructure (inventory of current IT resources and IT capabilities, including hardware, software, communications, personnel, capacity and utilization, strengths and weaknesses, and associated risks).
- Definition of information architecture model that addresses the information requirements of the organization. The information architecture model should be cross-referenced to the established data classification scheme with respect to data sensitivity and privacy requirements.
- Statement on technological direction taking into account technology standards, current technology base, operational and fiscal strengths and limitations, and any acquisition or system development plans.
- Statement on capabilities of IT and non-IT personnel responsible for performing IT-related tasks and activities and plans on staff development regarding skills and knowledge.
- Forecast of internal and external developments that could impact the IT strategic plan.
- Statements of technological solutions taking into account the organization and business processes, re-engineering opportunities, control objectives and preferred control practices, personnel requirements, and performance indicators.
- Acquisition and development schedules for the IT environment.
- Statement on operational, administrative, and quality service issues related to the organization's targeted IT environment, taking into account recommended policies and procedures.

The lack of a comprehensive strategic planning process that incorporates all IT functions places at risk the IT Department's and the PMO's ability to successfully address management's business objectives and user expectations through future system development projects and IT-related acquisitions. Without comprehensive strategic planning, the analysis and development processes may vary substantially among projects, potentially resulting in information systems that may be inefficient, incompatible, or have cost overruns on development or system maintenance. With respect to costs, the planning process should require identification of total cost ownership so that more comprehensive business case analysis can be performed for each development or acquisition project. It is important that the strategic planning initiated by the PMO be expanded to include the IT Department in a more comprehensive IT planning process. The strategic planning process should require that IT strategic and tactical plans be updated to reflect accomplishments, changes, and new initiatives. Having detailed, enterprise-wide IT strategic and tactical plans for the Trial Court is critical to the success of the MassCourts Project.

Regarding user department input in the development of IT-related planning and resource allocation, our audit determined that the IT Department had not established adequate channels for user input nor provided guidance for IT-related activities within the courts. At the time of our audit, working relationships between the IT Department and its user community were in need of being established or strengthened. While user input had been initially solicited for the PMO's MassCourts strategic plan,

mechanisms to solicit user input from an enterprise-based perspective had not been sufficiently established.

Auditee's Response of Recent Improvement and Corrective Action Taken

The gap between the IT department and user community has been greatly reduced through active Director involvement, querying of the user community, and periodic informative web postings and mailings. Also a policy and process were put in place for the user community to formally address any IT support issue. This process includes IT Director review, staff input, and follow-up.

Based on our interviews, it appeared that the IT Department's understanding of user requirements was more heavily driven on those issues brought to the department's attention by the users. Our observations, and through audits conducted at individual courts, indicated that users would not always request assistance or seek advice from the IT Department. In some cases, the level of satisfaction with the IT Department was quite low. It was also apparent that not all courts had a good understanding of their responsibilities regarding IT-related tasks and activities or clearly understood the role of the IT Department.

Benchmarking at the time of our audit against generally accepted management control practices, such as those outlined in the CobiT control model, we identified that key elements of an IT strategic planning process were not sufficiently in place. For example, the IT Department's tactical plans needed to be driven more from enterprise-based strategic plans taking into account all IT functions and initiatives rather than from a primarily MassCourts-based approach. At the beginning of our audit, documentary evidence of the level of sharing of planning-related information between the PMO and the IT Department was almost non-existent. The IT Department did not have readily available IT strategic planning documents that clearly indicated technological direction and specific planning activities between the PMO and itself. During our audit, we observed an increase in communication between the PMO and the IT Department. However, by the end of our audit, the IT Department still lacked a detailed understanding of the strategic and tactical direction being taken by the PMO. From a documentation standpoint, formal notes or minutes of IT Department meetings regarding strategic issues were generally not maintained. There was also evidence that the IT Department's efforts were driven by short-term demands placed on the department by the PMO and in meeting technical operational requirements. Input from the PMO to the IT Department appeared to be almost exclusively a combination of verbal communication, e-mails and memos reflecting a somewhat informal process. Furthermore, an extensive gap analysis had to be undertaken subsequent to the signing of the MassCourts contract to reconcile variances between the original RFR and the approved contract.

The strategic planning documents provided during the course of our audit did not clearly specify IT configuration requirements for the Trial Court and the MassCourts Project. For example, the MassCourts Project documents did not address business continuity planning or clearly identify the degree to which imaging and scanning systems would be used to reduce or backup hardcopy files at the courts for case management purposes. Given the importance of the MassCourts Project, it seemed counterproductive that the more extensive documentation available within the PMO was apparently not shared with the IT Department in a timely manner. From an operational perspective, short-term requirements placed on the IT Department by the PMO were not always requested with sufficient time to allow for an IT Department's assessment and valued input or feedback into the overall process.

Auditee's Response of Recent Improvement and Corrective Action Taken

The Information Technology (IT) Department Director and/or their designee attend all Project Office (PO) meetings. Support desk personnel have attended some training and are utilized on-site the day of any implementation to further learn and provide user support. Information Technology staff personnel have also been readily available for any PO inquiry or support.

At the beginning of our audit, the IT Department did not have readily available detailed results of assessments of existing systems. Essentially, very little written documentation regarding IT assessments was in place during fiscal year 2003. Although the drawbacks of the current IT systems across the Trial Court were well known, the IT Department lacked an inclusive IT strategic plan that covered all IT initiatives, projects and IT functions with an integrated and coordinated approach considering risk assessment results. In summary, our examination indicated that IT configuration management (strong inventory control, status accounting of all IT resources, assessments of IT resource capabilities, and database management) had not been a traditional priority of the IT Department.

We feel that the MassCourts Project provides an opportunity for increased communication and coordination between the AOTC and its IT user community by having court management and the Trial Court user community involved in the Project's planning and implementation. These efforts should help ensure that IT is used as a key enabler to be aligned with the Trial Court's mission and business strategies increasing the potential for a successful rollout of the entire MassCourts Project.

b. Information Technology Policies and Procedures

Our examination indicated that adequate IT policies and procedures were not in place to provide statements of required action and guidance within the IT Department and for guidance across the courts. Our evaluation of IT internal controls and related documentation at the beginning of our audit revealed that although the AOTC had certain control procedures in place, a set of formal IT policies had not been

documented or included in an internal control plan for IT functions. The absence of appropriate documented IT-related policies failed to establish a key element for a framework of controls and did not adequately set management direction. Documented policies and procedures also specify appropriate tasks and activities to be performed to mitigate risk. Our audit interviews with AOTC management confirmed that they were well aware of the absence of IT policies for the IT Department and the individual courts. We acknowledge that there had been limited efforts to develop policies and standard practices, but that these were not driven by strategic initiatives and risk analysis. The absence of a clearly-defined and workable process to develop, promulgate, and ensure adequate understanding and compliance with IT policies, standards and procedures significantly inhibited the issuance and implementation of appropriate IT-related policies and standard procedures.

Auditee's Response of Recent Improvement and Corrective Action Taken

A variety of policies have been published and the need for any further policies is being investigated and those policies will be developed when identified.

It is our understanding that subsequent to our fieldwork and summary discussions with AOTC management, a concentrated effort by the IT Department has been underway to develop IT-related policies. The fundamentals of internal control described below should be considered in these efforts.

Risk Assessment

Our audit revealed that there was little or no evidence that the AOTC's IT Department or the Trial Court performed risk assessments of IT operations or the IT environment. At the time of our audit, the AOTC did not have a systematic approach to risk identification for IT functions or an established risk management function in place. While risk assessments may have been performed on other operational areas within the AOTC or the Trial Court, a framework for conducting IT-related risk assessments was not in place. In that regard, policies, procedures and defined responsibilities pertaining to IT-related risk assessment had not been established. Although the AOTC's Internal Control Guidelines state that risk assessment should be periodically performed, management had not encouraged staff to use risk assessment as a tool to provide information for the design and implementation of IT-related internal controls, monitoring and evaluation mechanisms, or IT strategic planning.

The results of performing risk assessment assist management in meeting their responsibility to establish an internal control framework by identifying vulnerabilities and undesired events to be prevented or detected and corrected. By having risk assessment provide focused information on the nature and magnitude of potential risks, the organization is able to better ensure that a sufficiently comprehensive system of internal control is in place. In the absence of an established, systematic risk assessment framework, it is extremely difficult for management to identify all relevant risks and attain a

sufficient understanding of the level of residual risk associated with operational and control objectives. In turn, that increases the probability that management will be unable to meet its responsibility for providing an appropriate framework or system of internal control. The absence of conducting risk assessment, or risk analysis, limits the IT Department's ability to make necessary changes to IT-related internal controls that impact the department's or the Trial Court's IT functions. The failure to sufficiently identify inherent risk and control risk often delays organizations from making necessary changes to their internal control framework and control practices, thereby increasing the residual risk that operational and control objectives will not be met.

A systematic risk assessment framework should incorporate regular assessments of relevant IT risks and vulnerabilities to the achievement of business objectives. This information would help form a basis for determining how the risks should be managed or mitigated to an acceptable level. A coordinated effort should be made to ensure that IT-related risk assessment is part of the risk assessments performed on other operational areas for which those operations or business processes are enabled by technology.

The essential elements of risk assessment include the identification of business objectives and associated business processes, critical success factors, tangible and intangible assets, asset valuation, threats, vulnerabilities, stated controls and safeguards, and the likelihood and impact of potential risks and threats. Accordingly, the risk assessment process should consider business, legal, regulatory, technology, and human resource risks. The process should require that risk assessments be performed at the enterprise level and the business process and system-specific level for on-going functions and activities as well as new strategic initiatives and projects. The process of conducting IT-related risk assessments should solicit input from management, internal and external users, the IT Department, and Internal Audit.

Because IT-related vulnerability assessments were not conducted, it is likely that information for managing risk had not been identified or brought to management's attention. Given that the Trial Court is moving toward web-enabled enterprise-based systems, the role of vulnerability assessment increases significantly. In that regard, vulnerability assessment becomes an important tool for network and application security, network management, and system availability. Security specialists, along with management, process owners and Internal Audit, should be involved in the identification and assessment of the vulnerabilities and the development of risk mitigation solutions.

The lack of adequate risk assessment inhibits the AOTC and the IT Department from providing reasonable assurance that its mission and goals will be accomplished and that IT assets will be adequately safeguarded and used effectively and efficiently within the AOTC and the Trial Court. Not conducting IT-related risk assessments nor having a risk management function in place limits the ability to adequately address internal control and ensure an overall coordinated strategy to mitigate risk within the Trial Court's IT environment.

Documentation

Although the AOTC did have certain IT-related control procedures, there was a significant lack of documented IT-related policies or procedures. At the time of our audit, the AOTC did not have sufficiently-developed or documented IT policies and procedures for IT-related organization and management, IT strategic and tactical planning, system access security, physical security and environmental protection over IT resources, hardware and software inventory, IT configuration management, implementation and use of IT resources, provision of IT services, program change control, contracted services, quality assurance and improvement, disaster recovery and business continuity planning, and on-site and off-site storage of back-up copies of magnetic media.

Auditee's Response of Recent Improvement and Corrective Action Taken

The Deputy Directors, through line management, have been documenting department processes and continue to identify additional areas where documentation may be needed. Additional policies are being identified and development will be ongoing by the IT Director.

Documentation is a fundamental requirement for a system of internal control. In that regard, documentation should include policies and standards to outline the "rules of the road", procedures to describe how to perform tasks and activities, written descriptions of business processes and systems, and systems of record. Understandably, the latter would include records of business events captured to transaction files (or stores) and updated to master files (or stores), suspense files, tickler files and appropriate management and audit trails.

While recognized as a management responsibility, neither AOTC, nor the IT Department, had taken on the task of developing, documenting, and promulgating policies and procedures relating to IT functions at the AOTC or across the Trial Court. Documented IT policies and procedures are essential to ensure that an organization's roles and responsibilities are defined, communicated, and aligned with management objectives. Documented IT policies and procedures also facilitate effective direction and adequate control.

Auditee's Response of Recent Improvement and Corrective Action Taken

When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their respective court or office and post it. The policies are also posted on the Trial Court web site.

The lack of formally-documented policies and procedures limits management's ability to provide guidance and oversight for IT activities at both the AOTC and across the Trial Court. In addition, a significant portion of the IT Department's knowledge base of IT functions and activities could be lost

should key personnel terminate employment. Documentation of policies and procedures also preserves historical knowledge and enhancements made over time of IT functions and activities. Documentation of key processes and activities within an IT function helps to provide clear guidelines regarding the exercise of control practices and monitoring and evaluation of expected results. Documented policies and procedures should address all IT functions including IT planning, risk assessment, risk management, defining information architectures, data ownership, security, virus protection, authorized use of IT resources, training, monitoring, and reporting.

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. Formal documentation of policies and procedures also enables personnel to develop a broader understanding of their duties and improve their knowledge and level of competence.

In the absence of formal IT policies, standards, and procedures, employees may rely on individual interpretations of what is required to be performed or how to best control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result, and important control practices may not be performed as needed and key IT control objectives may be inadequately addressed. In addition, management may not be adequately assured that desired actions have, or will, be taken. Furthermore, the absence of documented IT policies and procedures undermines the ability to monitor and evaluate the performance of IT processes, computer and network operations, and application systems and to provide management with sufficient feedback and assurance. In addition to documentation being a generally accepted control practice, Massachusetts General Laws, Chapter 647, requires that all state agencies have documented and approved internal control procedures, and Chapter 211B Section 9 notes that “the chief justice for administration and management shall be responsible for the management of court personnel, facilities, administration, security, and court business and shall have the authority necessary to carry out these responsibilities including, but not limited to, the following:--(ii) the responsibility to provide planning and policy-making functions, including the implementation of such planning and policy-making decisions”; and (iii) “the responsibility to provide departments of the trial court with technical assistance concerning recordkeeping [and] auditing” Although the AOTC has made a good effort to document internal controls related to fiscal management, at the time of our audit sufficient effort had not been made to document IT-related controls that are part of the overall internal control framework.

Auditee’s Response of Recent Improvement and Corrective Action Taken

When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their respective court or office and post it. The policies are also posted on the Trial Court web site.

At the time of our audit, there was no apparent mechanism by which policies and procedures applicable to IT functions performed at the AOTC or across the Trial Court could be promulgated by the IT Department. While efforts to initiate policy development on the part of the IT Department was limited, there was little evidence of management directives placed upon the IT Department to assess the need and/or develop IT-related policies and procedures. Recognizing that the PMO was in the process of planning for the implementation of the MassCourts Project, it would be reasonable to expect that the PMO and the IT Department would have had discussions and joint initiatives regarding the development of IT-related policies and procedures. We note that subsequent to the close of our audit, the IT Department had begun an effort to develop IT policies.

Auditee's Response of Recent Improvement and Corrective Action Taken

The courts have been made aware of the policies and are empowered to enforce them, as are the IT Departments, Field Technicians and Support Desk personnel. Also an initiative is on-going, that when fully implemented, will allow the IT Department and the courts to more stringently enforce asset management and software inventory through a vendor product.

In addition to the general absence of IT-related policy and procedure development, an adequate framework was not in place to define and assign IT-related responsibilities, establish points of accountability, and enforce compliance with IT policies and procedures within the user community. Barriers to policy and standard procedure development, issuance, and enforcement may be an impediment to the success of the MassCourts Project. While the success of the MassCourts Project will depend upon many elements, critical success factors include having an appropriate framework of IT-related policies and procedures in place and understood, assigned responsibilities, points of accountability, and compliance monitoring and oversight.

To assess the adequacy and appropriateness of IT policies and procedures, the framework for policy and procedure development and implementation should include change control processes for ensuring that policies and procedures are reevaluated and updated periodically, or upon significant changes to the IT or business environment. The framework should require the review and approval of policies, standards, directives and procedures and include appropriate communication mechanisms and channels to ensure that policies and procedures are understood and accepted by all users throughout the AOTC and the Trial Court.

Auditee's Response and Corrective Action Taken

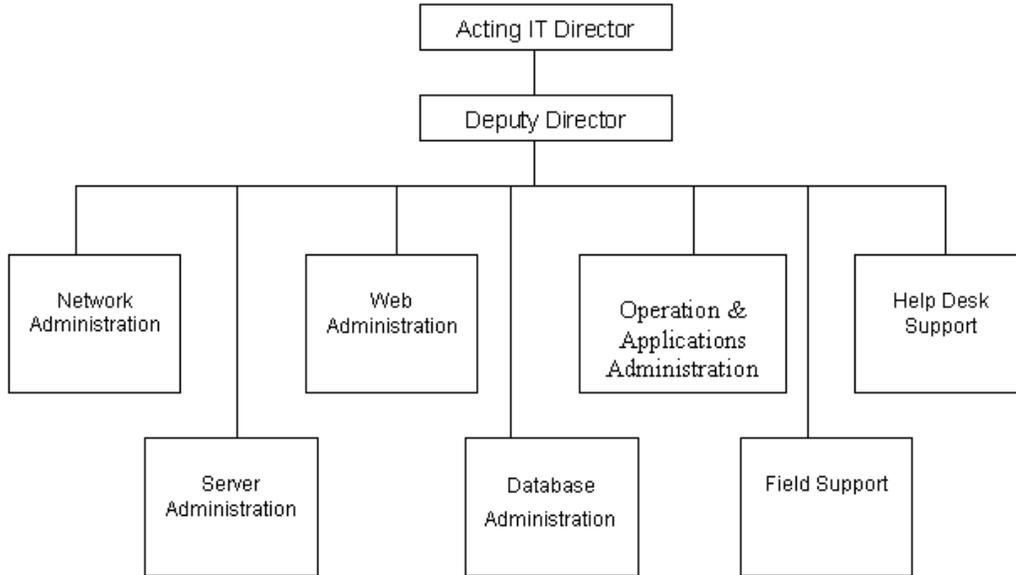
All published policies are routinely reviewed by the IT Director and staff. When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their court or office and post it. The policies are also posted on the Trial Court web site.

Management is responsible for ensuring that there are internal controls in place to provide reasonable assurance that organizational objectives will be met, and that undesired events would be prevented or detected and corrected in a timely manner. Management should also ensure that the fundamental cornerstones for an internal control structure are in place, namely stated control objectives and control practices, risk assessments, documentation, competent personnel, and monitoring and evaluation.

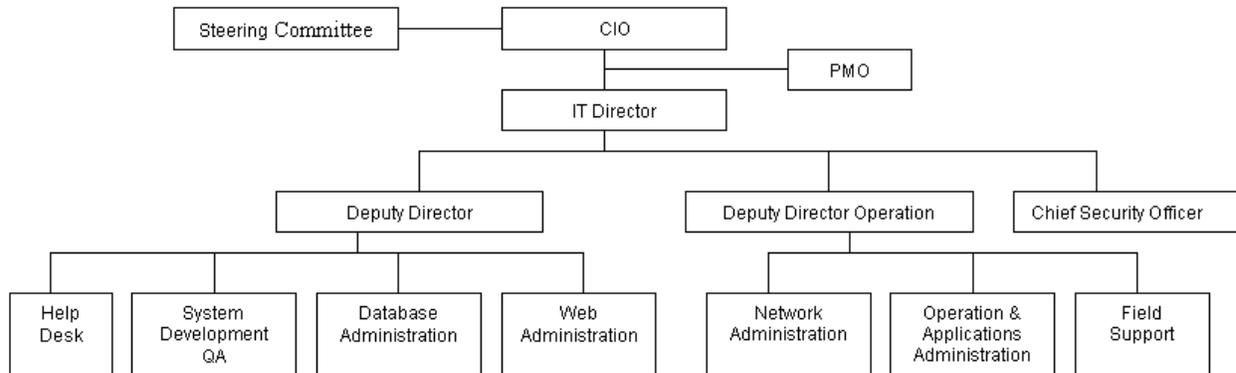
c. IT Organizational Structure and Human Resource Management

Our review of the IT Department's organizational structure indicated that positions were defined and that an established structure as reflected by a formal organization chart was in place. Our observations during the course of the audit were that IT functions and activities were performed within the framework of positions reflected by the IT Department's organizational chart. Generally, we found that IT Department job descriptions delineated roles and responsibilities and reporting lines. The organizational structure properly addressed unity of command and had an established chain of command. IT functions within the IT Department were established primarily from an operational standpoint rather than from a management control perspective. For example, there was inadequate segregation of duties regarding the help desk and access security functions. In addition, when viewing IT-related functions across the courts, not all IT-related functions come under one umbrella or report to a single point of accountability.

The organizational chart below reflects the IT Department's stated organizational structure at the time of the audit.



The following is a depiction of a potential organizational structure to improve management controls related to span of control, key IT functional areas, and the formation of a steering committee function. Although the steering committee is presented at the same level of the chief information officer (CIO), the steering committee could be placed above the CIO with the CIO’s membership included. The organization chart below may be used as a guide with refinements as needed.



From a functional perspective, the IT Department’s organizational structure did not include formal assignments for all areas of responsibility that would be generally expected of a department of similar mission and extent of IT user or customer base. For example, assignments of responsibility for risk management, customer and third-party relationships, and quality assurance and improvement were not

apparent. As the MassCourts Project moves into its implementation phase and the supporting role of the IT Department is better defined, the responsibilities for additional, or expanded, functional areas will need to be assigned and points of accountability established. In addition, from an enterprise perspective, the Trial Court would benefit from having the central IT organization establish a management and control framework for IT functions to ensure adequate communication and coordination among the IT Department, PMO and personnel performing IT functions at individual courts.

Key elements in improving the AOTC's IT organizational structure include establishing an oversight mechanism such as an IT steering committee for all IT activities, clarifying responsibility and communication lines between the PMO and IT Department, and adopting an enterprise-based organizational structure to encompass all staff within the Trial Court performing IT tasks and activities.

Regarding oversight, a formal IT steering committee was not in place to provide guidance and oversight to the IT Department. Given the scope of service areas across the courts and the importance of oversight from a governance perspective, the service activities of the IT Department lacked a key element of review and approval. Control objective requirements for organizational structure and human resource management require that a planning or steering committee be established to oversee IT functions responsible for complex projects and services across multiple departments and users.

Considering that part of the role of a steering committee is to serve in an advisory capacity, we acknowledge that the PMO had, at least, a policy advisory committee from which advice could be sought or would be provided. However, there was no well-established IT advisory and steering committee over all IT functions within the AOTC or the courts. Moreover, the lack of an IT steering committee has contributed to inadequate oversight with regard to the allocation and control of IT resources, advice in setting IT priorities, and failure to address IT internal control issues and activities.

As part of our review of the AOTC's organizational structure, we reviewed the relationship between the IT Department and the PMO. In viewing IT functions within the AOTC, there were two distinct IT organizational units; namely the IT Department and the PMO. Given the magnitude of the MassCourts Project, it is understandable that a program management office would be established to help manage the acquisition, development and implementation of the IT systems. Although we do not take exception to the establishment of the PMO, from the perspective of IT management, our concern lies with the lack of a formal relationship between the PMO and the IT Department at the time of our audit. The absence of clearly defined reporting and communication lines and a very low level of collaboration between the two organizational units reflected this. Our observations indicated that often inadequate lead times were given to the IT Department to properly review requests made by the PMO to the IT Department for either infrastructure changes or human resource needs. We also found that there was little documentation of meetings between the PMO and the IT Department. In addition, general observations indicated that

because of the established focus on the PMO and the absence of sufficient communication between the PMO and the IT Department, it appeared that the PMO exercised autonomy over the IT Department.

Auditee's Response of Recent Improvement and Corrective Action Taken

The PO and IT department have developed a very open and proactive relationship, which continues to evolve as the project evolves.

Enterprise Structure:

Although the AOTC had an established IT Department to provide IT services to the courts, efforts had not been initiated to formulate, or define, and communicate roles and responsibilities for IT-related functions and activities on an enterprise-based IT organizational structure. The overall organizational structure for the IT Department and IT-designated positions across the courts needed to address all of the IT activities and tasks performed. In that regard, IT functions across the enterprise should be aligned with the business requirements of the Trial Court to facilitate IT strategic initiatives and provide effective direction and adequate control. Prior to the implementation of MassCourts, a staffing analysis should be conducted to identify staffing requirements to support IT functions including activities performed by the IT Department and court-based personnel.

Our observation during the audit, and at other IT audits performed at separate courts over the audit period, was that there were staff within the courts who performed various IT-related functions. The tasks and activities ranged from general IT-related instruction to granting access privileges to automated systems. It appeared that these individuals may have been assigned IT responsibilities on the basis of their technical skills and knowledge in order to assist their courts by filling the void of the court not having designated IT personnel. This represented a short-term solution to a long-term problem regarding IT support and staffing.

Based upon our IT audits that were conducted at individual courts, it appeared that senior management had not implemented adequate supervisory practices for IT functions across the Trial Court to ensure that IT-related roles and responsibilities were properly exercised. In addition, management should ensure that staff having IT-related responsibilities had sufficient authority and resources to carry out those responsibilities and that there was adequate management reporting. Further, efforts needed to be made to ensure that key performance indicators and metrics are established. Because IT functions and activities will be required to a greater extent across the entire Trial Court with the MassCourts implementation, roles and responsibilities of personnel performing IT-related functions across the enterprise must be defined, communicated and understood.

As the use of systems and technology increases across the courts, IT responsibilities within the IT Department and for court-based personnel will need to be better defined and assigned. For example, the

IT Department, reflecting a service provider perspective, would include systems support and availability, custodial responsibility for data, access security administration, and network management. The user community responsibilities would include data integrity, source document protection, and shared responsibility regarding security and business continuity planning.

Generally accepted control practices indicate the need to have a single point of responsibility for logical access security and physical security of IT resources. Security over IT resources, including the computer equipment, application systems, and data files requires a coordinated physical and logical security strategy. However, at the time of our audit, there was no single point of accountability for physical and logical security at AOTC and there appeared to be little communication or coordinated effort between the parties responsible for these two areas of responsibility.

To deliver appropriate IT services, the IT organization and IT-related staff within the Trial Court must satisfy certain business requirements. For a defined and cohesive organizational structure to support IT functions, management should consider:

- Management's direction and supervision of IT functions
- IT's alignment with the business needs of the enterprise
- Clear roles and responsibilities (job and position descriptions)
- Segregation of duties
- Staffing levels
- Identification of key personnel and cross training
- Organizational positioning of security, quality assurance, and internal control functions
- Unity of command
- Span of management
- Defined points of accountability
- Reporting lines
- Centralization/decentralization considerations
- Oversight and monitoring and evaluation requirements

In placing the IT function in the overall organizational structure, senior management should ensure an adequate level of authority and independence from user departments to guarantee effective IT solution development and deployment, and to establish open lines of communication with top management to help increase awareness, understanding, and skills required for identifying and resolving IT issues.

We noted the following during our audit:

- The IT organizational structure throughout the Trial Court had not been formally evaluated.
- The IT-related responsibilities and support functions at the individual courts were not adequately defined and responsibilities and job functions were not clearly delineated.
- Security administration (system access security) was managed and performed by the IT Department's Help Desk. Security functions should be segregated from standard IT operations.

Regarding human resource management, we observed that management had not established and maintained procedures for identifying and documenting the training needs of all personnel and that performance evaluations were not performed in the IT Department or on IT liaison personnel within the Trial Court. To ensure sound human resource management, control over the IT process of managing human resources must take into account the business requirement of acquiring and maintaining a motivated and competent workforce and maximizing personnel contributions through sound, fair and transparent personnel management practices to recruit, train, evaluate, compensate, promote and dismiss staff. The following factors should be considered with regard to IT personnel management:

- Training and qualification requirements
- Security and control awareness development
- Cross-training and job rotation
- Objective and measurable performance evaluation
- Balancing internal and external resources
- Succession plan for key positions
- Identifying the need and extent for IT contract services
- Orientation training for new hires to the courts including training on their IT-related roles and responsibilities and, to the degree necessary, access to related IT policies and user procedures

AOTC management should ensure that personnel are performing only those duties stipulated for their respective jobs and positions and IT management should regularly verify that personnel performing specific IT tasks are qualified on the basis of appropriate education, training and/or experience, as required. Senior management should also implement a division of roles and responsibilities, excluding the possibility for a single individual to subvert a critical process. In particular, segregation of duties should be maintained between the following functions:

- Information systems use
- Data entry/computer operation
- Network management
- System administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit and quality assurance

d. Monitoring and Assurance

AOTC had not established adequate monitoring and evaluation policies, procedures and functions to determine whether controls were in effect and that control objectives for IT processes and activities would be met. The absence of adequate mechanisms to provide management with assurance that controls were in place and in effect undermines the internal control structure for IT and the business processes

supported by technology. Assurance mechanisms for the management of IT, including control self-assessment, quality assurance, and an increased Internal Audit role, were needed within the IT Department and across the entire Trial Court.

The effectiveness of internal controls should be monitored in the normal course of operations through management and supervisory activities, comparisons, reconciliation and other evaluation procedures. Deviations should be documented and evoke analysis and corrective action. Serious deviations and failures to take corrective action on material control deficiencies should be reported to senior management. For effective monitoring of IT activities and internal control processes, management should ensure that relevant performance indicators or benchmarks are in place and that data is being collected to create management information and exception reports to be measured against desired performance targets.

AOTC management had not established a quality assurance function designating the IT Department the responsibility for performing quality assurance activities. In addition, AOTC had not defined, documented and maintained a quality approach with policies and objectives consistent with the AOTC and Trial Court philosophies. As a result, an IT-related quality philosophy had not been implemented for IT functions and a quality assurance mechanism was not in place to review and monitor against established standard policies and procedures. Management should ensure that IT Department personnel performing quality assurance functions have appropriate expertise in system development, programming, quality assurance, application systems, controls, and IT communication. Management should also establish a standard approach regarding quality assurance covering both general and project-specific quality assurance activities. The approach should prescribe the types of quality assurance activities (such as reviews and examinations) to be performed to achieve the objectives of a general quality plan. The plan should identify quality standards and require specific quality assurance reviews.

The combined organizational placement of the IT Department and decentralized IT functions along with the responsibilities and size of the quality assurance group should be established to satisfy the requirements of the overall enterprise. Quality assurance staff should be suitable in numbers and skills with roles and responsibilities that are defined, communicated, and aligned with enterprise-based business objectives. Management should consider the need to communicate IT-related quality objectives to the user community to help provide feedback on IT systems and services and to ensure adequate awareness of quality standards and user rules to be applied within the IT environment.

At the time of our audit, the AOTC's Internal Audit Department had not been required to evaluate the controls or performance of IT operations and functions performed by the IT Department, PMO or by individual courts. In addition, we found that the Internal Audit Department of the AOTC was under the control of the Fiscal Services Director posing the question of adequate independence and whether the department is placed at a high enough level within the overall organizational structure.

Our conclusions, based on our audit work, were that routine monitoring and testing of the AOTC's system of IT internal controls did not occur. In addition, our audit revealed that IT documented policies and procedures did not always exist or were limited in content, and that the AOTC's internal control guidelines did not adequately address IT control objectives and controls. As a result, without monitoring and evaluation activities such as control self-assessment, quality assurance, and internal auditing, AOTC management cannot be assured that appropriate management control practices for IT functions have been implemented and consistently applied.

During our audit, we noted that the Trial Court's Internal Control Guidelines stated that individual courts were responsible to establish internal controls and that the responsibility for policy and control procedures was placed at the individual court level. This approach works at cross purposes for enterprise-based management and control for those tasks and activities that should be subject to standard policies and procedures. Importantly, to ensure consistency, established IT standards should be applied to the AOTC and the Trial Court under a single high-level control framework.

e. Relationship Management

Based on interviews during the AOTC audit and input from auditees from other court audits, it was apparent that the IT Department had not cultivated an adequate working relationship with the user community throughout the Trial Court system. Although there was limited communication between the courts and the IT Department, there appeared to be a general lack of understanding on the part of most courts of appropriate IT policies and procedures, or generally accepted IT practices, and IT initiatives. There was also no formal established relationship among personnel responsible for physical security, system access security, and IT configuration management and fixed-asset accounting.

Auditee's Response of Recent Improvement and Corrective Action Taken

When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their court or office and post it. The policies are also posted on the Trial Court web site. Also a periodic web posting, by the Director, aids in informing the user community on initiatives that are being undertaken by the IT department.

One of the cornerstones for the success of an IT department is to build and manage a working relationship with its user, or client base. Inadequate communication between the IT Department and all courts has contributed to a lack of understanding on the part of users with respect to their own responsibilities regarding automated systems and IT resources. Based upon IT audits performed at individual courts during and prior to this audit, users appeared to be generally dissatisfied with the services provided by the IT Department. Although there appeared to have been some improvement over

our audit period, further effort is needed to strengthen the relationship between the IT Department and the user community. We note that at the beginning of our audit, the IT Department was at a somewhat negative position regarding its relationship with some individual courts.

Auditee's Response of Recent Improvement and Corrective Action Taken

A policy and process are in place that allows for the user community to provide formal input into the quality of services received. This process includes staff involvement and user follow-up. Also the Director has readily broadcasted his openness to directly receiving telephone calls or emails. All of which are responded to.

The IT Department's management should undertake the necessary actions to establish and maintain optimal coordination and communication and a liaison structure between the IT function and other parties of interest inside and outside the IT function throughout the Trial Court system (i.e., users, suppliers, security officers, and risk managers).

Recommendation:

1. IT Organization and Management

We recommend that AOTC management through its IT Department develop a comprehensive framework for establishing, maintaining and monitoring IT internal controls. We view these recommendations as extremely critical to help ensure the success of the MassCourts project.

AOTC should formalize an organizational structure, define IT roles and responsibilities, and establish an IT steering committee for IT operations and IT-related functions. The primary function of the IT steering committee should be to oversee the allocation and control of IT resources, advise in setting IT priorities, review IT activities, and approve IT strategic and tactical plans. Senior management, in conjunction with the IT Department, PMO and the IT steering committee, should establish an IT strategic planning framework and then define an enterprise-based IT strategic plan and an IT strategic plan for the IT Department. Operational, or tactical, plans should be developed based on the approved strategic plans. Importantly, the IT strategic plan needs to be aligned with overall strategic initiatives and responsibilities for the Trial Court.

Prior to developing or changing the IT Department's IT strategic plan, the Director of the IT Department should assess the existing information systems in terms of the degree to which the systems support the AOTC's and the Trial Court's business requirements. The assessment of existing systems should include user satisfaction, risk assessment, the degree of business automation, and the functionality, stability, complexity, cost, and strengths and weaknesses of the systems.

Auditee's Response of Recent Improvement and Corrective Action Taken

An initial Business Impact Analysis was completed by the IT Department and several initiatives are underway that address these issues and other opportunities are being investigated as to their applicability.

We recommend that the AOTC's project management framework be extended to IT Department projects and that a statement be required defining the nature and scope of every project to be clearly documented before work on the project begins. The statement should include defined measurables and milestones for each phase of the project that would be reviewed and approved by designated managers before the next phase of the project is initiated.

The AOTC should establish control procedures for the processing of data to ensure that an adequate level of separation of duties is maintained and that work performed is routinely verified. The control procedures should cover transaction processing from the point of origination through the processing of the data to output to help ensure data integrity. Established controls would require that audit trails be provided to facilitate researching and tracing of transaction processing and the reconciliation of output.

We recommend that AOTC establish a process by which IT-related policies and standard procedures can be developed and promulgated for IT functions performed by the IT Department, personnel across the Trial Court, and by third-party entities. The process should include benchmarking to generally accepted management control practices and input from risk assessments, relevant expert review, and an appropriate exposure process.

Auditee's Response of Recent Improvement and Corrective Action Taken

Policies that have been developed and published to the courts have been well received and relevant. Any additional policies are either under development or being investigated.

The AOTC's IT Department should reassess the adequacy of standard procedures for IT operations, including network operations, to identify required changes in light of the MassCourts Project. Standard procedures for computer and network operations should be reviewed periodically by management to ensure overall effectiveness and adherence to standards and control practices. For example, control practices should ensure that sufficient chronological information is recorded in operations logs to enable timely analysis, reconstruction, and examination of processing and other activities surrounding or supporting processing activities. For remote operations, such as connectivity to an individual court, specific procedures should ensure that communication links to the remote sites be defined, secured, and monitored.

We recommend that the AOTC assess the extent to which its IT-related policies and procedures provide sufficient formal guidance for IT-related tasks and activities. The AOTC needs to strengthen its current planning process to incorporate IT strategic planning such that IT strategic plans are developed by

the IT Department in conjunction with the PMO and other relevant parties. The IT strategic plans should be linked to and support the overall strategic plan for the AOTC at large and serve as a foundation for developing IT tactical or operational plans. Both the strategic and tactical plans should identify objectives and deliverables for internal and vendor-provided services. Senior management, in conjunction with the IT Department and the IT steering committee, should define an IT strategic plan by identifying IT initiatives required to support business objectives. Prior to developing or changing the enterprise-based IT strategic plan, an assessment should be performed as to the degree to which existing information systems and newly-implemented software support the AOTC's and Trial Court's business requirements.

We recommend that the AOTC, in conjunction with the IT Department and the PMO, perform a knowledge and skill assessment at all staff levels to address competency and skill requirements for current and future IT and IT-related initiatives.

a. **IT Strategic Planning**

We recommend that AOTC management establish an IT strategic planning framework that specifies the roles of the IT Department, PMO, and user community to develop IT strategic and tactical plans. Importantly, an enterprise-based vision for IT should be defined that serves as a framework for IT initiatives, policies, standards, and guidelines.

We recommend that AOTC management:

- Develop an enterprise-based IT strategic plan that incorporates the MassCourts Project and all other IT initiatives and functions. The plan should also include strategic initiatives of the IT Department.
- Incorporate project management techniques, risk assessment, performance measurement, and assurance mechanisms into the strategic planning process to provide feedback and to assure that management control practices are operating as intended.
- Establish a baseline for the IT platforms, networks, and integrated systems while the MassCourts Project is being implemented.
- Conduct performance, risk, and control assessments of IT systems and the operational and IT processing environments on a regular basis.
- Develop strategic planning control mechanisms over all IT processes to determine whether technological direction will satisfy the business requirement of taking advantage of available and emerging technology offered through MassCourts Project.
- Create and maintain a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.

We recommend that the IT Department:

- Enhance its mission statement to support and provide oversight for enterprise-based management of IT within the Trial Court. The mission statement should identify all services provided to address the Department's primary business objectives.
- Formalize the process of developing and maintaining IT strategic and tactical plans adopting a structured format and content requirements for the plans.
- Develop a strategic plan to address all IT initiatives, projects, and IT functions including access security, data center operations, network administration and security, inventory control and IT configuration management.
- Develop documented IT tactical plans, based on IT strategic plans, that identify IT Department tasks and activities and joint initiatives with the PMO and other entities.
- Create and regularly update a technological infrastructure plan that is in accordance with the enterprise-based IT strategic plan. The technological infrastructure plan should encompass aspects such as systems architecture, technological direction, and, as required, data conversion and migration strategies.

Auditee's Response of Recent Improvement and Corrective Action Taken

A draft IT mission statement is under review. The focus is to better tie IT services to business objectives.

b. IT Policies and Procedures

We recommend that AOTC management:

- Establish an internal control framework that provides the foundation for the AOTC and Trial Court's overall approach to security and IT internal control. We recommend that the CobiT control model be adopted as the underlying internal control framework to which IT platform and application system-specific control requirements would be linked. The framework should require identification of operational and control objectives, risk assessment, control responsibilities and accountability, monitoring and evaluation, and internal control reporting.
- Establish a mechanism by which policies and procedures applicable to IT functions within the AOTC and the Trial Court can be developed, promulgated, and implemented.
- Ensure that IT-related organizational policies are clearly communicated, understood and accepted by all levels within AOTC and the Trial Court.
- Document IT-related policies and procedures to address defined standards for IT contract staff. Management should define and implement relevant policies and procedures for controlling the activities of consultants and other contract personnel hired by the AOTC and managed through the IT Department or the PMO to ensure the integrity, security and availability of the Trial Court's IT resources and information assets.
- Ensure that appropriate procedures are in place to determine whether personnel understand and have complied with the implemented IT-related policies and procedures. Senior management should establish compliance procedures for ethical, security and internal control standards.
- Establish sufficient assurance mechanisms for operational and control practices to ensure adequate monitoring and evaluation of internal controls, including IT-related policies and procedures and management control practices to enable periodic management review to help ensure control effectiveness and adherence to control requirements.

- Ensure that appropriate resources are available for policy development and implementation and monitoring of compliance with adopted policies and procedures.
- Apply project management techniques to policy and procedure development and implementation requiring evaluation milestones and targets to support monitoring and evaluation efforts.
- Develop and communicate a policy regarding quality management.
- Ensure that IT-related policies include quality assurance and quality improvement to monitor, evaluate and strengthen IT functions and services.
- Establish IT policies that incorporate intellectual property rights covering in-house as well as contract-developed software.
- Establish a security awareness program to be implemented across the Trial Court. The program, which should be incorporated in orientation training, should identify security objectives, practices, and responsibilities so that an enterprise-based approach can be taken that incorporates generally accepted control practices.
- Enhance the current AOTC policy requiring risk assessment by providing constructive guidance and procedures on conducting IT risk assessments, reporting of results, and using the results of the risk assessment to design and enhance management control practices and detailed control procedures.
- Establish a general risk assessment approach to address IT functions and operations supported by technology. The risk assessment approach should define the scope, boundaries, and methodology to be adopted for risk assessments and delineate who will be responsible for conducting and reporting on the risk assessment results. The risk assessment approach should also identify requirements for the appropriate skill and knowledge necessary to identify risks and vulnerabilities and assess IT and business impact.
- Implement a structured approach on conducting IT-related risk assessments that incorporate the examination of the underlying elements of risk and the cause/effect relationship between them.
- Require that the analysis of risk identification and business impact be reported in narrative form and by quantitative and/or qualitative measurement of each risk and impact.
- Establish within the IT Department a risk management function that results in the generation of an IT risk action plan, comprehensive risk assessments, control reviews, and an understanding of the level of residual risk initially for high-level IT control objectives. The identification of levels of residual risk will assist business process owners and the IT Department in determining whether appropriate levels of control are in place and in effect. Furthermore, efforts to gain an improved understanding of residual risk enables one to make knowledgeable decisions regarding what level of control provides “reasonable assurance” that control objectives will be met.
- Encourage risk assessment as an important process in providing information to assist in the design and implementation of internal controls, and as input for IT strategic planning and monitoring and evaluation mechanisms.
- Conduct a risk assessment of current IT initiatives to identify potential risks and vulnerabilities. Risks and vulnerabilities should be periodically reassessed through the final implementation of major projects, such as MassCourts, to address critical and essential IT Department and PMO responsibilities.
- Require the Internal Audit Department to include within its scope of review and examination an evaluation of IT-related policy and procedure compliance.

c. **IT Organization/Management Structure**

We recommend that AOTC management:

- Establish a single point of responsibility and accountability for IT within the Trial Court.
- Modify the current IT organizational structure to establish clear lines of communication between the PMO and the IT Department.
- Establish a Chief Information Officer (CIO) function for the AOTC to enhance IT management and separate the functions of policy and standards development from IT operations.
- Have the IT Director (responsible for IT functions and operations) report to the CIO and realign the PMO to report to the CIO, possibly as a staff function.
- Establish an IT steering committee to provide oversight and general review of IT direction for the IT Department and the PMO. The IT steering committee membership should include representatives from senior management, user management in the Trial Court, and the IT Department. The committee's role and responsibilities should be documented. The committee may serve a vital liaison role on key projects between the IT organization and the user community, supplementing standard communication channels. An important role of the committee is to review the assignment of IT-related responsibilities within the user community. The committee should meet regularly, maintain documented minutes of meetings, and report to senior management.
- Establish a quality function managed within the IT Department as part of the overall assurance mechanisms to be implemented.
- Establish an access security administration function separate from the Help Desk services. Ensure that adequate resources are applied to the access security administration function to provide reasonable assurance that security-related objectives will be addressed.
- Identify and ensure there is adequate cross-training for key IT personnel performing mission-critical and important IT functions within the IT Department, PMO, and across the Trial Court.

Enterprise-based IT Organization

- Ensure that all personnel in the courts performing IT functions, including the IT liaisons, know their roles and responsibilities and follow approved IT policies and procedures, including reporting requirements of the IT Department. Ensure that court-based personnel performing IT-related tasks receive adequate supervision and training.
- Ensure that all court personnel performing IT-related tasks have sufficient authority to exercise the role and responsibility assigned to them.
- Inform personnel as to their degree of responsibility for internal control and security.
- Begin to work toward having a single point of accountability for physical and logical security. We suggest that AOTC start with joint efforts to identify vulnerabilities and assess risks of unauthorized access to and use of IT resources. The identification of risks may also lend itself toward developing or modifying existing control policies or practices.
- Ensure that security management responsibility be established at the organization-wide level to address overall security issues across the AOTC and the Trial Court.
- In conjunction with the MassCourts Project requirements, conduct an IT staffing analysis encompassing the IT Department and IT-related positions across the courts to identify required positions and IT-related responsibilities to be addressed. The analysis should

include personnel primarily responsible for non-IT functions who perform IT-related functions.

- The IT Department should define and implement relevant policies and procedures for establishing relationship management with third parties and for controlling the activities of consultants and other contract personnel to ensure the protection of the AOTC's and the Trial Court's resources and information assets.
- Regarding project management, AOTC should establish a framework of reporting requirements across the courts and for the IT Department to support IT-related function reporting (feedback to tactical and strategic plans) using an established base of performance metrics for enterprise management.
- Develop guidelines to address relationship building by using the MassCourts Project to establish a framework for building working relationships among the IT Department, PMO, and the courts.
- Establish regular user group meetings and technical outreach programs.
- Identify key IT personnel for mission-critical and important IT functions within the IT Department and the Trial Court, and ensure that adequate cross training is provided, if possible, and establish succession plans for mission-critical IT functions and positions.
- With respect to human resource management, ensure that knowledge and skill levels be periodically assessed and that management regularly verifies that personnel performing specific tasks are qualified (this is especially important for personnel performing IT-related functions within the courts) on the basis of appropriate education, training and/or experience.
- Regarding defined responsibilities, ensure that new hires sign a computer use policy agreement and understand their responsibility for information security and internal control.

d. **Monitoring and Assurance**

We recommend that AOTC management:

- Establish formal monitoring and evaluation functions for all IT operations and activities to assess the effectiveness of IT functions and determine whether internal controls are in place and working as intended to meet control and operational objectives.
- Operational security and internal control assurance should be determined and periodically reassessed. Assurance mechanisms ranging from control self-assessment to independent examinations by Internal Audit should be employed.
- Establish a standard approach regarding quality assurance which covers both general and project-specific quality assurance activities.
- Establish a framework of reporting requirements for monitoring and assurance across the courts and the IT Department. For example, quality assurance reports should be submitted to the management of business processes and within the IT organization. Consideration should be made for providing summary quality assurance reports, especially for major IT initiatives, to be also submitted to the IT steering committee.
- Develop and maintain an overall quality plan based on the organizational and IT long-range plans, incorporating a continuous improvement philosophy.
- To support monitoring and evaluation, ensure that appropriate performance indicators and metrics are defined and applied to IT functions and services to measure the results of IT-related activities and to support performance assessment.
- Define and implement IT system development and technical standards and adopt a system development life cycle (SDLC) methodology governing the process of developing, acquiring, implementing and maintaining information systems and related technology. The selected

SDLC methodology should be appropriate for the systems to be developed or acquired and the technology platforms and networks supporting them. The quality assurance function should develop appropriate review programs using the IT standards and SDLC requirements as review criteria.

- Assess user satisfaction at regular intervals regarding the adequacy of IT services provided. The user satisfaction analysis should identify the degree of importance of the service along with a performance rating.
- Review on an annual basis the system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.
- Develop programming, program documentation, and testing standards.
- Require that the quality assurance approach include a post-implementation review of information systems that have been placed in production to assess the integrity of the system and whether SDLC requirements were followed.
- Enhance Internal Audit's capabilities to conduct general and application control examinations and related IT auditing work. As noted before, Internal Audit should report at a high enough level of management within the AOTC organization to ensure independence from the areas subject to audit, such as individual courts or departments within AOTC.

e. Relationship Management

We recommend that AOTC management:

- Establish a liaison structure between the IT function (IT Department and the PMO) and various other parties of interest internal and external to the Trial Court (user community, other AOTC departments, Commonwealth's Information Technology Division, and third-party contractors and vendors).
- Identify key users, departments, and external entities where working relationships are required.
- Develop mechanisms for soliciting input and communicating IT-related information between the IT function and other entities.
- Recognize, through user groups or other means, communities of interest, such as users of particular technology or those performing certain IT activities where knowledge sharing and coordinated efforts would be of benefit.
- Adopt a formal process or mechanism to ensure user group participation for IT activities, including the rollout of new technology, training, and identification of problems with current applications or technology.
- Establish a formal exposure process requiring distribution of draft copies of policies and procedures for formal comments for a limited time frame prior to their adoption.
- Develop working relationships between those responsible for logical access security and those responsible for physical security, as well as between access security administration and network administration.

2. **System Access Security**

Our audit disclosed that adequate controls were not in place or in effect to provide reasonable assurance that only authorized users had access to AOTC and Trial Court application systems. System access security over the AOTC's network and Trial Court application systems needed to be strengthened to ensure that only authorized users have access to systems and data files and that unauthorized access is prevented or detected. Although limited control procedures were being followed by the IT Department in conjunction with individual courts to authorize and activate user privileges to automated systems, no documented or comprehensive policies and procedures regarding access security control existed at the time of our audit. We found that users, who had been authorized in a variety of ways, had their access privileges activated by the IT Department's Help Desk or by individuals with super user access privileges at a limited number of court facilities. Our audit determined that access privileges for several hundred user accounts should have been deactivated for individuals no longer employed within the courts. In addition, access security procedures needed to be strengthened regarding password administration and timely deactivation of access privileges that were no longer required or authorized.

Failure to implement adequate controls regarding system access security could result in unauthorized system access or use, or unauthorized disclosure of confidential information. If unauthorized access were gained to the automated systems or data files residing on network file servers or microcomputer workstations, an increase in the risk of unauthorized disclosure, modification, or deletion of critical and important data, such as confidential information regarding case management, warrants, or criminal history, is possible. Unless appropriate management control practices and access control mechanisms can be implemented, the potential risks in access security will increase significantly as the web-enabled MassCourts application system is installed across the Trial Court.

At the beginning of our audit, we found that very limited controls were in place regarding system access security, and security administration was not being adequately managed or monitored subsequent to the activation of user accounts. We note that staff at the IT Department's Help Desk were performing limited security administration functions. Having the Help Desk perform access security administration not only restricted the level of resources required to properly manage the security function, but also posed a segregation of duties problem by having the two life cycle functions performed by the same personnel. Part of the segregation of duties problem rests with having a help desk established to support IT functions being placed in the position to control or restrict access to IT resources.

We found that a standard mechanism or uniform process for access authorization was not in effect across the Trial Court. Although the IT Department required users to complete a "User Access Request Form", a formal process ensuring that documented authorization was submitted in a consistent manner and properly filed was not in place since the procedure was often not followed. Along with accepting the User Access Request Form, the

Help Desk appeared to accept various forms of authorizations ranging from telephone calls to E-mails and letters. We also found that control procedures were not in place to ensure that authorization documentation requirements were enforced and properly maintained. We found that once the authorization request was received, the Help Desk generated a standard password for the user. However, users, in particular at individual courts, were never required to change their passwords.

At the time of our audit, controls needed to be strengthened regarding timely deactivation of access to E-mail, BasCOT, FORECOURT and WMS. An appropriate mechanism was not in place to ensure timely notification to trigger deactivation of access privileges for users no longer needing authorized access. There were no formal written procedures in place for the Human Resources Department or the individual courts to promptly notify the appropriate IT Department personnel responsible for security administration of changes in employee status that would necessitate change or deactivation of access privileges. Such changes in employee status would include job responsibilities, departmental transfers, leaves of absence, or employment termination. To help ensure that only authorized access privileges are maintained, timely notification information of any changes in user status that would impact an individual's level of access authorization should be made to a designated security administrator. The Commonwealth of Massachusetts' Internal Control Guide for Departments that was promulgated by the Office of the State Comptroller states, in part "an employee password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility". Management should ensure that appropriate and timely actions for access security are taken regarding job changes and terminations so that internal controls and security are not impaired or adversely impacted.

Auditee's Response of Recent Improvement and Corrective Action Taken

The Human Resource Department has routinely and consistently provided the IT Department with a list of terminated employees. That list is in turn used to delete user accounts and access and to provide some basic asset management.

A review of the system access policy that was communicated to individuals within the AOTC and the Trial Court (listed on the AOTC's internal website) as part of the "Information Technology Policies and Procedures," fails to address data ownership, confidentiality of information, and the composition and use of passwords. Based on interviews and reviews with staff at various courts, we found that password policies were unavailable, and there was no evidence that passwords had been changed on a regular basis, or that generally accepted password administration and use guidelines were followed. For example, a password to the Warrant Management System could be composed of as little as of one character. Under these circumstances, the risk is greatly heightened of unauthorized access and modification or manipulation of data. Also noted on the AOTC internal website under the IT Department's Frequently Asked Questions regarding gaining access to WMS is the following: "The User ID is up to eight letters and numbers long. Most commonly, the User ID consists of the

first seven letters of the last Name and first letter of the first name. User ID's are always in lower case. The Initial password for User ID is "change1t". Regardless of the lack of appropriateness of the control, far too much information is publicly disclosed on the website, resulting in inadequate system access security controls even at the authorization and authentication phases.

Generally accepted security practices also require that appropriate preventive and detective system access security controls be in effect to provide reasonable assurance that only authorized users can gain access to systems and data files. Furthermore, such practices require that security levels in effect meet the organization's requirements to protect data and information and permit access on a need to know and need to perform basis, as authorized by the data and system owners. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data, and to limit access to system functions and data to only authorized users. Control practices should include formal procedures to authorize, activate, authenticate, and to change or deactivate access privileges when an employee's or user's status changes.

Our audit also disclosed that there was no policy in place to establish specific levels of authorization for users, and that a comprehensive user profile report or list of all AOTC and Trial Court system users could not be made available. We found that a data/information architecture model for court systems had not been developed as a basis for data management and security. The information architecture model would identify data elements and specify their information classes or security categories. Such models classify information to reflect the degree of sensitivity or privacy required. Security levels for each of the data classifications identified above a level of "no protection required" should be defined and implemented. Procedures should be in place to ensure that the information architecture model and the classification of data elements to security categories are kept up to date. The security levels should represent an appropriate set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in an enterprise-based environment should be established to address web-enabled application systems and changes in technology and the Trial Court's business environment. IT security should be managed in a manner that security measures are in line with business requirements.

Auditee's Response of Recent Improvement and Corrective Action Taken

Policies have been developed and published that address these issues and others are being identified for development.

At the beginning of the audit, we brought to the attention of the IT Department's senior management security that there were deficiencies regarding access security to automated systems. We found that there was a significant number of access privileges that had not been deactivated or deleted for a large number of individuals who were no longer employed by the courts. At that time, over one thousand unauthorized user accounts remained on the system. Our access test of the E-mail system used by the majority of court staff revealed that

on July 2, 2002 there were 6,145 active E-mail users. Based on a comparison of this list to a formal payroll list for the same period, we found that 1,046 (17%) user IDs and passwords needed to be removed from the E-mail system. The list of the 1,046 user accounts was comprised of 618 staff that were no longer employed and 428 user accounts of individuals who could not be readily identified. We noted that the courts had not employed some of the former employees for over two years. Our examination disclosed that 36% of the user accounts to the Warrant Management System were listed as being authorized, but were for former employees. Analysis of access security to other application systems revealed that 40% of BasCOT-Probate and Family Court, 27% of Civil BasCOT-District Court; and 24% of Criminal BasCOT-Boston Municipal Court authorized user accounts were for persons no longer employed by the courts. We also found that passwords had not been changed in some cases for periods ranging from five to ten years.

When we advised the IT Department that user accounts needed to be deactivated, a concentrated effort was made by the IT Department to delete user accounts of those users no longer requiring or authorized access to the Trial Court's E-mail system. A strong effort was made to identify and document all user accounts that needed to be deactivated. The IT Department indicated that they reviewed and verified the user's status before transferring users to a new E-mail system. However, by the end of our audit, no written policies or formal procedures had been implemented to remove in a timely manner users no longer authorized to gain access to the network or to the various applications. During the audit, we had recommended that user account lists be reconciled to application systems with respect to the individual user's authorized access levels.

Auditee's Response of Recent Improvement and Corrective Action Taken

User access lists were initially cleaned up, early last fall, through an audit, directed by the Director of IT and conducted by the individual courts. That data was then used by the IT department to update the Internet access lists. To date a monthly (sometimes twice a month) termination list is provided by the Human Resource Department to the IT Department. This was initiated early last fall and provides for a more timely and proactive approach to eliminating user accounts and access.

A process has been put in place that allows for a proactive approach to eliminating employee accounts and access.

Also during our examination of system access, a penetration test of E-mail at the AOTC central office revealed that access could be gained to the desktop and related files without using a logon ID or password, specifically to "my documents" and E-mail. Our test, using audit staff accounts, confirmed that an unauthorized party could read opened and saved E-mails, and by impersonating the last person to have logged on the system, new E-mail messages could be sent in their name. In addition, we determined that one could read and change the content of files saved in "my documents". According to IT Department staff, the new E-mail system had the same security flaw as the previous system. Understandably, given that information could be stored on over

5,000 workstations within the AOTC and the Trial Court, sensitive information could be viewed or altered by unauthorized personnel.

Auditee's Response of Recent Improvement and Corrective Action Taken

Several initiatives are being actively investigated to address this. One is a new desktop operating system and the other is a new way of handling email.

Our audit revealed that the PMO was working toward establishing information system architecture rules for the MassCourts application system. However, there was no documented information architecture model for the current application systems in operation. The information architecture model and information rules will be of benefit given that the MassCourts application system will depend upon database management technology, including a data dictionary, that should be subject to appropriate security and change control procedures. A general classification framework placing data in information classes (i.e., security categories) should also address the assignment of data ownership and defined access rules for the information classes. At the time of the audit, there was little evidence that the PMO or the IT Department was in the process of defining and documenting ownership and security categories for information classes under the MassCourts Project.

We found that AOTC management needed to:

- Establish a centralized access security function that incorporates appropriate control and reporting mechanisms for any decentralized security activities.
- Implement an overriding security policy that complies with the Commonwealth's Information Technology Division's enterprise security policies and that underscores that security is not a goal but a process and a means.
- Assess the need to have superuser accounts available to court personnel and having such superusers activate users to the systems. Suggest that this be significantly restricted given the risks associated with unmanaged superuser accounts.
- Assess the adequacy of access logging and analysis.
- Determine the extent to which intrusion detection and prevention technology will be used to support security objectives for web-enabled systems.
- Perform a risk assessment and incorporate the results into an IT security plan.
- Document and implement an IT security plan.
- Establish procedures for updating the IT security plan to reflect changes in the enterprise-based IT configuration.
- Establish a process whereby the impact of system change requests on IT security is assessed.
- Establish procedures for monitoring the implementation and maintenance of the IT security plan and access security function.
- Ensure that IT security policies and procedures are aligned with other IT-related policies and procedures.
- Restrict system access and use of IT resources by implementing adequate authorization, identification, and authentication mechanisms, and by linking users and IT resources with access rules.
- Implement appropriate controls to prevent and detect unauthorized access through web-enabled systems, or any other entry points in place.

- Establish framework for formally appointing and defining security responsibilities of data owners and data custodians.
- Document an approval procedure specifying the responsibilities of data or system owners responsible for granting access privileges.
- Ensure that contracts with third-party contractors and vendors include appropriate terms and conditions to address data and information security, integrity and availability.
- Establish a control process to periodically review and confirm access privileges. Periodic comparison of IT resources accessed to authorized user privileges should be made to identify any deviations in access rules or access gained.
- Document controls to ensure that the identification and access privileges of users, as well as the identity of system and data ownership, are established. This should be managed to support centralized access security administration and reaccreditation of security on a periodic basis.
- Perform security examinations and risk assessments to determine whether control practices are in effect and that residual risk is within acceptable bounds.
- Communicate a security awareness program for IT security within the Trial Court
- Consider establishing a security committee including individuals responsible for logical security, network management, system development and testing, physical security, and Internal Audit.
- Document a policy requiring that access violations and security activity are logged, reported, reviewed and appropriately escalated in a standard manner to identify and resolve incidents involving unauthorized activity.
- Establish a computer security incident reporting mechanism with capability to address security incidents. Consideration should be made for providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.
- Establish controls to protect all security-related hardware and software at all times against access and unauthorized change to maintain their integrity and availability.
- Document procedures for actions to be taken regarding malicious software, such as computer viruses, worms, or malware, and establish a framework of adequate preventive, detective and corrective control measures, and occurrence response and reporting.
- Establish patch management procedures to ensure that identified vulnerabilities are addressed in a timely manner.
- Implement strong documentation requirements for maintaining a management record regarding implementation of security strategies and security administration. For example, documentation of why access rules for IT devices are changed may prove to be extremely valuable when researching a security-related matter, or when implementing new devices.
- Establish procedures to ensure that authentication mechanisms for permitting access are reviewed periodically, or at least annually.
- Provide sufficient resources, such as enterprise security tools and appliances, to meet IT security objectives and support a viable IT security function.

Although our audit's examination of access security focused on logon ID and password administration, we believe that the Trial Court should review the security strategy for the MassCourts application system in light of

the difficulties encountered by many organizations to adequately secure web-enabled applications. In such environments, the goal of ensuring an appropriate degree of security that provides reasonable assurance that only authorized access and use of systems is permitted requires an on-going, well-directed security function with the right tools. Because none of the singular approaches (firewall, intrusion detection and prevention, or application controls) are sufficiently adequate, current strategies promote multi-layered, in-depth approaches. However, security management requirements are still significant. We encourage the AOTC to collaborate with the Commonwealth's Chief Security Officer at the Information Technology Division, and solicit external expertise, including that from the vendor providing the MassCourts application system, to assess the viability of the security strategy for the future. We also encourage the AOTC to employ, as MassCourts is implemented, multiple assurance mechanisms to test, evaluate, and verify the appropriateness and viability of security measures. The latter would include vulnerability assessments, penetration testing, risk assessment, independent and internal security assessments, metrics, as well as built-in mechanisms.

The development and maintenance of a viable security function to administer access privileges and ensure that appropriate controls are in effect to prevent and detect unauthorized access in a web-enabled processing environment requires significant effort and appropriate resources. However, given the importance of the function and the associated risks, it is an effort that must be fully addressed. Today, there is an escalating threat environment with rapid increases in the number of vulnerabilities and the exploits to take advantage of them. The viruses and worms propagated are ever more dangerous than those introduced years earlier. In that regard, the defense of installing corrective patches, or patch management, is difficult to adequately address in large and complex IT environments. Consideration should be made to determine whether practical migration strategies for pushing patches down through the IT environment could be accomplished automatically. Such approaches, while providing a degree of ease for system management of software updates, may pose some problems in testing and verifying the patches.

Looking toward intrusion detection systems, they can serve both as a detective control and a means to implement infrastructure changes. Issues that need to be resolved involve the number and use of these sensors. Understandably, one sensor in a multi-access point environment is not enough. We believe that there is merit to supplementing signature-based network intrusion detection systems with anomaly-based solutions.

The analysis, which depends on having a good understanding of how critical the systems and data are, requires identifying all possible access points and potential access methods. The security strategy needs to consider a wide range of factors such as normal user logons, allocation and use of super user or system administrator access, firewall and port management, protocol and rules change, replacing dial-in with VPN access, deployment of wireless access entry points, anti-virus protection, application-based controls, network security, threat management, encryption, and management and user commitment to security. We believe that security as

a process needs to become part of the business fabric, and that enterprise security management techniques should be applied.

The realm of security elements extends well beyond logon and password management to having intrusion detection devices automatically changing routing tables. It also extends to illegitimate use of legitimate authority. Although it is important that security responsibilities be reinforced through security awareness programs, the use of systems and the types of tasks executed by authorized users should be subject to review to identify unusual activities. Clearly, the latter requires having an understanding of what constitutes normal activity so that anomalies can be detected. In addition, security is not just about barriers; it is also about enabling users to perform their jobs and meet organizational objectives. The value of security depends on having protection of IT resources, authorized access to systems and data, operational effectiveness and efficiency, assurance mechanisms, and managing risk.

Recommendation

In order to improve system access security controls at the AOTC, we recommend that management establish an appropriate access security framework that incorporates generally accepted control practices and complies with the Commonwealth's Information Technology Division's security policies and guidelines. We recommend that AOTC:

- Document appropriate IT security policies and procedures to support enterprise-based IT security.
- Establish an IT security awareness program to communicate IT security policy to each IT user and ensure a thorough understanding of the importance of IT security. The program should also state that IT security benefits the overall organization and all employees, and that security is a responsibility of each employee. The IT security awareness program should be supported by and represent the view of management.
- Designate levels of access privileges to IT systems after confirming that the access privileges granted are appropriate to the employee's job responsibilities. The same determination should be made for personnel from third-party contractors who have been granted access to IT systems.
- Establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and deactivating user accounts to improve security and overall user account management. Regarding access security policy and procedures, ensure from an access security perspective that timely notification and action be taken to deactivate user access privileges by developing and implementing a standard electronic form to notify access security administration of changes in user or employee status requiring modification or deactivation of access privileges.
- Establish a data classification scheme with respect to sensitivity and privacy matters.
- Establish a framework for formally appointing data owners and custodians to assign security roles and responsibilities and support data management objectives. While it appears that data ownership may rest with individual courts, data ownership rules need to be clearly defined.

- Implement a standard process for granting authorized users access privileges to automated systems.
- Establish access procedures and requirements for password syntax rules, password composition, rules of use, password confidentiality, password length, frequency of changing passwords, responsibility for safeguarding passwords, authorization procedures, and notification of changes in access privileges.
- Reassess the use and control of super user accounts and develop guidelines for super user or system admin-level access.
- Establish an IT security incident reporting mechanism to address security incidents. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.
- Implement control practices to verify the authenticity of the party providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.
- Establish controls to protect all security-related hardware and software.
- Ensure that password security is maintained through appropriate administrative and user controls, such as restrictions on documenting controls, password encryption, restricted use of super user logons, prohibiting clear text transfers of logon IDs and passwords, and system controls.
- Implement adequate control procedures over cryptographic keys for selected encryption product(s) and strategy.
- Document procedures regarding the identification and corrective actions taken to address malicious software. Establish a framework of relevant preventive, detective and corrective control measures, and occurrence response and reporting.
- Ensure that virus protection measures are implemented across the enterprise to protect information systems and technology from computer viruses and related malicious software. Procedures should incorporate virus protection, detection, occurrence response and reporting.
- For connections to the Internet or other public networks, adequate firewalls and intrusion detection devices should be operative to protect against denial of services and any unauthorized access to the internal resources or system applications.
- Properly deploy security tools and software to support access security administration.

AOTC should adopt policies and procedures to 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. The policies and procedures should also address emergency access guidelines for mission-critical applications to ensure that under emergency or disaster recovery situations, only authorized access is granted. For security to be successfully implemented and maintained, the framework and intent of security must be clearly established and communicated to all appropriate parties. The key is a written security policy that serves to heighten security awareness throughout the courts.

Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between

organizations, addressing both security and compliance with relevant legislation. Management should implement procedures to ensure that all data is classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing “no protection” should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained.

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. Appropriate notification procedures of changes in user status should be in effect to ensure that access privileges are modified in a timely manner when job responsibilities or employment status changes. The security administrator should assess the impact of changes in employment responsibilities or status on the individual user’s existing level of authorization.

AOTC should also consider the use of access control software to prevent unauthorized changes and to detect or prevent unauthorized access to computer resources. Access control software can either be an inherent feature of the operating system or an add-on product that interfaces with the operating system.

Access control software generally performs the following tasks:

- Verification of the user
- Authorization of access to defined resources
- Restrictions of users to specific terminals
- Reports on unauthorized attempts to access computer resources, data or programs
- Establishes logon ID’s and user authentication
- Establishes rules for access

We recommend the appointment of a security administrator responsible to oversee user account management, including the creation and maintenance of user accounts and profiles of access privileges. The individual should ensure that appropriate logging of security and access activity is captured, analyzed and maintained to support IT security. Since passwords had not been changed in some cases for periods ranging from five to ten years, we recommend users be prompted by the automated systems to change their passwords for access to the application systems after a designated period of time. Such periods depend on security requirements, personnel changes and risks and generally range from 30 to 60 days. Access security procedures, password syntax rules, and password composition requirements should be clearly defined, properly organized and documented. Password administrative policies should advise users not to write down passwords, share passwords, or include passwords in electronic transmissions. In addition, authorization and authentication mechanisms should be standardized and reviewed periodically, or at least annually.

As AOTC is moving forward on the MassCourts Project, additional effort is needed to establish a workable information system architecture that identifies data ownership and appropriate security

categories/classification, such that all data is subject to data syntax rules and is appropriately defined.

These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly.

3. Inventory Control and IT Configuration Management

Our audit disclosed that inventory control practices over IT-related resources, including computer equipment and system and application software, needed to be strengthened to ensure that IT resources would be properly accounted for in the AOTC's system of record and that efficient and effective IT configuration management decisions could be made. The AOTC's inventory system of record for property and equipment should include all IT resources throughout AOTC and all court locations within the Trial Court. Although it is expected that each court will maintain an individual inventory record for local control, the master inventory file is to be maintained by the AOTC. The master inventory of IT resources was being maintained by the IT Department in lieu of having data on IT resources included in AOTC's fixed-assets inventory record.

Auditee's Response of Recent Improvement and Corrective Action Taken

An initiative is underway, using LANDesk, that when fully implemented will allow for the individual courts and the IT Department to more stringently address asset management.

With respect to AOTC's offices and data center, we determined that although IT resources were protected against physical security and environmental protection risks, controls over IT inventory needed to be strengthened. Moreover, with respect to IT resources across the Trial Court, the AOTC could not provide reasonable assurance that sufficient control practices were in place and in effect to properly account for and, when needed, report on IT-related resources. We found deficiencies in control practices, as evidenced by inaccurate and incomplete inventory data, to the extent that the AOTC's inventory system of record for IT resources as of May 16, 2002, valued in excess of \$17,000,000 for the AOTC and the Trial Court, lacked sufficient integrity to be relied upon. Although the IT and Fiscal Affairs departments made efforts during the audit period to collect and record inventory data regarding IT resources at all court locations, the data had not been verified by the close of our audit.

The AOTC 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." and that "The AOTC enters all newly-purchased items into the Trial Court inventory database to generate an updated inventory list against which each court office and division reconciles its previous inventory list each fiscal year." Although AOTC has overall responsibility for maintaining a master inventory file by the Fiscal Affairs Department for all fixed assets across the Trial Court, we found that the AOTC did not have an up-to-date, complete, comprehensive, and accurate master inventory list for IT-related assets at the AOTC and the Trial Court.

We determined through our audit that AOTC did not have specific policies and procedures in place regarding IT fixed-asset management requiring tagging of computer-related equipment; conducting a physical inventory and reconciliation on an annual and cyclical basis; maintaining a current, accurate and complete inventory record; and accounting for surplus property. The AOTC's documented policies and procedures regarding fixed assets did not provide guidelines for inventory control over IT resources.

Auditee's Response of Recent Improvement and Corrective Action Taken

When LANDesk is fully implemented appropriate policies and procedures will be put in place, which through its use and support by the individual courts, will allow for adequate inventory control of fixed assets.

Since AOTC's fixed-asset inventory record did not include IT resources, AOTC management indicated that the IT Department's inventory should be considered as the AOTC's system of record of IT resources. We note that during the course of our audit, a physical inventory was being conducted for IT-related assets by staff from the IT and Fiscal Affairs departments. Essentially, the overall effort of visiting the various courts and recording IT resources on hand was to establish a more up-to-date and accurate inventory. It is our understanding, as of the close of audit field work, that the effort to establish a comprehensive IT inventory had not included verification to records of purchase and surplus, or reconciliation procedures. There was no evidence available that the AOTC's system of record had been reconciled to documentation of all purchased IT equipment and software. We acknowledge the IT Department had lists of equipment recently purchased from a single vendor. We note that there was very little documentation to support prior year inventory practices or reconciliation. The IT Department had no record of completed physical inventories for prior years, nor was there any record of transferred or disposed of IT asset items. 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.

Our tests of computer hardware inventory revealed that inventory control required strengthening due to the lack of certain information or occurrences of incorrect data. For example, the physical location on the inventory lists frequently did not match physical locations of the items on the floor enterprise-wide. Our data analysis of the system of record determined that errors in identifying the proper location of certain computer hardware items was the result of inadequate tracking of the movement of computer hardware between the various court and department locations, as well as incorrect recording of serial and IT property tag numbers. In addition, the listing did not include acquisition and installation dates for all computer hardware, nor the value and historical cost of the asset.

With respect to data completeness, our data analysis of the population of 21,027 items disclosed the following:

Inventory Data Fields	Number of items missing adequate information	Percent of Missing Items
Historical cost	15,872	75.48%
Serial number	2,767	13.15%
Date item purchased	13,442	63.92%
Date item placed in service	17,327	82.40%
Tag number	2,868	13.63%
Location of item	Over 4,000 items listed as location unknown; Other items were never updated or adjusted upon transfer or relocation. Less than half of the items sampled were in the location as noted on the inventory record.	> 19.02%
Name of building		
Name of department		
Floor number		
Room number		
Assignment		
Ownership	Most items are listed as assigned to the person to who the item was shipped.	

Using a judgmental sample of 195 out of 21,027 IT-related items from the IT Department's inventory record of IT resources located at AOTC and the Trial Court, as of May 16, 2002, our test revealed that only 89 of these items were properly tagged and could be traced from their physical location on the floor to the AOTC IT-related asset records. We were unable to trace any items from the IT-related asset inventory list to the items located on the floor due to limited or blank location descriptions on the inventory list. We also tested 78 IT-related assets at the Hampshire Probate and Family Court. The OSA staff verified the Hampshire Probate and Family Court's inventory record to the IT-related assets found at the Court. The Court's inventory record was then reconciled to the AOTC IT Department's inventory record. Sixty-four of the items were towers or monitors – fifteen were correctly recorded as located at the Hampshire Probate and Family Court, while the other forty-nine were listed at other courts or without a location. Of these sixty-four items – six of the items (matched through their serial number) had incorrect IT control tags recorded on the AOTC list, and five of the items had tag numbers which

were also listed for another item on the inventory list. Of the fourteen printers found at the Court, only nine were recorded on the IT Department's inventory list. Further, two additional printers were recorded on the IT Department's inventory list and not found at the Court, one was located at another court, and one could not be located in a court location. No reports of lost or stolen equipment had been reported to the State, according to the AOTC Fiscal Affairs Department records since 2001. The inventory problems noted above were also found by other court IT audits conducted during the same period at separate courts, indicating a systemic problem regarding IT inventory control across the Trial Court. Given the extent of the MassCourts Project, strict inventory control to support a much higher level of IT configuration management is a critical success factor for the overall project.

Procedures should be in place to ensure that authorized and identifiable IT-related assets are recorded upon acquisition in the inventory system of record. These procedures should also provide for the authorized disposal of damaged or obsolete IT-related assets. Moreover, procedures should be in place to keep track of changes to the IT configuration (e.g., new item, status change from development to prototype, maintenance, base-line core item for business continuity planning, etc.). Movement of IT resources should support IT strategic initiatives or operational support objectives and should be properly authorized before asset relocation. All relocations of IT equipment should be properly logged (to a transaction file or source document) and appropriate updates should be made to the inventory master file. The authorization process, logging and control over relocation should be an integrated part of the IT-related asset inventory system of record including reviews of changed records. This information is essential to adequately monitor the life span of IT resources as well as their total value.

The role of IT configuration management should not be underestimated, especially in an IT environment the size of the Trial Court and with the MassCourts Project unfolding. A far more comprehensive approach is needed to address IT resource tracking, status accounting, and configuration control. Appropriate measures in configuration management can support multiple operational and control objectives, including providing valuable input to an IT strategic planning process.

The absence of adequate IT-related inventory control and configuration management on the part of the AOTC has hindered the process of ensuring timely, detailed IT system assessments, the results of which would be one of the primary inputs to a strategic planning process. The lack of an enterprise-based approach to IT configuration management hinders senior management, the IT Department, and the PMO from making decisions regarding IT resource allocation, configuration change management, and version upgrades and patch management. A contributing factor to the weak controls is that IT configuration management; including strong inventory control, IT asset tracking, resource status identification, accounting of all IT resources, and assessments of IT resource capabilities, did not appear to have been a traditional priority of the AOTC management.

Recommendation

We recommend that the AOTC review its current control guidelines to the control guidelines regarding asset management outlined in the Office of the State Comptroller's (OSC) "Internal Control Guide for Departments". Based on the results of the review, the IT Department should review, strengthen, and implement its formal policies and procedures regarding control of its hardware and software inventories. Once AOTC senior management has approved the policies and procedures, they should be distributed to the appropriate staff, and the staff should be instructed in their use.

We recommend that AOTC use one fixed-asset inventory system that includes IT resources, rather than having a fixed asset system of non-IT resources maintained by the Fiscal Affairs Department and a separate inventory for IT resources maintained by the IT Department, both of which are considered as the official system of record for fixed assets. By utilizing a single system, key users and departments or courts responsible for IT resources could reconcile their subsidiary records to a "read only" copy of their "view" of assets under their charge. Changes to the system of record's data could be made or "cleared" by the Fiscal Affairs Department.

In conjunction with the enhancing of policies and procedures, the AOTC should include procedures regarding the maintenance of a perpetual inventory that should be periodically reconciled to the physical assets master inventory record. Moreover, we recommend that the inventory list for the AOTC assets include fields to more adequately describe the asset. The fields should include, at a minimum: location, historical cost, serial number, description, date placed in service, tag number, and capacity of the system in order to properly track obsolete or inoperable equipment on its inventory record location. In addition, we recommend that the AOTC follow procedures regarding compliance with all state reporting requirements for fixed asset transfers or disposal.

To maintain a current and perpetual inventory record for its IT assets, the AOTC should record new purchases, donations, and equipment transferred to the AOTC in a timely manner, and then as necessary delete items that have been sold, donated, lost, or transferred to surplus property. In addition, transfers of equipment within and between departments and courts should be monitored and then recorded on the inventory record. Procedures should include a tracking system in order to keep track of all movement of fixed assets throughout the office or courts, as well as a listing of designated personnel responsible for the physical yearly inventory.

Once the IT-related asset inventory record has been implemented, we recommend that the AOTC periodically perform a physical inventory and reconcile the physical inventory items with the current perpetual inventory record. To maintain proper internal control, a staff person who is not responsible for maintaining the IT-related asset inventory record should administer or perform the periodic reconciliation.

Further, the inventory record should be used as a source for the financial records or reports of the AOTC. All AOTC property and equipment assets, including IT-related assets, should be included in the Trial Court's inventory system of record. System and application software should be included in the inventory and should be adequately identified as to product or system name, purpose, cost, owner, version, most recent patch (if applicable), license reference (if applicable), and degree of criticality with respect to business continuity planning.

We recommend that the IT Department address IT configuration management. AOTC management should establish a general framework regarding the acquisition and maintenance of its technology infrastructure. Configuration management procedures should be established to ensure that critical components of the organization's IT resources are appropriately identified and maintained. There should be an integrated process whereby current and future processing demands are measured and provide input to IT strategic planning and an IT resource acquisition process.

4. **Disaster Recovery and Business Continuity Planning**

We found that although the AOTC IT Department had addressed business continuity planning on a limited basis and that backup copies of magnetic media were available for recovery efforts, a sufficiently comprehensive business continuity and contingency plan for the AOTC's offices, Cambridge data center, and the Trial Court at large had not been developed by the AOTC. In addition, although the IT Department had on-site and off-site storage of backup media, there was no alternative-processing site to use to regain processing should the Cambridge data center be damaged or inaccessible for an extended period of time. As a result, if a disaster were to occur, the restoration of automated systems that are supported by the IT Department could not be attained within an acceptable period of time, thereby jeopardizing essential court operations.

At the time of our audit, we reviewed the AOTC's stated "Business Continuity Plan." The document primarily addressed emergency scenarios for Y2K for court management to continue to provide essential court-related functions and activities if a Y2K-related disaster should occur. The only section that pertained to information technology was "Automation Section" which dealt mainly with possible Y2K problems and did not address the current technology in use at the AOTC or the Trial Court. Furthermore, some of the completed sections contained inaccurate and outdated information. Although the procedures in this section were noted as "the normal contingency plans that are now used in the Trial Court system" the plan was not representative of an adequate business continuity plan. Instead, the plan generally pertained to the evacuation of the courts and did not deal with information technology, manual back-up systems and procedures, or recovery of hard-copy files.

During the course of the audit, our audit work at individual courts within the Trial Court indicated that users were not familiar with AOTC's plans regarding business continuity planning. The individual courts were also unaware of their responsibilities with respect to developing appropriate user area plans and contingency plans to address the loss of centralized and local processing capabilities. From our discussions with IT Department and court personnel, it appeared that little communication regarding disaster recovery and business continuity planning had taken place, and as a consequence, little collaborative effort had been made to ensure that adequate plans are in place to ensure the availability of automated systems, and/or continued operational processing for mission-critical processes.

Even as a preliminary step in addressing business continuity planning, AOTC management had not assessed the relative criticality of their automated systems and had not conducted a risk analysis to determine the extent of potential risks and exposures to IT operations. The risk analysis, once developed, should identify the relevant threats that could significantly degrade or render the systems inoperable, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence for each disaster scenario.

We acknowledge that AOTC is responsible for developing and testing a formal business continuity and contingency plan to restore automated functions in a timely manner, and that the AOTC has not identified or tested alternate processing sites for operations should a disaster render mission-critical or essential computer systems unusable or inaccessible. Additionally, the tasks and responsibilities necessary to carry out the completion of the AOTC and the Trial Court's duties and business objectives under various disaster scenarios for all relevant AOTC and court personnel had not been documented.

Without a comprehensive, formal, and tested recovery and contingency plan, including required user area plans, the AOTC's ability to regain critical processing capabilities and access information related to its various application systems would be impeded. Given the absence of recovery plans, a significant disaster impacting the AOTC's automated systems would seriously affect the AOTC's and the Trial Court's ability to regain critical and important data processing operations. Business continuity and contingency planning has assumed added importance given the potential processing disruptions that could be caused by man-made events. Further, the AOTC had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical important business functions processed through the WAN, the LAN servers, or the applications residing on the workstations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption to computer operations. Generally accepted practices and industry standards for computer operations support the need 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.

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

Auditee's Response of Recent Improvement and Corrective Action Taken

Several initiatives are under way to address Disaster Recovery (DR). A possible site (Brockton Court House) has been identified. The Infrastructure

team is presently investigating the DR design and what the connectivity and equipment requirements would be to use the Brockton Court House. A draft of that infrastructure and its associated cost are expected the week of February 17. Also a first pass on the Business Impact Analysis (identified the critical applications, determined restoration priorities, and associated outage times) has been accomplished; this is very basic and the business areas need to be involved.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the AOTC's information system environment, determinations of system criticality and the risks and exposures associated with the systems and supporting technology are relevant and reliable, appropriate IT and user area plans are developed based upon the relative criticality and importance of systems and associated risks, adequate resources are available, plans are adequately tested to ensure viability, and appropriate change management is in place to maintain business continuity policies, procedures and related plans.

During our audit, we observed that disaster recovery and business continuity planning had not been thoroughly factored in to the roll out and final implementation of the MassCourts application system. Given the importance of the MassCourts Project, a much stronger effort must be made to address system availability for the new enterprise-based application system.

Auditee's Response of Recent Improvement and Corrective Action Taken

All initiatives, aimed at Disaster Recovery, have included Project Office personnel in those discussions. This includes meetings with vendors who may be able to provide DR services to Oracle databases.

We determined that procedures regarding the generation and on-site and off-site storage of back-up media were adequate. The AOTC's IT Department did have adequate locations for on-site and off-site storage of the backup media. While the back-up copies will aid in a recovery strategy, the selection of an alternate processing site is essential to ensure recovery of automated systems should AOTC's primary data center be damaged or become inaccessible.

During the audit, we noted the following:

- There was no business continuity planning framework in place within the AOTC to address information technology. Efforts that had been made focused primarily upon generating and storing backup copies of electronic media in on-site and off-site locations. IT management had not established a business continuity framework, in cooperation with business process owners (individual courts), to define the roles and responsibilities, the risk-based approach/methodology to be adopted, review and approval procedures, and the requirements to document, approve and test business continuity and contingency plans.
- AOTC management could not ensure that the IT continuity plan would be in line with an overall business continuity plan for the Trial Courts (covering non-IT processing). The IT business

continuity plan (incorporating recovery of networks and AOTC-supported systems and any court-based systems) should take into account the IT strategic and tactical plans to ensure consistency.

- IT management has not developed and documented a business continuity plan containing the following:
 - Guidelines on how to use the business continuity plan.
 - Emergency procedures to ensure the safety of all affected staff members of the Trial Court.
 - Response and recovery procedures to bring the business processes and court functions to a required level of service (mission-critical to essential services).
 - Procedures to safeguard and reconstruct the central office, Cambridge data center, and any other essential facilities.
 - Communication procedures with employees, the public, equipment suppliers and vendors, third parties, and the media.
 - Contact information on continuity teams, management and staff impacted, users, vendors, and other state entities.
- AOTC management had not established a business continuity methodology to ensure that all concerned parties receive regular training sessions regarding notification, recovery, security, documentation and contingency procedures to be followed in case of an incident or disaster that renders IT inoperable for an extended period.
- AOTC management had not identified in a business continuity plan the critical application programs and data files, operating systems, personnel, third-party services, resources and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations had not been identified, documented, prioritized and approved by the business process owners in conjunction with IT management.
- AOTC management had not incorporated in the business continuity methodology a process to identify and approve an alternative back-up processing site and required hardware and other IT resources. If these types of services can not be established internally, the services and resources should be obtained under formal contract.
- IT management had not established procedures for re-assessing the adequacy of recovery plans (IT operations and business process areas) following business continuity plan testing or resumption of IT services.

Recommendation

The AOTC should implement procedures to evaluate the criticality of automated systems and processing environments and assess business continuity requirements on an annual basis, or upon major changes to user requirements, automated systems, or the IT environment. Appropriate business continuity plans should be developed, documented, and tested for the application systems residing on AOTC's computer systems. Procedures should be implemented to require detailed planning, documentation, and reporting of test results to assess business continuity plans and generate, if needed, an action plan for modifying the business continuity or contingency strategy.

Given the importance of the MassCourts Project, we recommend that a focused effort be made to ensure that business continuity planning (including recovery and contingency plans at the processing site level and the user level) be addressed for the new system. Since implementation of the new application system will extend over an eighteen to twenty-four month period, appropriate recovery and contingency

plans need to be in place over that period to ensure system availability. Understandably, the array of business continuity plans will likely become more manageable once the MassCourts application system is fully implemented.

We recommend that senior management and key users assess the relative criticality of AOTC's automated systems and perform a risk analysis of the IT environment and business operations supported by technology. Based on the results of the assessment and risk analysis, the AOTC should proceed with the development of a written business continuity plan for its mission-critical and essential functions with input and approval from an IT Steering Committee and senior management. We recommend that senior management and system users be closely involved in business continuity planning to ensure that there is a clear understanding of the Trial Court's IT environment, that determinations of system criticality and associated risks and exposures are correct, that appropriate information processing and user area plans are developed based on the relative criticality and importance of the systems, and that adequate resources are available. The business continuity plan should also address short-range and long-term planning for mission-critical and important systems. Since the success of the business continuity planning process requires management commitment, management responsibilities for direction and approval should be clearly defined.

A comprehensive business continuity plan should document the AOTC's recovery strategies for IT systems and network operations with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical and essential operations within required time frames. The information in the plan should include:

- Determination of mission-critical, essential, and less essential application systems and a statement of recovery objectives for each.
- Classification of types of delays and disruptions in IT services according to impact (e.g. catastrophic, severe, serious, or limited) should be clearly delineated.
- Identification of important software and data files for each mission-critical operation.
- Documentation detailing the responsibilities and activities of each IT functional area and its designated staff to support business continuity objectives.
- Definition of different levels of disruption from operator or hardware failures to major destruction or loss of processing capabilities.
- Emergency test procedures and test criteria.
- The names, addresses, and phone numbers of key recovery personnel. Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorized personnel and should be safeguarded against unauthorized disclosure. Consequently, sections of the plan need to be distributed on a need-to-know and need to perform basis.
- Up-to-date information regarding the current processing environment for hardware and operating system software, including communications software and network requirements, utilities, and job control language for all critical production jobs and systems development facilities.
- User area plans for all AOTC and Trial Court departments must be identified and documented in contingency plans for mission-critical systems indicating completion and/or latest revision dates.

- Procedures to ensure that user area plans are evaluated periodically, tested, and revised as necessary.
- Procedures for notifying management, users and other parties that oversee or are dependent upon the AOTC should processing be lost.
- Requirements for estimated processing time (elapsed and central processing unit), daily update, end of month processing, turnaround, reporting deadlines, minimum frequency of processing for each application, and recovery times should be stipulated.
- Copies of agreements for service and/or hardware replacement should be readily available since access to the agreements could become critical during an emergency. Copies of such agreements should be stored in the offsite storage location.
- Procedures for the purchase and or lease replacement of hardware and other specialized equipment should be noted.
- Completion or latest revision date and identification of who prepared and is responsible for each section of the recovery plan and user area plans should be specified.

As a necessary requirement to successful recovery, the AOTC needs to identify an alternate processing site(s) and ensure through appropriate testing the viability of the site(s). Considerations should be made as to the extent of readiness required by the alternate processing site(s). We recommend that AOTC solicit the assistance of Administration and Finance's Information Technology Division (ITD) in the development of recovery strategies and plans.

We recommend that AOTC, the PMO, and the IT Department also consider business continuity planning requirements in the allocation of IT resources across the courts. Given the importance of the Trial Court's automated systems, there may be adequate justification for a hot site. Understandably, the hot site should have a similar operating system so that the system software will be accessible for usage in the case of emergency, in order to implement the disaster recovery plan.

We further recommend that the business continuity plan, once developed and approved, be subject to regular testing to ensure its continued viability. We recommend that the plan be periodically reviewed and updated when needed, to ensure that it is current, accurate, and complete. The AOTC and court staff should be trained in their responsibilities in the event of an emergency or disaster, and personnel should be made aware of manual procedures that are to be used when automated processing is delayed for an extended period of time. A copy of this plan should be stored off-site in a secure and accessible location.

Finally, a strategy must be developed with AOTC oversight to assist courts with hardcopy file recovery efforts, by providing provisions for scanning and imaging of case management files.

APPENDIX A
FULL TEXT OF AUDITEE'S RESPONSE



ROBERT A. MULLIGAN
Chief Justice for
Administration & Management

The Commonwealth of Massachusetts

ADMINISTRATIVE OFFICE OF THE TRIAL COURT
Two Center Plaza
Boston, Massachusetts 02108

Tel: (617) 742-8575
Fax: (617) 742-0968

February 27, 2004

John W. Beveridge
Deputy Auditor
Office of the Auditor of the Commonwealth
One Ashburton Place, Room 1819
Boston, MA 02108

Dear Mr. Beveridge:

For the past several years the Administrative Office of the Trial Court has been moving towards developing and implementing an integrated, comprehensive computer system for the entire Trial Court known as MassCourts. The retirement of the prior Director of Information Technology Department presented a unique opportunity to reexamine the structure and function of that Department. To that end, the AOTC requested that the State Auditor conduct an "IT Audit" of the Trial Court's IT Department. It was hoped that such an audit would provide a working blue-print for the improvements that would be necessary to be sure that the correct structure, policies, and procedures were present to maintain and to operate MassCourts as soon as it was in place.

The Audit Report that you have provided fulfills those expectations. Thank you for the comprehensive and complete assessment of the IT Department. The recommendations and suggestions that are contained within that document provide the needed framework that will enable further progress to be made. This Office will move to implement those recommendations as quickly and as fully as resources allow. To begin with, the "CobiT Standards" will be adopted as applicable and appropriate to the work of the Trial Court and they will provide the baseline for all future endeavors. We greatly appreciate that your office has provided us with an electronic version of the CobiT standards to serve as a framework for this policy development initiative.

As the report notes, the audit covers the period from July 1, 2001 to July 21, 2003. Since the conclusion of the audit, there has been a change in the administration in the Trial Court as well as a change in the leadership of the IT Department. The report acknowledges that improvements have been made during the audit period, and we believe that considerable

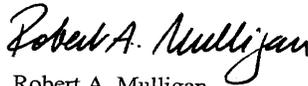
progress has continued after the end of the formal audit period. For example, as the Audit Report noted, "senior management under the new administration [of the Trial Court] has increased the level of collaboration among all departments at AOTC to improve IT management and strengthen internal control." Further, there has been a recognition of the need for formal written IT related policies and several of those policies have already been developed and implemented. More will be promulgated in the near future.

We have begun to address System Access and Security issues. The Audit Report noted, "a strong effort [has been] made to identify and document all user accounts that needed to be deactivated." In fact, formal communications between the Human Resources Department and the IT Department has resulted in the regular deactivating of IT access for former employees of the Trial Court. The need for a formal and accurate inventory control system has been recognized. The IT Departments has begun to actively pursue different options for an effective Disaster Recovery program.

I am attaching a document which identifies some specific recent improvements that have occurred as recommended in the audit report. These efforts, however, are not complete and much more remains to be done. The Administrative Office of the Trial Court will continue to work collaboratively with your Department in order to put in place the appropriate standards and controls for the Trial Court in its efforts to serve all the citizens of the Commonwealth.

Thank you again for providing us with such a thoughtful blueprint to guide our efforts to improve the IT environment.

Respectfully,



Robert A. Mulligan
Chief Justice for Administration and
Management

RAM/mab

Enc.

The following is the list of recent improvements provided in Chief Justice Robert A. Mulligan's February 27, 2004 letter of response. Each of the items listed below have been inserted in the text of the report. The page numbers listed below have been updated to reflect the current location in the final report.

Examples of Recent Steps Taken to Address Audit Report Issues

The following are specific examples of steps that have been taken to address issues raised in the audit report with particular reference to the relevant section of the audit report.

Page 20:

The Information Technology (IT) Department Director and/or his designee attend all Project Office (PO) meetings. Support desk personnel have attended some training and are utilized on-site the day of any implementation to further learn and provide user support. Information Technology staff have also been readily available for any PO inquiry or support.

Page 21:

Various policies have been published, addressing the areas of management control and resource utilization. The need for any further policies is being investigated and those policies will be developed when identified.

Page 21:

Policies have been developed addressing IT service delivery and the users expectations of that, to include service levels. The need for any further policies is being investigated and they will be developed when identified.

Page 22:

Several policies have been developed that address the management of IT across all courts and several other initiatives are actively being pursued which will further address this area.

Page 24:

The gap between the IT department and user community has been greatly reduced through active Director involvement, querying of the user community, and periodic informative web postings and mailings. Also a policy and process were put in place for the user community to formally address any IT support issue. This process includes IT Director review, staff input, and follow-up.

Page 25:

The Information Technology (IT) Department Director and/or their designee attend all Project Office (PO) meetings. Support desk personnel have attended some training and are utilized on-site the day of any implementation to further learn and provide user support. Information Technology staff personnel have also been readily available for any PO inquiry or support.

Page 26:

A variety of policies have been published and the need for any further policies is being investigated and those policies will be developed when identified.

Page 28:

The Deputy Directors, through line management, have been documenting department processes and continue to identify additional areas where documentation may be needed. Additional policies are being identified and development will be ongoing by the IT Director.

Page 29:

When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their respective court or office and post it. The policies are also posted on the Trial Court web site.

Page 30:

The above statements for page 29; first paragraph could be input here as well.

Page 30:

The courts have been made aware of the policies and are empowered to enforce them, as are the IT Departments Field Technicians and Support Desk personnel. Also an initiative is on-going, that when fully implemented, will allow the IT Department and the courts to more stringently enforce asset management and software inventory through a vendor product.

Page 31:

All published policies are routinely reviewed by the IT Director and staff. When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their court or office and post it. The policies are also posted on the Trial Court web site.

Page 34:

The PO and IT department have developed a very open and proactive relationship, which continues to evolve as the project evolves.

Page 39:

When policies are developed, they are approved by the CJAM and AOTC management, and subsequently disseminated via Human Resources (HR) to the courts. The HR representative in each court is asked to inform their court or office and post it. The policies are also posted on the Trial Court web site. Also a periodic web posting, by the Director, aids in informing the user community on initiatives that are being undertaken by the IT department.

Page 39:

A policy and process are in place that allows for the user community to provide formal input into the quality of services received. This process includes staff involvement and user follow-up. Also the Director has readily broadcasted his openness to directly receiving telephone calls or emails. All of which are responded to.

Page 40:

An initial Business Impact Analysis was completed by the IT Department and several initiatives are underway that address these issues and other opportunities are being investigated as to their applicability.

Page 41:

Policies that have been developed and published to the courts have been well received and relevant. Any additional policies are either under development or being investigated.

Page 43:

A draft IT mission statement is under review. The focus is to better tie IT services to business objectives.

Page 49:

The Human Resource Department has routinely and consistently provided the IT Department with a list of terminated employees. That list is in turn used to delete user accounts and access and to provide some basic asset management.

Page 50:

The above paragraph pertaining to page 49 could be inserted here as well.

Page 50:

Policies have been developed and published that address these issues and others are being identified for development.

Page 51: User access lists were initially cleaned up, early last fall, through an audit, directed by the Director of IT and conducted by the individual courts. That data was then used by the IT department to update the Internet access lists. To date a monthly (sometimes twice a month) termination list is provided by the Human Resource Department to the IT Department. This was initiated early last fall and provides for a more timely and proactive approach to eliminating user accounts and access. A process has been put in place that allows for a proactive approach to eliminating employee accounts and access.

Page 52:

Several initiatives are being actively investigated to address this. One is a new desktop operating system and the other is a new way of handling email.

Page 59:

An initiative is underway, using LANDesk, that when fully implemented will allow for the individual courts and the IT Department to more stringently address asset management.

Page 60:

When LANDesk is fully implemented appropriate policies and procedures will be put in place, which through its use and support by the individual courts, will allow for adequate inventory control of fixed assets.

Page 67:

Several initiatives are under way to address Disaster Recovery (DR). A possible site (Brockton Court House) has been identified. The Infrastructure team is presently investigating the DR design and what the connectivity and equipment requirements would be to use the Brockton Court House. A draft of that infrastructure and its associated cost are expected the week of February 17. Also a first pass on the Business Impact Analysis (identified the critical applications, determined restoration priorities, and

associated outage times) has been accomplished; this is very basic and the business areas need to be involved.

Page 67:

All initiatives, aimed at Disaster Recovery, have included Project Office personnel in those discussions. This includes meetings with vendors who may be able to provide DR services to Oracle databases.

APPENDIX B**Auditor's Reply**

We commend the initial efforts made by the AOTC to implement corrective action based on discussions during and subsequent to our audit. We are pleased that the recommendations presented in our audit report will serve as a blueprint for strengthening control and addressing IT governance within the Trial Court. We believe that senior management under the new administration has improved communication among AOTC departments to improve IT management and strengthen IT internal control. While progress regarding the development of IT-related policies and procedures for the Trial Court's IT environment has been made, further effort in this area, as noted by the AOTC, as well as addressing other pertinent issues is needed. For example, IT strategic and tactical planning needs to be adequately defined and communicated to address all IT-related functions across the courts and be aligned with overall strategic planning for the Trial Court's business objectives. Furthermore, the establishment of a steering committee to provide oversight, guide IT direction, review and approve IT policies and procedures, and evaluate IT performance will assist the IT Department in meeting its primary business objectives.

We reiterate the importance of reevaluating the IT organizational structure across the courts to ensure clearly-defined roles and responsibilities, adequate points of accountability, clearly-established reporting lines, and proper segregation of duties with respect to security and internal audit functions. It is also imperative that monitoring and evaluation of control practices within the IT environment be formalized and integrated into management practices, quality assurance, and internal audit activities to help provide appropriate assurance mechanisms that operational and control objectives are being met. The AOTC's Internal Audit group should develop the capability to conduct general IT control and application system audits and be realigned within the organizational structure to ensure adequate independence and reporting to a higher level of management.

Regarding access security, we acknowledge that AOTC had initiated corrective action by terminating user privileges for employees who were no longer employed by the Trial Court, and had established that user accounts would be deactivated on a monthly or bi-monthly basis in the absence of a framework of timely notification of required access changes. Clearly, it is important to implement appropriate policies, procedures and mechanisms to ensure timely notification so that modification or deactivation of access privileges can be performed as soon as IT security is notified. Although the Auditee's response stated that "the Human Resource Department has routinely and consistently provided the IT Department with a

list of terminated employees,” evidence gathered during the audit indicated that the HRD reporting had not been in effect and that cumulatively there were over one thousand user accounts for various systems that needed to be deactivated. We believe that efforts to establish a comprehensive IT security strategy and administrative framework and obtain and implement appropriate technical tools will greatly assist the Trial Court in addressing access security over its IT systems and IT processing environment.

With respect to system availability, a thorough risk analysis of the application systems and the IT environment must be completed through your business impact analysis. The analysis should include current and future application systems and supporting platforms. In conjunction with your user community, the AOTC should develop, document, and test disaster recovery/business continuity strategies and contingency plans for the Trial Court as well as periodically review and update the plans to ensure their viability and the accuracy and completeness of required information. The IT Department needs to formally identify a viable alternate processing site to ensure the resumption of IT operations within an acceptable time period.

Although we have identified certain control practices that would aid the MassCourts Project, the success of the Project will remain at risk until an appropriate framework of controls for IT governance is established, including full management commitment and appropriate assurance mechanisms for all IT functions within the IT Department and across the Trial Court. Although our audit was not specifically focused on the MassCourts Project, we believe that strong project management techniques and controls are necessary to integrate this major IT initiative throughout the Trial Court. In that regard, project management techniques need to be supported by comprehensive documentation, action item tracking, and management and audit trails to enhance the project team’s ability to respond and provide improved accountability across the entire enterprise. Effective tracking and oversight controls for monitoring and evaluating vendor performance and the progress of the Project are a necessary ingredient for project management. If the Project is not meeting its cost, schedule or performance goals, management should determine the reasons for the deviations, the corrective actions planned by the contractor/developer, and whether the corrective actions are likely to achieve baseline goals within established completion dates. If required, project management should determine a new approach to achieve project objectives and alert management through clear lines of communication of the positive or adverse impacts of the required changes. High-level oversight and an enterprise-based framework will help prevent projects from falling prey to narrow silo-based viewpoints where costs and benefits are assessed at an individual department level, versus an enterprise level. We encourage the Project Management Office to ensure that operational, security, and informational requirements of the entire enterprise are taken into consideration when evaluating and reassessing the Project’s requirements.

We believe that the new administration and management team's commitment to develop and implement an enterprise-based IT control framework for the Trial Court will significantly improve the likelihood of success for IT initiatives.