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. 2007-1106-7T

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

February 12, 2007 to April 16, 2008

OFFICIAL AUDIT REPORT

JULY 22, 2008

TABLE OF CONTENTS

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. At this time, Administrative Justices became responsible for the administration of each court department. The 1978 statute also created a central administrative office managed by the Chief Justice for Administrative and Management who is responsible for the overall management of the Trial Court. The statute provides for the central office, referred to as the Administrative Office of the Trial Court (AOTC), to develop a wide range of centralized functions and standards for the benefit of the entire Trial Court. The Massachusetts Trial Court is under the general superintendence of the Supreme Judicial Court. The Trial Court judges, of which there are 362, sit in more than 130 locations across the state. Overall the Trial Court employs more than 7,000 people.

AOTC's primary objective is to enhance the administration of justice in the Commonwealth. The AOTC is comprised of nine departments which are: Court Capital Projects; Court Facilities; Fiscal; Information Services; Judicial Institute; Legal; Human Resources; Planning and Development; and Security. Trial Court Information Services (TCIS) provides IT services to the AOTC and the courts throughout the state. The mission for TCIS is to "pro-actively support the data processing and information system needs of the Trial Court using computers and communication technology." TCIS has responsibility for the selection, implementation, operation and support of computers and networks used by the Trial Court.

TCIS is located at three sites, an office environment at Three Center Plaza in Boston, and two data centers located in Cambridge and Worcester. The Cambridge data center is the AOTC's primary data center providing IT support for the Trial Court's network operations and computer systems. The Worcester data center, which was being constructed during our audit period, housed computer equipment by the close of our audit. The TCIS is under the direction of a Chief Information Officer (CIO) who reports directly to the Chief Justice for Administration and Management. The TCIS is staffed by 55 employees, of which 30 are located at Three Center Plaza and perform administrative and fiscal duties, as well as help desk functions. The Help Desk assists Trial Court Departments and employees by providing access security administration and technical support. Twenty of the TCIS staff are located at the Cambridge Data Center and manage the network operations and perform back-up functions for the AOTC and Trial Court computer systems. There are five technical field support staff outside of the main office and data centers who are responsible to handle technical assistance service calls from various courts. As of the close of our audit, there were no permanent TCIS staff assigned to the Worcester data center.

At the time of our audit, the AOTC's computer operations included mainframes, file servers, and over 6,400 computer workstations located at the AOTC office and at court facilities throughout the state. The AOTC's local area network (LAN) and wide area network (WAN) have combined characteristics of a star topology and ring topology. All the local courthouses have ring networks that connect to a central mainframe computer. Generally, courts are connected to the Cambridge Data Center by single or multiple T1 lines.

Since our prior audit report (No. 2002-1106-4T), issued June 22, 2004, the AOTC has implemented a number of new technologies and standards. A new desktop backup infrastructure has been implemented that facilitates the nightly backup of desktop data to a centralized infrastructure using EMC Centera archival disk storage. The desktop data that is backed-up is stored in two Trial Court facilities and synchronized in real time between the locations. This same storage infrastructure is being used to store document images for the Probate and Family Court. In addition, the Trial Court has installed a series of Lightweight Directory Access Protocol (LDAP) servers to act as a central authentication infrastructure for the Trial Court.

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 access to the Internet. The AOTC network provides connectivity for various Trial Court application systems. The Basic Court Operation Tools (BasCOT) continues to be used for civil and criminal case management by Probate and Family Courts and the District Courts for civil case processing. The Case Management and Court Operations (FORECOURT) application system is used for case management by the Superior Courts. Court Activity Records Information (CARI), Juvenile Court Records and Information System (JURIS) and Probate Receipt Accounting (PRA) are also supported at the Cambridge Data Center. PRA processes and tracks receipts and disbursements under the supervision of the probation office within the various court divisions. The Office of the Commissioner of Probation uses CARI to present the complete and statewide history of criminals in a central file. JURIS tracks juvenile subjects from the time a complaint or petition is filed against or behalf of the individual, through the probationary period of the individual, and maintains all pertinent docket and probation information. Authorized users at AOTC also have access to the Commonwealth's Information Technology Division's (ITD) mainframe providing connectivity for access to the Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS). The AOTC also utilizes several software packages, including Open Office, WordPerfect, and Excel. In addition, the TCIS Help Desk staff use the HEAT (Help Desk Automation Expert Tool) application system to track user requests, and handle the requests and document the resolution of those requests. The system provides the capability to organize and distill information and generate reports on Help Desk activity.

In January 2003, the AOTC selected the vendor MAXIMUS to develop and implement a new comprehensive case management application system. The rollout of this new software application, known as MassCourts, started in February 2005. In addition, working with MAXIMUS, the Trial Court has implemented a stand-alone imaging system for the Probate and Family Court that has been used since January 2006 to capture documents filed with the court.

The MassCourts application, when fully installed at all Trial Court locations, is intended to be a comprehensive case management system that will provide case entry, docketing, scheduling, case-related financial management, automated reports, notices and forms, and electronic storage of case documents available through the Trial Court Intranet. The system will allow the Trial Court to manage all case-related information and enable all departments and divisions of the Trial Court to share information and monitor and track cases as they proceed through the legal system. The system's data provides a base for AOTC and the Trial Court to help establish and measure progress toward achieving realistic goals.

The Office of the State Auditor's examination focused on the current status of prior audit results and a review of the implementation status of the MassCourts application system.

.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Administrative Office of the Trial Court (AOTC) for the period of July 1, 2004 through April 16, 2008. The audit was conducted from February 12, 2007 to April 16, 2008. The scope of our audit included an examination of selected control practices and procedures to determine the status of corrective actions taken since our prior IT audit report (No. 2002-1106-4T), issued June 22, 2004, regarding IT organization and management, system access security, inventory control of computer equipment, procedures for IT infrastructure planning, and disaster recovery and business continuity planning. During our audit, we assessed the current status of the MassCourts project.

Audit Objectives

Our primary audit objectives were to determine whether AOTC had initiated and implemented corrective action on prior audit results as reported in our prior audit report (No. 2002-1106-4T), and whether the IT control environment provides reasonable assurance that control objectives would be met to support AOTC and the Trial Court's business functions. More specifically, we sought to determine whether AOTC and the Trial Court Information Services (TCIS) had a defined organizational structure and that TCIS organizational and management controls were in effect over information technology activities to ensure such activities would be managed effectively and efficiently. In conjunction with our review of TCIS organization and management, we determined whether AOTC had established a sufficient IT planning framework to generate and implement strategic and tactical plans to help fulfill the AOTC's mission and goals. We sought to determine whether IT policies and procedures were adequately documented. We also sought to determine whether quality assurance standards existed and whether adequate monitoring and evaluation procedures were in place for IT-related activities.

A further objective was to determine whether adequate controls were in place to prevent and detect unauthorized access to AOTC's network, application systems and data files, including the Trial Court's primary application (MassCourts) available through the AOTC's network and workstations.

Our objective with respect to the AOTC's IT inventory control was to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly accounted for in a complete inventory record, available when required, and safeguarded against unauthorized use, theft, or damage. We also sought to determine whether appropriate data was being recorded in the inventory system of record to support configuration management decisions.

Regarding system availability, we sought to determine whether controls were in place to provide reasonable assurance, through business continuity planning and access to backup copies of system and data files, that required IT processing of mission-critical and essential computer operations could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible.

Finally, we sought to assess the current status of the MassCourts application roll-out and to determine whether adequate management controls were in place to support the continued implementation and future operation of the MassCourts application and to provide reasonable assurance that project objectives would be met. We also sought to provide an independent review of the project status by reviewing user surveys at selected District Courts and Court management feedback on MassCourts Lite to ensure that the information provided to AOTC management is accurate and project problems are detected in a timely manner.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of the AOTC's relevant operations, and the IT infrastructure, including the MassCourts application system; reviewing documentation; and interviewing management and staff regarding TCIS' mission, operations, and IT organization and management. We also reviewed the prior audit findings and auditee responses presented in the previous audit report (No. 2002-1106-4T).

To determine the appropriateness of documented IT controls, we identified IT functions, conducted a high –level risk assessment, reviewed documentation regarding the TCIS' mission and operations, and documented IT policies and procedures. We interviewed the AOTC's Chief Information Officer, MassCourts IT Project Executive, and the MassCourts IT Project Manager. We also interviewed AOTC staff at the central office 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 TCIS. 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 TCIS staff, observed operations, and performed selected audit tests.

Regarding our examination of organization and management, we interviewed TCIS senior management, completed questionnaires, analyzed and reviewed the organizational structure and reporting lines of TCIS, and requested documented IT policies and procedures. We reviewed and analyzed existing IT-related policies, standards, procedures and strategic plans to determine their adequacy. We also evaluated the organizational structure of the TCIS to support IT functions. To determine whether the IT-related job descriptions and specifications for TCIS staff were up-to-date and reflected current responsibilities and technology knowledge requirements, we obtained a current list of TCIS personnel and compared the list to the department's current organizational chart and employee IT-related responsibilities. To determine whether an IT-related steering committee was in place and providing adequate oversight of IT functions and processes across AOTC and the Trial Court, we interviewed senior management and staff of the TCIS, assessed the need for oversight, and reviewed the Court Management Advisory Board's reports and minutes of committee meetings.

We reviewed the adequacy of operational and management controls, including documentation of TCIS' mission, 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 whether assurance mechanisms were in place and in effect to monitor compliance with the established policies and procedures. 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 management control practices for IT operations and functions.

Regarding our examination of access security controls, we reviewed policies and procedures to authorize, activate, and deactivate user privileges to access the AOTC's network and associated application systems. The application systems, which reside on various AOTC file servers, are accessed through microcomputer workstations located at the AOTC's administrative offices and throughout the Trial Court. We reviewed control policies and procedures regarding logon ID and password administration, including requirements for password composition, length and frequency of change. We evaluated the appropriateness of documented policies and guidance provided to AOTC and Trial Court personnel by interviewing the AOTC's security staff and TCIS management and comparing current security practices to generally accepted security practices. In addition, we reviewed control practices used to assign AOTC and Trial Court staff access to the application programs and data files. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed, observed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes.

We observed the procedures followed by the TCIS operations staff for granting users access to the Trial Court network and e-mail system, and providing the users with Internet access. We also observed the process of the staff of the MassCourts Implementation Team to provide users system access and access privileges to the MassCourts application. Further, we observed the operations staff and the MassCourts Implementation Team staff's use of the LDAP application to compare the system-generated user account list to the Trial Court payroll list. The resulting exception lists were cleared through e-mails to appropriate supervisors.

To further determine whether there were adequate controls in place to prevent unauthorized entry to the AOTC's network, e-mail system, and the MassCourts application, we conducted testing of our own to verify that the new procedures were in effect. The testing included a comparison of Trial Court employees on the current payroll list and authorized non-employees, selected at random from two of the trial courts, to the access lists for the AOTC network, e-mail system, and the MassCourts application. Our audit did not include a review of access to the legacy systems still on the network.

To determine whether adequate controls were in place and in effect for inventory control of computer equipment, we reviewed AOTC's inventory policy and procedures for control of property and equipment. To identify AOTC's system of record for IT equipment, we interviewed the CIO, the Deputy Director of TCIS operations, and staff from the Fiscal Affairs Department who were responsible for maintaining inventory records. We then requested and reviewed inventory records for the trial courts and departments. Further, we reviewed the data records to determine whether they contained adequate fields of information for financial and IT configuration management.

To verify the integrity of the information on the AOTC's inventory listing, we assessed the level of data completeness for required data fields from a sample of available inventory records. To determine whether the AOTC's available inventory system of record was current, accurate, and valid, we compared a selected sample of IT-related inventory items listed on the inventory record to the actual computer equipment on hand. Due to a lack of a complete system of record, we judgmentally selected inventory items from a listing for departments located at Center Plaza, containing a population of 500 IT-related inventory items. We then selected a random sample of 60 items out of the population of 500 items listed on inventory record and conducted inventory tests at the AOTC offices at Center Plaza. Since at the time of our audit, only 56% of the required inventory records had been completed, received and maintained in the Fiscal Affairs Department, we did not conduct inventory tests at selected court locations.

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 Trial Court and 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 TCIS staff and AOTC management 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 would be available to allow the Trial Court and AOTC to recover its IT functions in a timely manner in the event that the Cambridge Data Center is damaged or inaccessible.

To gain an understanding of the current status of the MassCourts application rollout 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 MassCourts Project Manager, and other staff working on the project. We reviewed project documents related to the planning and status of the project, including staff resources, deliverables, and tasks breakdown. We conducted user surveys at 15 of the 63 district courts to determine whether the MassCourts Lite application system supports the mission of the AOTC by providing a comprehensive approach to case management information, and whether the system was meeting the needs of the user, or if changes were required. We also conducted follow-up interviews with some of the initial users and District Court management to determine whether improvements were made to the application system and the in-house training since our initial surveys. The results of the surveys were intended to provide candid responses from users located within the Trial Court's Clerk Magistrate and Probation Offices to help improve the MassCourts Lite application. The surveys focused on system response time, application functionality, training, IT support, and user comfort level and user satisfaction. During the audit, the results of the user surveys were discussed with TCIS management upon completion to assist in timely corrective action, if needed.

Our review was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry 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. Review results for selected areas were benchmarked to CobiT's maturity models included in CobiT 4.1. 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

We found that under the current AOTC leadership the rollout of the MassCourts application system is progressing in a systematic and efficient manner to allow Trial Court staff to understand and effectively use the system. Our review and assessment of the operations of the MassCourts application system installed by the AOTC indicated that the application is supporting the introduction of a comprehensive approach to case management information within the District Court Department, the Boston Municipal Court, the Probation Department, the Land Court, and the Housing Court Department. With respect to overall cost, AOTC management has been tightly monitoring project expenditures and working closely with MAXIMUS, the developers of MassCourts, to attain appropriate IT value by ensuring that expenditures are necessary and cost beneficial, and that the bond amount of $75 million is not exceeded.

To date, MassCourts has enabled AOTC management to receive data systematically for the production of management reports and to monitor metrics, such as time standards. The value delivered through the standardized data obtained through MassCourts will define and allow monitoring of key metrics and allow management to respond to changes or deviations in a timelier manner. The performance metrics will assist management in assigning appropriate accountability for the delivery of timely justice across the Trial Court. With regard to functionality, the MassCourts application when fully installed in all the Trial Court Departments will allow case-related information to be managed comprehensively by providing case entry, docketing, scheduling, case-related financial management, system generated reports, notices and forms, and storage of case documents.

We found that steps have been taken to strengthen IT governance and IT controls within the AOTC and the Trial Court and that corrective action has been taken to address several of the issues and recommendations presented in our prior audit report (No. 2002-1106-4T), issued June 22, 2004. Our prior IT audit had found that AOTC needed to develop and implement a comprehensive IT governance and control framework and assurance mechanisms to ensure that IT control objectives would be met. Our current audit has revealed that overall IT governance has improved at AOTC. However, our review indicated that although improvements in control practices had been made since our prior audit, IT general controls with respect to certain aspects of IT organization and management, system access security, inventory control for computer equipment, and business continuity planning needed to be further strengthened, documented, and monitored.

Regarding IT organization and management, we found that managerial direction has significantly improved in terms of value delivery, resource management, risk management, performance measurement, and IT strategic planning related to the MassCourts rollout. We also found improvement in terms of communication and defining organizational structure for IT functions. The current administration, under the direction of the Chief Justice, has aligned IT resources to meet business objectives and strategic goals. For example, the administration has been able to establish performance measurement goals and related metrics across all trial courts to review the progress of outstanding cases using standardized data delivered through the case management system and other sources.

Regarding strategic and tactical planning initiatives, we found comprehensive IT strategic and tactical plans in place and aligned with court functions with an improved degree of oversight for the MassCourts application rollout. We found that the CIO provides oversight by meeting with key department management and staff on a regular basis and is advised by the Court Management Advisory Board. We found that the milestones regarding the MassCourts rollout were based more on a systematic approach using operational goals and tactical logistics rather than predefined or arbitrary timeframes. However, the Trial Court Information Services (TCIS) should expand the scope of the IT strategic and tactical plans to include other IT initiatives, tasks and activities beyond the MassCourts rollout to be addressed by TCIS, such as the reconfiguration of the data centers and determination of an alternate processing site.

Regarding IT policies, our current audit indicated that although AOTC has certain policies in place to assure operational efficiency and the ability to meet its primary business objectives, we found that formal internal control documentation for IT-related activities needed to be enhanced for system access security, inventory control of computer equipment, and business continuity planning.

Our current audit also revealed that the AOTC's TCIS has been using a systematic approach to risk identification for IT functions related to the MassCourts rollout and other operational areas within the AOTC and the Trial Court. However, we found AOTC had not documented a comprehensive framework to identify and assess the impact of IT-related risk to court operations or detailed the instructions for conducting IT-related risk assessments.

With regard to IT organizational structure, since our prior audit report, the AOTC has established a single point of responsibility and improved direction and accountability for IT operations and IT project management within the Trial Court under the direction of a Chief Information Officer (CIO). The overall organizational structure for TCIS has been reorganized to include IT operations, the project management area, and IT positions across the courts to address IT services, the business requirements of the MassCourts rollout, and training related IT activities. We also that found since our last audit, efforts have been made to define and communicate roles and responsibilities for IT-related functions and activities on an enterprise-based manner. AOTC should assign responsibilities across the Trial Court to include evaluation of data integrity, quality assurance, source document protection, and access and data security.

The TCIS has formalized its organizational structure and clearly defined roles and responsibilities of IT management and staff. The organizational structure properly addressed unity of command and span of control and had an established chain of command under the CIO. IT functions within the TCIS are adequately established from an operational as well as a management control perspective. We found that TCIS job descriptions delineated roles, responsibilities, and reporting lines. Also, the AOTC has established an oversight committee to provide general guidance with respect to IT direction for TCIS.

With respect to training for IT-related functions, we found that court personnel who are, or will be, performing IT functions or using technology, including the local user experts (LUE), have or will receive training to perform the tasks assigned to them based on their roles and responsibilities within their individual court. The training, which is being coordinated with the rollout of the MassCourts application, is being provided by the TCIS through classroom instruction, on-line training through the Intranet, and the distribution of reference material to assist staff in performing MassCourts functions. However, we believe that security awareness training should be made part of current and future training programs.

With respect to our prior audit recommendations concerning AOTC's need to improve IT monitoring and evaluation functions, although the AOTC had initiated corrective measures, we found that monitoring and evaluation functions still require enhancements. The controls that have been established and are in effect relate to management objectives for system access to the AOTC network, email, the Internet, and the MassCourts application, however, the policy and procedures need to be formally documented.

AOTC management has provided assurance mechanisms for the MassCourts rollout. IT management is also monitoring and evaluating performance of IT operations through the Help Desk by reviewing various incident reports captured through the HEAT (Help Desk Automation Tool) application system. Also, regarding monitoring and evaluation functions, the AOTC has developed reports on performance metrics to allow Trial Court management to measure and evaluate the activity of cases being cleared to the business objectives established by the Chief Justice for Administration and Management. As noted in the AOTC Metric Report, "The court metrics project represented an initiative aimed at enhancing the delivery of quality justice by systematically promoting the timely and expeditious disposition of cases by: establishing time standards for all court departments; adopting common metrics for measuring improvement on the timely disposition of cases; setting common, specific goals for each of these metrics across all court departments; and, producing regular reports on progress toward achieving the goals". We believe that the AOTC should expand responsibilities to include monitoring functions for data integrity, quality assurance, source document protection, as well as access and data security.

Regarding system access, although our current audit disclosed that AOTC has improved system access security control, controls for user account management related to password composition and frequency of password changes, and access to legacy systems needed to be strengthened. The Lightweight Directory Access Protocol (LDAP), is used by the TCIS as an authentication tool to confirm, on a regular basis with the state's HR/CMS system, that only authorized employees log into the system and have been allowed privileges to the network, email, Internet, or MassCourts application.

Although there were some documented controls and informal procedures in place for authorizing and maintaining user accounts, documented policies and procedures were not fully in place to provide adequate assurance that only authorized individuals would have the proper levels of access to automated systems and related data files. We also found that password standards needed to be established and documented, and once in place, should be monitored to ensure that user IDs and appropriate password standards are being followed. Current passwords for court employees are often not changed on a timely basis.

With respect to access security administration, the AOTC still needs to establish an access security management function to provide a single point of accountability for physical and system access security. This function would also help to provide reasonable assurance that security-related objectives will be addressed and ensure uniformity of practice and clear lines of responsibility.

With respect to virus and intrusion protection of the local area network, we found that the TCIS had installed centralized anti-virus controls and performs periodic network risk and security analysis. As the Trial Court continues to move toward a web-enabled application system, access security functions will need to be further strengthened in the areas of intrusion detection and prevention, application security, and 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. AOTC's internal control policy and procedures require completing an annual inventory including details for adequate information to be recorded on the inventory record. The AOTC policy directs responsibility for physical inventories and reconciliations to the individual courts and divisions. However there is no merging of the information received into a single comprehensive master inventory system of record that includes all IT-related assets. At the time of our audit, the records maintained in the Fiscal Affairs Department indicated that only 56% of the trial courts and divisions had filed the required annual physical inventory data. In addition, there is no review of the inventory records supplied by the courts and received by the Fiscal Affairs Department to verify that reconciliation has been properly completed.

Although the TCIS is responsible for the acquisition, installation, and accounting for IT resources, AOTC's inventory records maintained in the Fiscal Affairs Department did not provide AOTC management with adequate information to assure that all IT-related assets are properly recorded on the inventory record. Our test samples of computer hardware at the AOTC central office revealed that the inventory record lacked integrity as in many instances cost information was not recorded and the recorded location of computer equipment on the inventory was incorrect thereby increasing the risk of missing or misallocated computer equipment. Moreover, variances existed between the inventory system of record and the data collected on IT equipment connected to the network as provided through the LanDesk application. Due to the unreliable information on the LanDesk files, no further valid testing could be conducted. TCIS was conducting a full physical inventory of computer equipment to update their records at the end of our audit period.

Regarding business continuity and contingency planning, we noted that the AOTC does not have a comprehensive disaster recovery and business continuity and contingency plan for the AOTC's offices, Cambridge Data Center, and the Trial Court at large. Moreover, an alternative-processing site has not been designated to be used to regain processing should the Cambridge Data Center be damaged or inaccessible for an extended period of time. We note, however, that several initiatives were under way to address business continuity planning and reduce the risk of not being able to regain IT processing. The AOTC has implemented a number of new technologies and standards including a desktop backup infrastructure that facilitates the nightly backup of desktop data to a centralized infrastructure using EMC Centera archival disk storage. Also, the AOTC has made efforts to identify an alternate processing site(s) for the processing, storage and restoration of automated systems that support the AOTC and the Trial Courts. During this process TCIS management has assessed the relative criticality of their automated systems and conducted a risk analysis to determine the extent of potential risks and exposures to IT operations.

We continue to note that without a comprehensive, formal, and tested disaster recovery and business continuity 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. Until the recovery plans are formalized and in place, a significant disaster impacting the AOTC's automated systems could seriously affect the AOTC's and the Trial Court's ability to regain critical and important data processing operations.

MASSCOURTS ASSESSMENT AND STATUS

Our review of the MassCourts application system indicates that the system will serve as a comprehensive and integrated case management system for the entire Trial Court. Our assessment indicates that the rollout of the MassCourts application system is progressing in a systematic manner under the current leadership team at AOTC to ensure operational efficiency. The standardized data obtained through MassCourts will assist AOTC management in analyzing key metrics and allow management to respond in a more efficient manner to any changes or deviations affecting the delivery of timely justice across the trial courts. Trial Court Information Services (TCIS) has established project–specific quality assurance activities to help manage the rollout of the MassCourts application and has established formal monitoring and evaluation functions for the MassCourts activities. These functions have allowed the Trial Court management to assess whether MassCourts functions are working as intended to meet operational objectives within the Trial Court.

The MassCourts system was a concept that was initially conceived back in the mid-1990's. At the start of the Trial Court Automated Case Management Project, the professional consultant firm Deloitte was contracted to perform planning activities to assist the AOTC advisory board in deciding whether to buy or build a system. The initial decision was to build a system, which for a variety of reasons at the time, made the project very difficult. The decision was to develop an integrated system in a manner that all court staff and members of the legal community would use as a common platform, enabling information and data to be transferred across departments, and the courts would have the ability to maintain standard case management information.

During the initial stages, the focus was on developing the new system. The consultants established all the required definitions and captured all the business practices used in conjunction with the software acquisitions. In so doing the consultants laid the foundation for the development of a comprehensive case management system. The consultants also developed many of the interim applications, as many court departments did not have automated systems at the time of the project's initial start-up. The concept of transitioning from having no automated systems to having a sophisticated application such as the MAXIMUS application, with nothing in between, would have been very difficult. Therefore, the consultants delivered a series of interim application systems that were used to implement of the Court's basic automated systems. These basic court application systems provided a transitional platform that gave the Court tools to begin to capture case inventories, defendant inventories, and scheduling information. This basic information is now being used as input to the new, much larger comprehensive application. The consultants did assist with the planning and designing of the infrastructure that was installed at that time and still in use today. Because of the difficulties in trying to develop such a comprehensive case management system, AOTC management revised their initial decision and decided to purchase and modify a commercial case management application system to minimize future costs and stay within the limits of the original bond funds.

Initial spending against the bond funds of $75,000,000 started in fiscal year 1997 and was largely used for consulting services in the attempt to develop planned software for the Trial Courts. Other spending areas included computer hardware installed in many of the courts, network services, salaries and benefits, training, and administrative costs. According to the AOTC, at the time Chief Justice Robert Mulligan took office in October 2003, a decision had already been made to select MAXIMUS as the designer of the comprehensive case management system and spending against the bond funds through fiscal year 2003 was approximately $50,655,000, which included initial payments to MAXIMUS.

The organizational structure of the information technology function and project management at the AOTC was realigned under the direction of the CIO, Craig Burlingame. We found that the CIO provides oversight by meeting with key department management and staff on a regular basis and is advised by the Court Management Advisory Board. Judge James McHugh, who is a Judge on the Appeals Court, and has a strong background in technology, serves as special advisor to the Chief Justice for Administration and Management. These actions gave the IT department within the AOTC a new structure, as well as new leadership.

As of March 31, 2008 there are two versions of MassCourts, a “Lite” version and a full version. The Lite version of MassCourts, introduced into the District Courts, does not include docketing and case-related financial information, or many of the automated reports, notices and forms, which will be included in the full MassCourts version. The full version of MassCourts is operating in two court departments, the Land Court and the Housing Court, a total of six divisions, and was scheduled to be implemented in a third department, the Probate and Family Courts on June 16, 2008. MassCourts Lite is operating in 57 of the 63 divisions of the District Court and six of the eight Boston Municipal Courts. One of the Boston Municipal Courts is operating on the CourtView client/server. On the Probation side of the courts, 64 of the 105 divisions are operating under the Lite version of MassCourts, while one division is operating on the CourtView client/server.

From a control perspective, MassCourts has enabled the AOTC to systematically receive data for the production of management reports, and to monitor court activity and use metrics such as time standards. This data has allowed the Chief Justice to embark upon a court-staffing model, by empirically documenting the number of staff needed based on the volume of cases and the complexity of cases in each court. Working with the National Center for State Courts, a data-driven model has been developed The use of this data has underscored the importance of MassCourts which provides information to AOTC management in a more timely, consistent, and efficient manner.

The MassCourts project and rollout of the application system has progressed, supported by spending during the period fiscal 2004 through March 31, 2008 of approximately $19,870,000, bringing the total spending against the bond amount to about $70,525,000. This leaves an unexpended balance of approximately $4,475,000 of which $3,423,000 is encumbered to MAXIMUS in anticipation of its delivery of the remaining software and service deliverables required by the contract. As of March 31, 2008, there was approximately $1,052,000 available in bond funds. Since fiscal year 2004, the AOTC has attempted to stretch the bond funds by moving expenses to operating cost rather than to be charged against the bond funds. Since Court staff are currently using the MassCourts application, one of the transfers of expenditures from bond funds was a transfer of staff working on the technical development of MassCourts to being more appropriately funded by state payroll through the Trial Court budget.

To assess user satisfaction with the newly implemented application system, we developed a MassCourts user survey questionnaire that focused upon system response time, application functionality, pre-implementation training, IT support, user comfort level, and user satisfaction. The results of our MassCourts user survey initially indicated that some of the users interviewed in April 2007 found this application to be overly slow, especially during peak processing hours. Users indicated that this resulted in delayed processing of information or processes and caused some anxiety and stress upon the users attempting to complete daily functions. However, during our follow-up interviews in October 2007, the system response time had improved through changes made within the AOTC network. We also found at the time of our follow-up interviews that some users felt that there was still too much navigating to access and change data through the various MassCourts screens and that entering more information to the system was too time consuming. As one would expect, court staff who were more familiar with technology were able to attain a working knowledge of MassCourts quicker than staff who were not. The TCIS appeared to be well aware of barriers to “quick” implementations and developments, and developed training support to assist courts in implementing the system. The increased understanding of the issues surrounding systems implementations resulted in more realistic rollout schedules.

Our survey indicated that users at the District Courts initially felt that the classroom training provided to them was ineffective, in some cases, partially due to elapsed time between the classroom instruction and the system’s implementation. As a result of our feedback, the AOTC and the TCIS has added reference material in the form of detailed step by step procedures, on their network website, to address changes made to the application or when known problems or perceived problems arise.

Our review of the reference material, which has been added to the AOTC Intranet, appeared to address many of the problems brought to us by the users. However, during our follow-up interviews most of the users were unaware that the reference material was available on the Intranet. We recommended that TCIS work with and help the Administrative Office staff to inform the divisional personnel of the availability of the reference material and thereby build a stronger departmental sense of ownership. Many users gave high grades for the on-site training and support provided by local and regional support personnel.

Our interviews at courts revealed that many supervisors and managers were unaware of the detailed procedures of how the application works, or whether staff were properly entering the data in the system. Therefore, court management would be unable to answer questions or assist in the processing of information or adequate oversight of the staff. We have recommended improvements be made in the monitoring and evaluation of data integrity for information contained in the MassCourts application.

Users also brought to our attention a number of application process issues which in turn were brought to the attention of TCIS management. Many of these issues were reviewed and included in the updated reference material included on the Intranet. Other issues, isolated to one or two users, need to be addressed in re-training exercises. We recommend that TCIS work with the Administrative Office staff to coordinate retraining as appropriate. In a collaborative environment where IT Application ownership is a shared responsibility it's important that the Administrative Office and their departmental staff who may be the best trainers are owners of IT competence responsibilities.

Our follow-up questionnaire administered from a sample of courts visited five months after the initial surveys indicated that many of the staff were more comfortable with the MassCourts application and believed that information was being processed in a timelier manner. However, during our follow-up interviews, some staff indicated that they were still referring to paper documents for information contained in the MassCourts system. The reason for this action was that certain staff members were not sure if they were selecting the proper legal charges from the selections available in the application to match the information received from the courtroom. Some users felt that follow-up training to address any outstanding issues would be helpful now that court personnel had time to use and learn the system.

Our review of the current status of the MassCourts application rollout indicated that adequate project management controls were in place to support the continued implementation and future operation of the MassCourts application. We also determined that the controls provide reasonable assurance that project objectives would be met. We determined that adequate controls were in place and in effect for the project and adequate committee oversight of the MassCourts rollout was being provided.

As the MassCourts rollout continues, AOTC needs to fully develop appropriate internal control policies and procedures and incorporate security features into the fabric of the application to ensure compliance with the established standards. As the application is expanded across multiple departments of the Trial Court and the AOTC, it is essential that a court-wide security function be established to create, oversee and enforce policies dealing with data security and data integrity.

AUDIT RESULTS

1. IT Organization and Management

Our prior audit (No. 2002-1106-4T), issued June 22, 2004, indicated that although Trial Court Information Services (TCIS) had certain controls in place, the overall framework of controls pertaining to the department and the IT environment that it served lacked adequate policies 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, as well as the management of IT resources. Management control practices needed to be strengthened to provide more comprehensive guidance through documented policies and procedures and monitoring and evaluation mechanisms to provide reasonable assurance that control objectives would be met. Management is responsible to ensure 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.

Our follow-up evaluation of IT organization and management controls revealed that the AOTC had improved IT management and organization controls with respect to strategic planning, documented IT policies and procedures, risk assessment, organizational structure, monitoring and assurance, and relationship management. Although recognizable improvements have been made in control practices, controls require further enhancements, and procedures in place and in effect need to be more formally documented, and monitored and evaluated to meet IT organization and management control objectives. Formal documentation and monitoring and assurance mechanisms are necessary to ensure adequate understanding and compliance with IT policies, standards and procedures.

a. Information Technology Strategic Planning

The results of our prior 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. Regarding the planning process, the results of our current audit indicated that TCIS had developed IT-related strategic and tactical plans for the IT environment currently centered on the rollout of the MassCourts application. The CIO meets with key department management and staff on a regular basis, usually daily, and with lead staff on the MassCourts project on a weekly basis, and is further advised by the Court Management Advisory Board. TCIS is assisting in the process of performing a knowledge and skill assessment at all staff levels of the Trial Court to address competency and skill requirements for current and future IT and IT- related initiatives. The IT strategic planning process needs to encompass IT functions and activities that extend beyond those individuals under the MassCourts project. Although the MassCourts Project is the most significant IT effort underway, including all IT functions and activities in the IT strategic planning process will strengthen IT planning and management control. Strategic planning is an essential tool that supports an entity's accountability in the allocation of limited resources. Effective strategic planning should also direct the TCIS' actions and allow performance measurements, risk assessments, and assurance mechanisms to be used as effective management tools.

AOTC's current IT strategic plans need to encompass the following components:

- Statement of critical success factors for IT and TCIS.
- Statement of IT requirements to adequately support the enterprise's business objectives, and 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 judicial branch. The information architecture model should be cross-referenced to the established data classification scheme with respect to data sensitivity and privacy requirements.
- Forecast of internal and external developments that could impact the IT strategic plan.
- Acquisition and development schedules for the IT environment.
- Statement on operational, administrative, and quality service issues related to the Court's targeted IT environment taking into account recommended policies and procedures.

The AOTC and TCIS are effectively using management tools such as establishing milestone and performance measurements to manage the MassCourts rollout and operational areas, such as Help Desk functions. Performance measures are also providing management with metric-based feedback against which the progress of strategic initiatives for MassCourts is being evaluated. However, the lack of a comprehensive strategic planning process may hinder TCIS' ability to successfully address management's other business objectives and define future technological direction. 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.

As noted in our prior audit TCIS needs to develop a mission statement outlining its overall purpose and key duties. The statement needs to be enhanced to adequately identify the department's role in supporting enterprise-based management of IT across all courts and include establishing appropriate IT-related policies and guidelines, setting strategic direction for IT functions and configuration management, and providing oversight of IT activities beyond the MassCourts rollout. Although TCIS has established some limited policies to address the management of IT-related functions, the procedures and guidelines need to be more adequately detailed and include monitoring mechanisms to ensure compliance. The planning process should also address IT configuration management for all IT resources, including the computer systems and networks supporting the application systems.

b. Information Technology Policies and Procedures

Our prior examination indicated that adequate IT policies and procedures were not in place to provide statements of required action and guidance within TCIS and for guidance across the courts. Another concern identified during the prior audit was an inadequate internal control structure over and within IT activities.

Our current audit indicated that although AOTC has certain policies in place to help ensure operational efficiency and the ability to meet its primary business objectives, a complete set of formal policies and procedures for all IT functions have not been adequately documented in an internal control plan. At the time of our audit, AOTC did not have fully documented policies for all IT activities across the Trial Court that addressed topics such as access security and inventory control of IT resources. It is important to ensure that the fundamental cornerstones for an internal control structure are in place, namely stated control objectives and control practices and documentation. Examples of essential documentation that the AOTC needs to improve include:

- Comprehensive policies regarding access security for AOTC's key information systems.
- Comprehensive policies regarding IT inventory control and configuration management for AOTC and Trial Courts across the Commonwealth.
- Disaster recovery and business continuity and contingency plans for AOTC's applications and activities.
- Documentation of all IT standards and applicable quality review procedures for IT activities and functions.

While the lack of adequate documentation can result in the loss of departmental knowledge should key personnel terminate employment, it also represents insufficient guidance in areas where management direction should be articulated to minimize the risks of not addressing operational and control objectives. Documentation of key processes and activities within an administrative IT function helps to provide clear guidelines regarding their implementation and the expected results.

Risk Assessment

Our prior audit revealed that there was little or no evidence that the AOTC's TCIS or the Trial Court performed risk assessments of IT operations or the IT environment. At the time of our prior audit, the AOTC had no systematic approach to risk identification for IT functions or an established risk management function in place.

Our current audit revealed that the AOTC's TCIS has been using a systematic approach to risk identification for IT functions related to the MassCourts rollout and other operational areas within the

AOTC and the Trial Court, such as the establishment and implementation of the Worcester Data Center. Although risk assessments have been conducted, a comprehensive framework for conducting IT-related risk assessments should be established to provide a stronger base for risk management and control assessment. A comprehensive framework for conducting risk assessment 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 skill and knowledge requirements necessary to identify risks and vulnerabilities and assess IT and business impact. In this regard, policies, procedures, and defined responsibilities pertaining to IT-related risk assessment need to be established. Although the AOTC's Internal Control Guidelines state that risk assessment should be periodically performed, management had not required staff to use risk assessment as a tool to provide information for the design and implementation of IT-related internal controls, as well as monitoring and evaluation mechanisms. An effort should be made to ensure that IT-related risk assessment is part of the comprehensive risk management approach for operational areas and business processes 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 and business process owners, internal and external users, TCIS, and Internal Audit. The absence of a sufficiently comprehensive IT-related risk assessment framework and a risk management function limits the ability of the AOTC to adequately address internal control and ensure an overall coordinated strategy to mitigate and manage risk within the Trial Court's IT environment.

Documentation

In our prior audit we noted that although the AOTC did have certain IT-related control procedures, there was a significant lack of documentation for IT-related policies or procedures. Our current audit revealed AOTC had developed certain IT-related control procedures and had distributed them across the Trial Court system. However, our audit revealed that the AOTC has not sufficiently developed or documented IT policies and procedures for system access security, hardware inventory and IT configuration management, disaster recovery and business continuity planning, and certain aspects of IT-related organization and management, such as monitoring and assurance mechanisms. We do note that the TCIS has started to take on the task of developing, documenting, and promulgating policies and procedures relating to IT functions at the AOTC and across the Trial Court.

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. Documented IT policies and procedures also facilitate effective direction and adequate control. The lack of fully 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. 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.

c. <u>IT Organizational Structure and Human Resource Management</u>

Our prior audit noted that from a functional perspective, the TCIS’ 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.

Our current review of the TCIS indicated that a formalized organizational structure and an updated organization chart for IT-related functions were in place. In addition, we note that the TCIS organizational structure has been improved reflecting better focus on functional areas and the elimination of a separately managed Project Management Office under which MassCourts development had been assigned. The revised structure also reflects an improved management approach where centralized IT functions are far more coordinated with increased opportunity for collaborative effort. We found that IT functions and activities were performed within the framework of positions that is reflected by TCIS’ organizational chart and that TCIS job descriptions delineated roles, responsibilities, and reporting lines. The organizational structure properly addressed unity of command and had an established chain of command under the Chief Information Officer (CIO). IT functions within the TCIS were adequately established from an operational as well as a management control perspective. In addition, key elements such as the Court Management Advisory Board have improved the AOTC’s IT organizational structure by establishing an oversight mechanism and clearly defined reporting and communication lines with the TCIS by putting the project under the CIO.

<u>Enterprise Structure</u>

We found at the time of our prior audit, 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.

Since our last audit, the AOTC has reorganized the structure of TCIS that provides IT services to the AOTC and the Trial Court. Efforts have been initiated to define and communicate roles and responsibilities for IT-related functions and activities on an enterprise-based IT organizational structure. The overall organizational structure for TCIS has been reorganized to include IT operations and project management functions. Also, the AOTC has worked with the Trial Court to structure and train designated IT positions across the courts to address the requirement of the MassCourts rollout and related IT activities. Furthermore, during our audit we observed that management has established on-line courses for desktop applications available on AOTC's network and reference documentation to support the training needs of personnel using the MassCourts application. The AOTC, along with the Trial Court, has conducted a staffing analysis to identify staff training requirements in individual courts needed to support IT functions at a local level and be available to other staff to provide additional training and handle questions for court-based personnel on the MassCourts rollout and implementation.

As the use of the MassCourts application systems and related technology increases across the courts, AOTC management needs to continue to ensure that both TCIS and user community responsibilities include data integrity, source document protection, and access and data security. In addition, we found that formal relationships and defined points of accountability needed to be established among the functions for physical security, system access security, IT configuration management and fixed-asset accounting, and disaster recovery and business continuity planning.

d. Monitoring and Assurance

Our prior audit revealed that the 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.

Our current audit indicated that the AOTC has established policies and procedures for monitoring and evaluating IT controls that include functions to verify that controls are in effect and that control objectives for certain IT processes and activities are being met. These activities include portions of systems access security and Help Desk functions. The monitoring and evaluation controls that have been established and are in effect relate to management objectives for system access to the computer network, email, the Internet, and the MassCourts application. IT management has implemented adequate mechanisms to provide assurance to AOTC and Trial Court management that project management controls are in place and in effect for the MassCourts rollout. IT management is also monitoring and evaluating performance of IT operations through the Help Desk by reviewing various incidents captured through the HEAT application and recording the results in formal management reports.

We found however, that monitoring and evaluation criteria needed to be established to strengthen evaluation and assess compliance with IT policies documented to date within the TCIS and across the entire Trial Court. The effectiveness of IT-related internal controls should be monitored in the normal course of operations through management and supervisory activities, comparisons, reconciliation and other evaluation procedures, as well as, by the Internal Audit function. Deviations should be documented and result in further analysis and corrective action.

The AOTC's Internal Audit Department does not currently monitor or evaluate the controls or performance of IT operations and functions performed by the TCIS or by individual courts. The AOTC's Internal Audit Department has distinct knowledge about court operations including processing of financial transactions, has an increasing understanding of MassCourts, and is in a position as an audit function to evaluate IT-related controls. However, given that the Trial Court system is increasingly supported by information technology, the Internal Audit function should incorporate the review of IT controls and IT activities within its audit scope. The knowledge that AOTC's Internal Audit Department possesses would enhance the monitoring of data quality of case information connected to the MassCourts application and be helpful in preparing for financial modules to be included through the full version of the MassCourts application. Without monitoring and evaluation activities, such as assurance mechanisms and those that could be provided though Internal Audit, AOTC management cannot be adequately assured that appropriate management control practices for IT functions have been implemented, are consistently applied, and working as intended.

e. Relationship Management

During our prior audit we noted that based on interviews of AOTC's IT staff and input from various court staff, that the IT Department had not cultivated an adequate working relationship with the user community throughout the Trial Court system.

Based on interviews during our current AOTC audit and input from court personnel during our MassCourts surveys, we found that significant improvements have been made in relationship management, and that an improved working relationship has developed between TCIS and the user community throughout the Trial Court system. Current IT policies, procedures, and generally accepted IT practices, although limited, have been communicated to the AOTC staff and the Trial Court through the AOTC Intranet. Other initiatives that have strengthened the relationship between TCIS and the user community include creation of local user experts, provision of classroom and on-line training, expanded assistance through the Help Desk, and the establishment of the Court Management Advisory Board that includes system user perspectives from senior court management.

Recommendation:

We recommend that both AOTC and TCIS management continue to implement a comprehensive framework for establishing, maintaining, and monitoring IT internal controls. We recommend that continued effort be made to ensure that adequate and appropriate IT-related policies and procedures are in place that identify operational requirements and provide guidance for all IT functions and activities. Other essential policy and procedure documentation requiring improvement beyond the MassCourts rollout are in the areas of access security for AOTC's key information systems, contingency plans for AOTC's IT operations, inventory control and IT configuration management, technology and IT operational standards, and application quality review and monitoring procedures for systems and data.

Although long-term and short-term strategic planning for the MassCourts rollout is well documented, both IT long- and short- term strategic plans for other TCIS operations need to be further developed and documented. TCIS management, in conjunction with the AOTC and Trial Court management, should define and document a strategic information technology plan that includes other TCIS areas beyond the MassCourts project. From an IT governance perspective, the IT strategic plan should be aligned with AOTC's and the Trial Court's mission, goals, and strategic plans.

The absence of clearly defined and formally documented policies and procedures significantly inhibits their implementation. Furthermore, management should ensure that the documentation of IT policies and procedures, although improved since our prior IT audit report, be understood and accepted by all levels in the organization. In addition, management control practices should be established to ensure compliance with IT policies and procedures. We recommend that management establish milestones for the implementation and exercise of the policies and procedures as well as formal mechanisms and processes to monitor compliance with the established guidelines. The Internal Audit function should include IT functions in their scope of review and evaluation such audit areas as system access security, data integrity, and IT inventory control.

Auditee's Response:

> *We agree with this recommendation. As noted in the cover letter, much of our focus since the last audit has been on the establishment of new processes, the updating of infrastructures, and the implementation of MassCourts. We acknowledge that we now need to follow-up on many of these efforts to insure that in all cases we have created appropriate formal documentation and have considered appropriate methods for monitoring and compliance activities. Within the infrastructure area we have begun the utilization of an automated intranet based WIKI as a repository for key infrastructure documentation and notes. This allows all of the staff in the infrastructure group to access appropriate documentation which is being maintained within this online tool. We hope to*

> *expand the use of this tool further over time to allow ease of maintenance and ready access to important technical documentation.*
>
> *We acknowledge that a more complete strategic plan including the elements mentioned would be of value. We have made a conscious decision over the past several years to keep MassCourts as the key focal point of strategic advancement in the IT area. This will continue for the next few years. We believe that the MassCourts leadership group that has been established and has met regularly for the past several years could be an ideal group to use for input and validation of a broader and more comprehensive strategic plan.*

We agree with this recommendation. We do believe that since the prior audit we have increased the quantity and quality of IT documentation; however, there is still more work to be completed. As mentioned in item #8 above (see page 44)*, we have taken some steps to establish an electronic method for maintaining and accessing key infrastructure documentation. We believe that adequately addressing this audit finding will include not only the establishment of the documentation that is appropriate but also doing so in a way that will best facilitate its maintenance over time.*

As noted in your report, for our primary IT initiative, MassCourts, we have included risk assessments as part of our project planning agenda, and we believe this element of our activities has contributed to our success to date with the MassCourts implementations. We agree that the use of broader risk assessment strategies and components would have value. As we move to develop broader strategic IT plans for the Trial Court, we will insure that the use of a formalized Risk Assessment strategy is a component of these planning efforts. We appreciate the feedback and validation of the actions we have taken to improve the organization structure regarding the TCIS organization and the MassCourts project resources. We believe the current organization has been structured in a way that is better meeting the needs of the administrative office and of all Trial Court employees in the field.

In addition to those changes already made, we would like to note that over the past year we have been discussing the creation of a third Deputy CIO position in addition to the Deputy CIO for Support Services and the Deputy CIO for Infrastructure that exist today. This third Deputy would be the Deputy CIO for Policy and Planning. A review of many of the items in this most recent audit report is a further validation that establishing such a position to work with our CIO in these two critical areas is needed. We will be moving to finalize the establishment of this position in the near future.

We believe there are many opportunities to establish additional capabilities for monitoring and assurance related to IT systems and IT Policy. Some of this may be achieved by the new metrics initiative mentioned in response #12 (see page 45)*, some may be achieved by incorporating additional activities for our Internal Audit functions, and still others may result as a byproduct of the metric efforts already underway and referenced elsewhere in your report and this response thereto. We believe that MassCourts as an enterprise application will give us new and important ways to conduct centralized monitoring and assurance programs. There have already been a number of areas where we have been able to utilize information within MassCourts to validate that court personnel are completing requisite transactions consistently across court divisions. There have been other areas where new automated procedures have been established to insure that required activities occur consistently based on business rules.*

Auditor's Reply:

We commend the initial actions taken by AOTC to initiate corrective action based on our audit recommendations. We believe that by expending the scope of strategic planning and monitoring and evaluating activities to address IT functions in addition to the MassCourts project will help ensure that all IT functions and activities are being preformed in accordance with your established standards. We acknowledge AOTC's efforts for improving documented IT policies and procedures and agree that its efforts should continue in this area to ensure an appropriate level of IT governance and standards for IT activities. Coupled with these efforts, expanding risk assessment strategies and risk management will enable the Trial Court to continue to maximize IT value and provide secure and continuously available network systems.

Structural organizational changes such as the creation of a Deputy CIO should be correlated to monitoring and assurance functions related to the suggested policy and planning portfolio. The metrics initiatives will provide a solid foundation for improving and implementing assurance mechanisms throughout the Trial Court system. Continued support by AOTC senior management will ensure that IT organization and management controls are enhanced and continue to be aligned with AOTC's business objectives.

2. System Access Security

Our prior IT 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 to the AOTC's network and Trial Court application systems needed to be strengthened to ensure that only authorized users had access to systems and data files and that unauthorized access is prevented or detected.

Our current audit disclosed that adequate user account management controls were in effect to provide reasonable assurance that system users would be properly authorized to access the AOTC's network, email system, and the MassCourts application. Although we did not examine network security and firewall management, nothing came to our attention during our audit to indicate that there were material weaknesses in the area. However, access security needed to be strengthened regarding password composition, frequency of password changes, and access to legacy systems. Generally accepted security practices 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. Although access security policies and procedures have not been fully formalized and approved by AOTC management, control procedures were in effect and were being followed by TCIS in conjunction with individual courts to authorize, activate, modify and deactivate user privileges to the AOTC's network, email, and the MassCourts application, as well as to reconcile access user lists. However, there were no reconciliation procedures in place for access security to the legacy systems, such as ForeCourt, BasCOT, and the Warrant Management System (WMS). At the time of our audit, controls needed to be strengthened regarding timely deactivation of access to these systems until they are replaced fully by MassCourts.

We reviewed the automated procedures performed by the TCIS on a weekly basis to reconcile authorized users to AOTC's network, email and MassCourts application. The review by TCIS included a comparison of all Trial Court employees and authorized non-employees to the access file which lists the current network users, and a comparison of all Trial Court employees and authorized access non-employees to the access file which lists the MassCourts application user. We noted that an authorized users list generated from the system access file was run against the LDAP file created by the TCIS staff containing HR/CMS information compiled through the state warehouse on court employees. The names on the access list that did not match to the LDAP file were followed-up via email with management of the appropriate court location where the individuals were assigned. An email message was returned to the AOTC within one day with adequate information to resolve the variance. Based on a test of two randomly selected courts, we confirmed that all employees having access to the automated systems were properly authorized.

At the time of our audit the TCIS had developed several individual security profiles for the Housing Court Department's use of MassCourts. The logic for these profiles came from discussions with the Housing Court Local User Experts (LUE) and the AOTC's Internal Audit Department, and from knowledge gained from the MassCourts Lite process in the District Courts. Five levels of security were determined as needed for the initial rollout and will be adjusted for the courts once MassCourts is implemented. We found that TCIS had implemented standard access security profiles for the MassCourts application and had reassessed the use and control of super user accounts. We found that TCIS had limited the number of IT support staff assigned a "super user" profile that was needed to access security areas and to troubleshoot support calls. As the MassCourts rollout continues, AOTC management should ensure that IT responsibilities, duties and system access privileges of court personnel are reassessed and refined to match respective jobs and positions. Through the assistance of LDAP, TCIS has been able to deactivate security access privileges in a timely manner for users no longer needing certain levels of access, as well as those no longer authorized to access the network, email, the Internet, or the MassCourts application.

Although standard procedures for granting authorized users access privileges to the network's various applications have been updated, AOTC's policies and procedures do not adequately address data ownership, confidentiality of information, and the composition and frequency of change of passwords. Based on interviews with staff at various courts, we found that password policies were not known, that passwords had not been changed on a regular basis, and that generally accepted password administration and use guidelines were not followed. We found, during our interviews, that District Court personnel were not required to change their passwords on the AOTC network, and there was no indication that password administration was being monitored. Also, there was no documented policy in place to establish specific levels of authorization for users upon completion of the MassCourts rollout. 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. We continue to note that security as a process needs to become part of the business fabric and that enterprise security management techniques should be applied.

We recognize that AOTC has made an effort to document access security controls. For example, AOTC issued Information Technology Policy #1 on August 13, 2003, which formalized some policies regarding IT-related security for all Court employees, and AOTC's "Internal Control Guidelines Section 2.3.1" contain limited documented policies concerning password administration. While certain controls were documented, the policies need to be enhanced to adequately address password administration and access security over the legacy systems.

Recommendation:

In order to improve system access security controls at the AOTC, we recommend that management strengthen their access security framework to more fully incorporate generally accepted control practices. We suggest that AOTC consult sources for generally accepted security principles and practices, such as NIST, CobiT 4.1, ISO/IEC 17799, ISO/IEC 27001, and the Commonwealth's Information Technology Division's security policies and guidelines. The access security framework should be documented and include 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. Security management responsibility should be established at the organization-wide level to address risk assessment and overall security issues across the AOTC and the Trial Court. AOTC should identify requirements for a working relationship and points of accountability for those responsible for physical and access security to automated systems and supporting technology.

AOTC's IT access security policies and procedures should be clearly communicated to all court personnel and monitored for compliance. The policies and procedures for authorization and authentication should include the activation and deactivation process of users and levels of user privileges to the AOTC's network, email, MassCourts application system, and the remaining legacy systems. We further recommend that these documented policies and procedures adequately address data ownership, data classification, confidentiality of IT-based information, and password administration. To improve adequate password administration AOTC should 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. Password administrative policies should advise users not to write down passwords, share passwords, or include passwords in electronic transmissions.

To ensure appropriate user profiles, AOTC should establish and document the designated 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. The criteria for supporting different levels of security should be established and well documented to address web-enabled application systems and IT changes to the Trial Court's business environment.

We continue to recommend the appointment of a security administrator, or information security officer, 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 are not being changed on a regular basis, 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.

We continue to strongly recommend that AOTC establish an IT security awareness program to communicate IT security policy to each IT user and to 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.

Auditee's Response:

> *We agree that further refinements in password management on the internal Trial Court network would be appropriate. We believe we are utilizing best practice recommendations for password complexity, frequency of change, etc., on those systems that face the public Internet. As we complete all aspects of our LDAP implementation, we will be in a position to impose some of the recommended additional requirements internally through the windows desktop login process.*

> *We know that balancing password complexity, frequency of change, and other factors is a tricky proposition. Too frequent changes, or excessive complexity, can often result in users writing their passwords down. If this happens, and proper care is not taken to protect said passwords, these changes can actually reduce the quality of security and not enhance it. We value the input that has been provided in this area, and we are committed to making further changes in our security infrastructure that will enhance our overall security profile. As mentioned in your report, we have made great progress in this area, but we also know that there is more to do.*
>
> *The AOTC will review the recommended NIST, CobiT standards related to security policies and guidelines and where possible incorporate those standards and recommendations into revised security practices. We believe the previously mentioned online learning management system may be an ideal vehicle for the conveyance of additional information to all Trial Court personnel regarding security policies, responsibilities and standards. We agree that an aspect of all IT-related training in the future should include security awareness, password protection, etc.*

Auditor's Reply:

Due to the sensitive and confidential nature of data and information contained in the MassCourts case management system a comprehensive and documented access security framework is essential. We believe AOTC can enhance their access security policies and procedures by reviewing and further incorporating generally accepted security policies and practices. Incorporating security awareness through the on-going MassCourts training program will further support the enhancement of security practices.

3. Inventory Control and IT Configuration Management

Our prior 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.

Our current audit disclosed that AOTC needs to continue to strengthen inventory controls over IT equipment to provide reasonable assurance that the Court's computer equipment is properly recorded and accounted for and that the inventory system of record is monitored and maintained. Although we found AOTC had appropriate policies and procedures for ordering, purchasing, and receiving IT equipment, as well as having formal inventory control policies and procedures, the policies lacked adequate procedures for the monitoring and reconciling inventory records to ensure adequate data integrity. The AOTC's inventory system of record for property and equipment should include all IT resources located throughout the AOTC and all Trial Court locations and departments. Although it is required by AOTC policy that each court or department maintain an individual inventory record for local control, a central inventory system of record should be maintained by the AOTC's Fiscal Affairs Department.

Without complete inventory and reconciliation controls in place and in effect across the Trial Court, the AOTC cannot provide reasonable assurance that IT-related resources will be properly accounted for or reported on when needed. We found deficiencies in control practices, as evidenced by a lack of required physical inventory documentation for all courts and departments, inaccurate and incomplete inventory data on inventory records maintained in the Fiscal Affairs Department, and absence of reconciliation procedures.

The AOTC Internal Control Guidelines state, "All assets with a value over $100 must be inventoried on an annual basis and submitted to the AOTC Fiscal Affairs Department." The Fiscal Affairs Department has provided procedures and Microsoft Excel forms through the Trial Court Intranet for the recording of information to the inventory system of record. In addition, AOTC has provided an on-line tracking system to record and monitor the allocation and movement of fixed assets throughout the AOTC offices and court locations. The Fiscal Affairs Department has also made continued efforts during the audit period to collect and maintain inventory records. However, at the time of our audit only 56% of the individual courts or departments had submitted to the Fiscal Affairs Department completed inventories of computer equipment.

With regard to IT configuration management, TCIS has documentation to support the deprovisioning and disposal of computer equipment. In addition, through the use of the software application LanDesk, the TCIS was able to identify and monitor workstations and other IT equipment connected to the IT configuration and therefore available for IT operations. However, our tests of computer hardware inventory revealed that inventory control required strengthening due to the lack of certain information or occurrences of incorrect data in the system of record. For example, for IT equipment installed at the AOTC offices, the physical location stated on the inventory list reviewed frequently did not match the physical locations of the equipment on the floor. Our data analysis of the system of record determined that there were errors in identifying the location of certain computer hardware items. This appeared to be the result of inadequate tracking of the movement of computer hardware within the various courts and departments. In addition, the listing of IT equipment for the AOTC did not include acquisition and installation dates, value or historical cost, or the operational status for all computer equipment. This information is essential to adequately monitor the value and life span of computer equipment. Finally, due to the lack of detailed data in the records we were unable to determine the assignment of notebook computers to management and staff.

To test the accuracy of the recorded information on the records held in the Fiscal Affairs office, which AOTC deemed to be their official system of record, we selected the AOTC offices and divisions located at Center Plaza for our test sample. Using ACL we sampled 60 of 500 items and found that 24 of the items did not match the location noted on the inventory listing.

A further test was conducted comparing the list of 4,712 leased computers on the inventory list (maintained in the TCIS) to a listing of computers identified on the network through the LanDesk application. Only 1,832 could be matched, based on the information available on the two listings. We also noted that LanDesk information contained 3,464 cases where the number in the asset tag number data field was the same as the number in the serial number data field, and there were 2,021 blank spaces in the asset tag number data field. Due to the unreliable information on the LanDesk files, no further valid testing could be conducted.

Given the extent of the MassCourts Project, strict inventory control to support a higher level of IT configuration management is a critical success factor for the overall project. 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 rollout in process. A 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 hinders 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 organization-wide approach to IT configuration management hinders senior management and TCIS from making decisions regarding IT resource allocation, configuration change management, and version upgrades, as well as, patch management.

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 MassCourts application system, may be hindered. Complete formal 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. Accurate and complete inventory records, and associated data fields, are necessary to preserve the integrity of the inventory system of record. Otherwise, the inventory system could not provide Court management, or the Fiscal Affairs Department, with an accurate historic or current value for IT resources.

Recommendation:

We recommend that AOTC further revise and strengthen its current inventory policies and procedures to ensure that the Court's IT equipment is properly recorded, tracked and accounted for. These policies and procedures should be comprehensive, well documented (clearly communicated and understood by the user), and should include controls over IT equipment for the monitoring and reconciliation of inventory records to ensure adequate data maintenance. The reconciliation would involve the actual process of a physical count of IT items on a yearly basis, comparison to the previous year's inventory record to note variances. The variances should be identified using records of new items added to area, and disposed items removed from the court. Any variances not identified should be reported to Fiscal Affairs Department for proper follow-up and reporting.

We further recommend that the accounting of all IT equipment be a centralized function administered by the AOTC's Fiscal Affairs Department responsible for maintaining the official inventory system of record. All IT resources throughout the AOTC and all Trial Court locations and departments should be included in a detailed organization-wide listing maintain by the Fiscal Affairs Department from data supplied by each court and/or department required by AOTC policy to maintain an individual IT inventory record for local control.

We also recommend that the TCIS address IT configuration management by establishing a framework regarding the acquisition, identification, and maintenance of its IT infrastructure. The role of IT configuration management is important so that decisions regarding IT resource allocation, change management, version upgrades, and timely IT system assessments can be made.

Auditee's Response:

The AOTC Fiscal Affairs Department, in conjunction with TCIS, has implemented an electronic format (Microsoft Excel Spreadsheet) for the recordation of court and office assets on a standardized inventory listing. Increased efforts will be made to insure that the inventory listings are submitted to the AOTC in a timely manner on an annual basis. The submission of these inventory listings will allow the AOTC to create a database, that will contain a system-wide inventory listing. Additional instructions will be communicated to all courts and offices on reconciliation procedures necessary to solidify the accuracy of the central database.

Further, since the audit concluded, the TCIS organization has conducted a manual inventory of computer assets and has undertaken the initiative to utilize electronic data from a variety of sources (network scans, anti-virus software, online backups, etc.) to validate and monitor the inventory of network connected equipment within the Trial Court. We believe this effort will allow us to more accurately and quickly track IT assets that are connected to the state-wide network than would be possible using an annual physical inventory process.

Although we agree that greater inventory controls would be helpful, as it relates to the impact on MassCourts we believe the configuration management component considerations are minimal. Because the MassCourts application is web-based, the overall client configuration is minimal. A properly configured browser and acrobat reader are the only client components necessary to support the use of MassCourts. Obviously the presence of proper anti-virus software and other infrastructure considerations are important as well. We believe information available from the

LanDesk tool already being utilized can provide any needed information in support of this finding.

Auditor's Reply:

We are pleased that AOTC is taking further steps to strengthen the integrity of the fixed-asset inventory system of record for IT resources and improve inventory control policies and procedures. While the current software tools aide in managing IT resources, strengthening inventory control procedures will enhance resource knowledge for IT infrastructure management decisions. We agree with AOTC's plan to develop a master inventory system of record for all IT resources throughout the Trial Court system. We believe that controls to ensure adequate accounting of system-wide IT resources will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory and records of acquisitions and deletions (trade-in, loss, etc.) to the system of record. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for lost or missing IT equipment.

4. Disaster Recovery and Business Continuity Planning

Our prior audit report noted that the AOTC did not have a comprehensive, formal, and tested business continuity and disaster recovery plan or required user area plans. The AOTC's ability to regain critical processing capabilities and access information related to its various application systems at the time would have been impeded.

Our current audit determined that although the TCIS continued to have adequate on-site and off-site storage of backup magnetic media available for recovery efforts, improved backup of electronic media, and provisions to handle minimal alternative operations, the AOTC did not have a comprehensive business continuity strategy. According to the TCIS, workstation-based systems and data files that are backed-up are stored in two Trial Court facilities and synchronized in real time between the locations. This same storage infrastructure is being used to store the Probate and Family Court images of scanned documents. From our discussions with the AOTC's Director of Planning and Policy Development and the CIO, the development and drafting of appropriate user area plans and contingency planning to address the loss of centralized and local processing are in their preliminary stages.

While AOTC management is in the process of assessing the relative criticality of their operations, we found that in the event of a disaster, AOTC does not have a comprehensive approach to ensure the continuity of essential services. If a disaster should occur, there are no contingency plans developed by individual court departments to address critical functions throughout the AOTC and Trial Courts.

Based on interviews with senior management and reviewing current backup procedures, we determined that a written, tested business continuity plan was not in place to provide reasonable assurance that required IT processing and access to data files could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible. Although AOTC personnel were aware of the importance of the automated systems to court operations, a formal criticality assessment of application systems and IT risk analysis had not been completed. However, according to the TCIS a significant work has been completed to ensure that a recoverable database would be available upon demand as part of an off-site recovery strategy.

We determined that adequate controls over on-site and off-site storage of backup media were in place and in effect to assist recovery efforts when the alternative site is in place and formal policy and procedures are developed, and that the TCIS is now able to back all desktop information through a dual daily backup program. This daily backup would allow the TCIS to move the backed up data from a court (under limited disaster scenarios) to an available worksite with minimal downtime to allow the court to quickly recover operations. We also note that the AOTC has conducted and completed a study involving the movement of the primary data center and development and installation of a secondary data center. Further the AOTC has added the position of Director of Planning and Policy Development to develop business continuity plans for the Trial Court.

Our current audit continues to note that although the AOTC would be able to access backup data, the AOTC does not at this time have a designated or tested alternate-processing site should a disaster render the AOTC’s computer system unavailable or inaccessible. Given the absence of adequate business continuity plans, a significant disaster impacting the AOTC’s computer systems would seriously affect daily operations of the AOTC and the Trial Court.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the need for each entity to have an ongoing, business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, the organization should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

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 entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available. The AOTC should perform a risk analysis of the systems and clearly understand the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage the systems, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence.

Recommendation:

The AOTC should implement procedures to provide reasonable assurance that the criticality of systems is evaluated, business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the automated systems, and appropriate business continuity plans are developed for the applications residing on the computer systems. We recommend that senior management and key users review the computer environment and operations and perform a criticality assessment and risk analysis on the AOTC's automated systems. Based on the results of the assessment, the AOTC should proceed with the development of a written business continuity plan for its critical and essential functions.

The business continuity plan should document the AOTC's recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. Senior management should ensure that the written business continuity and contingency plan developed contains, at a minimum guidelines on how to use the continuity plan; emergency procedures to ensure the safety of all affected staff members; response procedures meant to bring the business operations back to their prior state or acceptable operational level before the incident or disaster; procedures to safeguard and reconstruct the primary site; coordination procedures with public authorities; communication procedures with stakeholders (employees, key customers, critical suppliers, and management); and critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.

We further recommend that procedures be developed to ensure that the criticality of systems is periodically reassessed; that the impact of changes in user needs, automated systems, or the IT environment is evaluated; and that staff are adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, and complete and remains viable. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel, and a complete hard copy of the plan should be stored in a secure off-site location.

Auditee's Response:

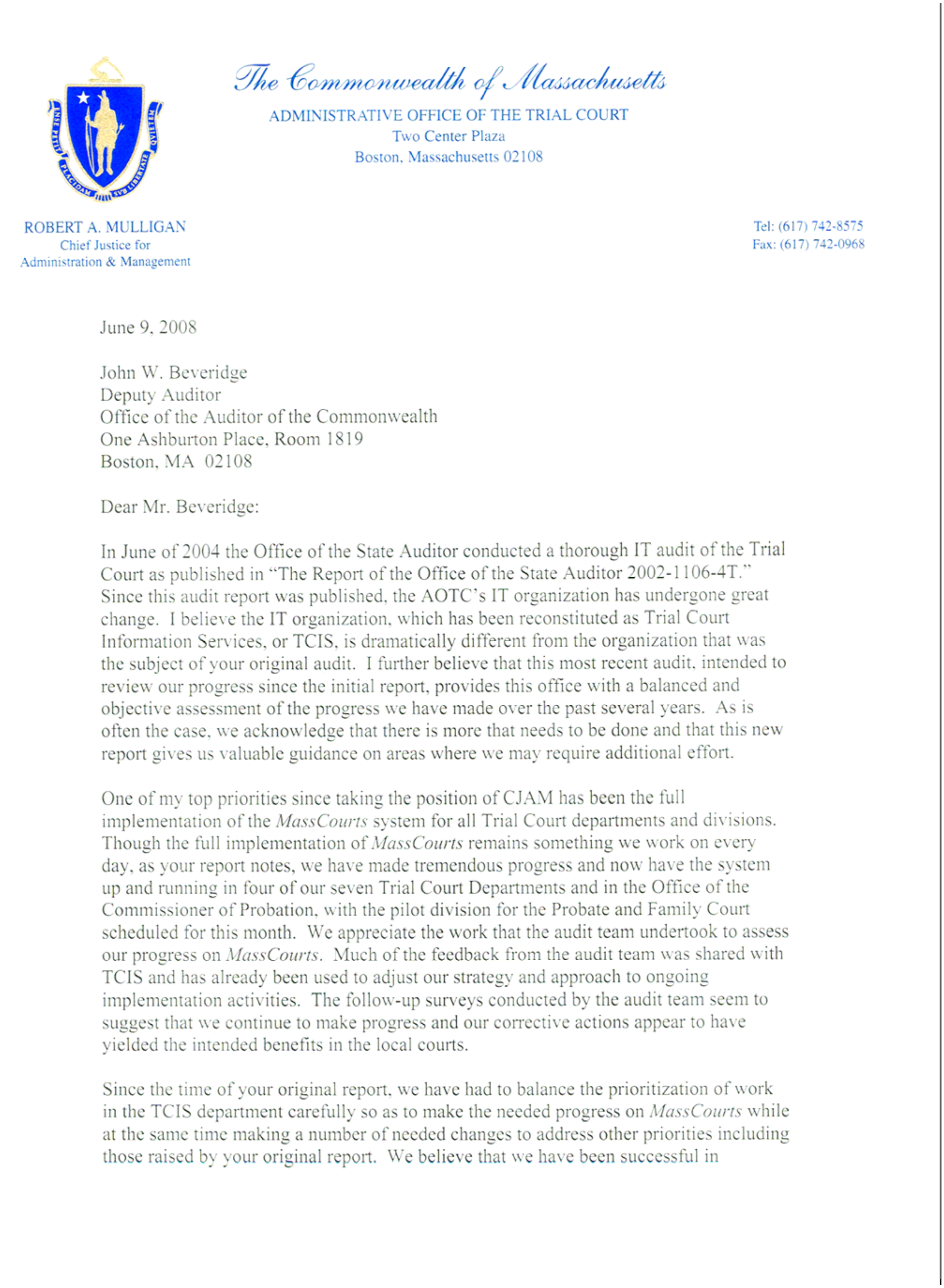
The AOTC understands and acknowledges the significant importance of both of these key plans. In the area of disaster recovery, as noted in your report, we have focused our efforts on the establishment of an alternative datacenter space in Worcester, and we have begun to populate that location with mission critical equipment that will be needed to establish our formal disaster recovery location. We will be working in the months ahead to complete the population of this datacenter with equipment and to complete the development of a formalized plan that outlines how this location would be utilized in the event of a disaster. In addition, we have worked closely with DCAM on the planning for, and the construction of, a new primary datacenter in the Boston area. The site location and engineering work on this initiative has been completed. Once this new construction is completed the AOTC will be able to have two fully operational state-of-the-art datacenters and a complete and comprehensive fail-over capability to use as part of our disaster recovery and coop plans.

Further, in the area of COOP, the Director of Policy and Planning in the Administrative Office is overseeing the development of a Continuity of Operations Plan. She coordinates her efforts with the Massachusetts Emergency Management Agency and the Supreme Judicial Court, as well as with the seven Trial Court departments and nine court administrative departments. All of the departments have outlined emergency requirements through a COOP survey. These responses are being coordinated and external expertise will be accessed, if needed, to develop a final court-wide COOP plan.

Lastly, as noted in your report, we have implemented an infrastructure for extensive online backups for Trial Court computers located throughout the Commonwealth. Using Connected, a software production from Iron Mountain Digital, over 5,500 workstations conduct an automated nightly backup of their content to central storage arrays located in two Trial Court facilities. This automated backup provides us with the capability to more quickly restore data that has been backed up from local desktops in the event of a serious event impacting one of the local courts. This capability, which has been added since your last report, will be a component of our Disaster Recovery and COOP Plans as they are finalized.

Auditor’s Reply:

We acknowledge the AOTC’s goal to document comprehensive plans for disaster recovery and business continuity and its efforts in establishing an alternate data center that will also serve as a formal disaster recovery location. In addition, the extension of automated nightly backup of AOTC and Trial Court workstations is a positive component of disaster recovery and business continuity planning. We believe, however, that until a comprehensive recovery strategy is documented and implemented, AOTC is vulnerable to a disruption in IT services. Once viable recovery and continuity plan are in place, the plans should be periodically reviewed and tested to provide an adequate degree of assurance of their continued viability.



The Commonwealth of Massachusetts

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

ROBERT A. MULLIGAN
Chief Justice for
Administration & Management

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

June 9, 2008

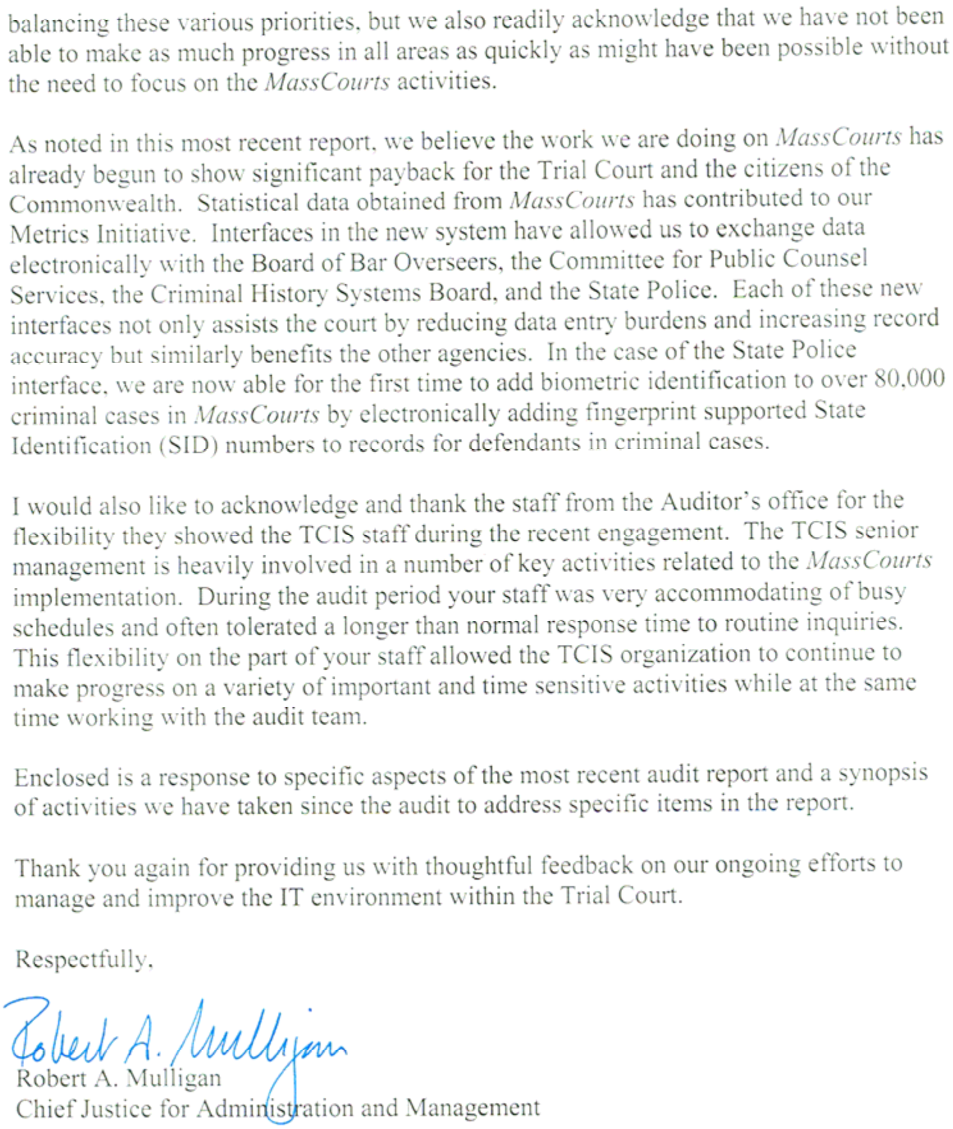
John W. Beveridge
Deputy Auditor
Office of the Auditor of the Commonwealth
One Ashburton Place, Room 1819
Boston, MA 02108

Dear Mr. Beveridge:

In June of 2004 the Office of the State Auditor conducted a thorough IT audit of the Trial Court as published in "The Report of the Office of the State Auditor 2002-1106-4T." Since this audit report was published, the AOTC's IT organization has undergone great change. I believe the IT organization, which has been reconstituted as Trial Court Information Services, or TCIS, is dramatically different from the organization that was the subject of your original audit. I further believe that this most recent audit, intended to review our progress since the initial report, provides this office with a balanced and objective assessment of the progress we have made over the past several years. As is often the case, we acknowledge that there is more that needs to be done and that this new report gives us valuable guidance on areas where we may require additional effort.

One of my top priorities since taking the position of CJAM has been the full implementation of the *MassCourts* system for all Trial Court departments and divisions. Though the full implementation of *MassCourts* remains something we work on every day, as your report notes, we have made tremendous progress and now have the system up and running in four of our seven Trial Court Departments and in the Office of the Commissioner of Probation, with the pilot division for the Probate and Family Court scheduled for this month. We appreciate the work that the audit team undertook to assess our progress on *MassCourts*. Much of the feedback from the audit team was shared with TCIS and has already been used to adjust our strategy and approach to ongoing implementation activities. The follow-up surveys conducted by the audit team seem to suggest that we continue to make progress and our corrective actions appear to have yielded the intended benefits in the local courts.

Since the time of your original report, we have had to balance the prioritization of work in the TCIS department carefully so as to make the needed progress on *MassCourts* while at the same time making a number of needed changes to address other priorities including those raised by your original report. We believe that we have been successful in



balancing these various priorities, but we also readily acknowledge that we have not been able to make as much progress in all areas as quickly as might have been possible without the need to focus on the *MassCourts* activities.

As noted in this most recent report, we believe the work we are doing on *MassCourts* has already begun to show significant payback for the Trial Court and the citizens of the Commonwealth. Statistical data obtained from *MassCourts* has contributed to our Metrics Initiative. Interfaces in the new system have allowed us to exchange data electronically with the Board of Bar Overseers, the Committee for Public Counsel Services, the Criminal History Systems Board, and the State Police. Each of these new interfaces not only assists the court by reducing data entry burdens and increasing record accuracy but similarly benefits the other agencies. In the case of the State Police interface, we are now able for the first time to add biometric identification to over 80,000 criminal cases in *MassCourts* by electronically adding fingerprint supported State Identification (SID) numbers to records for defendants in criminal cases.

I would also like to acknowledge and thank the staff from the Auditor's office for the flexibility they showed the TCIS staff during the recent engagement. The TCIS senior management is heavily involved in a number of key activities related to the *MassCourts* implementation. During the audit period your staff was very accommodating of busy schedules and often tolerated a longer than normal response time to routine inquiries. This flexibility on the part of your staff allowed the TCIS organization to continue to make progress on a variety of important and time sensitive activities while at the same time working with the audit team.

Enclosed is a response to specific aspects of the most recent audit report and a synopsis of activities we have taken since the audit to address specific items in the report.

Thank you again for providing us with thoughtful feedback on our ongoing efforts to manage and improve the IT environment within the Trial Court.

Respectfully,

Robert A. Mulligan

Robert A. Mulligan
Chief Justice for Administration and Management

Trial Court Responses to Specific Items in Report 2007-1106-T7:

#1, Page 12, with regard to “AOTC should assign responsibilities across the Trial Court to include evaluation of data integrity, quality assurance, source document protection, and access and data security”.

> The Trial Court has recently begun to pilot an additional performance metric based on the National Center for State Court *CourTools* standards related to “reliability and integrity of case files”. Additional details from the National Center are available here: http://www.ncsconline.org/D_Research/CourTools/Images/courtools_measure6.pdf
>
> This metric is being piloted in the Boston Municipal Court and involves a random sampling of 200 case files in each division, timing the retrieval of the physical file and further involves the validation of the files content. This validation is achieved via a comparison of the source document papers in the physical file with the case docket, and a validation that items on the docket are supported by the necessary source document papers. This initial pilot has been conducted in four divisions of the BMC and we expect to complete the remaining four divisions by the end of June 2008. We expect to learn from this pilot and we will be evaluating the potential to implement similar metrics in other locations in the coming years.

#2, Page 12, “However, we believe that security awareness training should be made part of current and future training programs”.

> As noted elsewhere in your report, TCIS has worked to establish online training content as part of the implementation activities for *MassCourts*. We believe our Online Learning Management system would be an ideal platform for establishing additional training components on “security awareness” and we will strive to do so as we develop additional online content in the future.

#3, Page 13, with regard to “We believe the AOTC should expand responsibilities to include monitoring functions for data integrity, quality assurance, source document protection, as well as access and data security”

> Additional information relative to this Item is covered in Item #1 above. As it relates specifically to our metrics initiative, we have discussed with the Court Management Advisory Board an initiative to validate the information submitted in support of our metrics program by conducting spot audits. We believe this effort, in conjunction with the additional *CourtTools* metrics on “reliability and integrity of case files” will further enhance the Trial Court’s confidence in the areas mentioned.

#4, Page 13, with regard to “the AOTC still needs to establish an access security management function to provide a single point of accountability for physical and system access security”.

> We agree with this recommendation in principle, and we recognize that the recommendation warrants further study and evaluation. We believe that since the prior audit we have made great strides, as referenced in your report, regarding our implementation of the single LDAP security directory which is integrated with the Commonwealth’s Human Resources System, HR/CMS. We know that the LDAP system has allowed us to insure that credentials used to access several key systems are always current. This method allows us to immediately withdraw credentials when an employee is terminated, update them when an employee changes positions, or add them when a new employee is hired. We believe this new infrastructure could be further enhanced by integrating it directly with the various systems that control physical security, and we will undertake a review of that shortly.

#5, Page 13, with regard to "As the Trial Court continues to move toward a web-enabled application system, access security functions will need to be further strengthened in the area of intrusion detection and prevention, application security, and access security administration"

> We agree with this recommendation. It is important, however, to note that the Trial Court utilizes the Information Technology Division of the Executive Branch as its Internet Service Provider. Without discussing the specifics in this public document, we do believe the ITD organization uses a quality Intrusion Detection System as part of operating our Extended DMZ which is exposed to the public internet. We also have made appropriate efforts to insure that any public internet facing infrastructures use a higher level of security including complex passwords, frequent password changes, etc. We will continue to review these practices to insure they offer the optimal level of security for Trial Court operated systems.

#6, Page 14, with regard to physical inventory and inventory controls.

> The AOTC Fiscal Affairs Department, in conjunction with TCIS, has implemented an electronic format (Microsoft Excel Spreadsheet) for the recordation of court and office assets on a standardized inventory listing. Increased efforts will be made to insure that the inventory listings are submitted to the AOTC in a timely manner on an annual basis. The submission of these inventory listings will allow the AOTC to create a database, that will contain a system-wide inventory listing. Additional instructions will be communicated to all courts and offices on reconciliation procedures necessary to solidify the accuracy of the central database.
>
> Further, since the audit concluded, the TCIS organization has conducted a manual inventory of computer assets and has undertaken the initiative to utilize electronic data from a variety of sources (network scans, anti-virus software, online backups, etc.) to validate and monitor the inventory of network connected equipment within the Trial Court. We believe this effort will allow us to more accurately and quickly track IT assets that are connected to the state-wide network than would be possible using an annual physical inventory process.

#7, Page 15 & 38 & 39, with regard to "We continue to note that without a comprehensive, formal, and tested disaster recovery and business continuity plan…"

> The AOTC understands and acknowledges the significant importance of both of these key plans. In the area of disaster recovery, as noted in your report, we have focused our efforts on the establishment of an alternative datacenter space in Worcester, and we have begun to populate that location with mission critical equipment that will be needed to establish our formal disaster recovery location. We will be working in the months ahead to complete the population of this datacenter with equipment and to complete the development of a formalized plan that outlines how this location would be utilized in the event of a disaster. In addition, we have worked closely with DCAM on the planning for, and the construction of, a new primary datacenter in the Boston area. The site location and engineering work on this initiative has been completed. Once this new construction is completed the AOTC will be able to have two fully operational state-of-the-art datacenters and a complete and comprehensive fail-over capability to use as part of our disaster recovery and coop plans.
>
> Further, in the area of COOP, the Director of Policy and Planning in the Administrative Office is overseeing the development of a Continuity of Operations Plan. She coordinates her efforts with the Massachusetts Emergency Management Agency and the Supreme Judicial Court, as well as with the seven Trial Court departments and nine court administrative departments. All of the departments have outlined emergency requirements through a COOP survey. These responses

are being coordinated and external expertise will be accessed, if needed, to develop a final court-wide COOP plan.

Lastly, as noted in your report, we have implemented an infrastructure for extensive online backups for Trial Court computers located throughout the Commonwealth. Using *Connected*, a software production from Iron Mountain Digital, over 5,500 workstations conduct an automated nightly backup of their content to central storage arrays located in two Trial Court facilities. This automated backup provides us with the capability to more quickly restore data that has been backed up from local desktops in the event of a serious event impacting one of the local courts. This capability, which has been added since your last report, will be a component of our Disaster Recovery and COOP Plans as they are finalized.

#8, page 21, with regard to "Formal Documentation and monitoring and assurance mechanisms are necessary to ensure adequate understanding and compliance with IT policies, standards, and procedures."

We agree with this recommendation. As noted in the cover letter, much of our focus since the last audit has been on the establishment of new processes, the updating of infrastructures, and the implementation of *MassCourts*. We acknowledge that we now need to follow-up on many of these efforts to insure that in all cases we have created appropriate formal documentation and have considered appropriate methods for monitoring and compliance activities. Within the infrastructure area we have begun the utilization of an automated intranet based WIKI as a repository for key infrastructure documentation and notes. This allows all of the staff in the infrastructure group to access appropriate documentation which is being maintained within this online tool. We hope to expand the use of this tool further over time to allow ease of maintenance and ready access to important technical documentation.

#9, Page 22, with regard to the establishment of a more complete IT strategic plan.

We acknowledge that a more complete strategic plan including the elements mentioned would be of value. We have made a conscious decision over the past several years to keep *MassCourts* as the key focal point of strategic advancement in the IT area. This will continue for the next few years. We believe that the *MassCourts* leadership group that has been established and has met regularly for the past several years could be an ideal group to use for input and validation of a broader and more comprehensive strategic plan.

#10, Page 23, with regard to "a complete set of formal policies and procedures for all IT functions have not been adequately documented in an internal control plan…"

We agree with this recommendation. We do believe that since the prior audit we have increased the quantity and quality of IT documentation; however, there is still more work to be completed. As mentioned in item #8 above, we have taken some steps to establish an electronic method for maintaining and accessing key infrastructure documentation. We believe that adequately addressing this audit finding will include not only the establishment of the documentation that is appropriate but also doing so in a way that will best facilitate its maintenance over time.

#11, Page 24, with regard to risk assessment.

As noted in your report, for our primary IT initiative, *MassCourts*, we have included risk assessments as part of our project planning agenda, and we believe this element of our activities has contributed to our success to date with the *MassCourts* implementations. We agree that the use of broader risk assessment strategies and components would have value. As we move to develop broader strategic IT plans for the Trial Court, we will insure that the use of a formalized Risk Assessment strategy is a component of these planning efforts.

#12, Page 25 & 26, with regard to IT Organizational Structure and Human Resource Management.

We appreciate the feedback and validation of the actions we have taken to improve the organization structure regarding the TCIS organization and the *MassCourts* project resources. We believe the current organization has been structured in a way that is better meeting the needs of the administrative office and of all Trial Court employees in the field.

In addition to those changes already made, we would like to note that over the past year we have been discussing the creation of a third Deputy CIO position in addition to the Deputy CIO for Support Services and the Deputy CIO for Infrastructure that exist today. This third Deputy would be the Deputy CIO for Policy and Planning. A review of many of the items in this most recent audit report is a further validation that establishing such a position to work with our CIO in these two critical areas is needed. We will be moving to finalize the establishment of this position in the near future.

#13, Page 27, with regard to Monitoring and Assurance.

We believe there are many opportunities to establish additional capabilities for monitoring and assurance related to IT systems and IT Policy. Some of this may be achieved by the new metrics initiative mentioned in response #12, some may be achieved by incorporating additional activities for our Internal Audit functions, and still others may result as a byproduct of the metric efforts already underway and referenced elsewhere in your report and this response thereto. We believe that *MassCourts* as an enterprise application will give us new and important ways to conduct centralized monitoring and assurance programs. There have already been a number of areas where we have been able to utilize information within *MassCourts* to validate that court personnel are completing requisite transactions consistently across court divisions. There have been other areas where new automated procedures have been established to insure that required activities occur consistently based on business rules.

#14, Page 30, with regard to "However, access security needed to be strengthened regarding password composition, frequency of password changes, and access to legacy systems…"

We agree that further refinements in password management on the internal Trial Court network would be appropriate. We believe we are utilizing best practice recommendations for password complexity, frequency of change, etc., on those systems that face the public internet. As we complete all aspects of our LDAP implementation, we will be in a position to impose some of the recommended additional requirements internally through the windows desktop login process.

We know that balancing password complexity, frequency of change, and other factors is a tricky proposition. Too frequent changes, or excessive complexity, can often result in users writing their passwords down. If this happens, and proper care is not taken to protect said passwords, these changes can actually reduce the quality of security and not enhance it. We value the input that has been provided in this area, and we are committed to making further changes in our security infrastructure that will enhance our overall security profile. As mentioned in your report, we have made great progress in this area, but we also know that there is more to do.

#15, Page 31 & 32, with regard to further security improvements

The AOTC will review the recommended NIST, CobiT standards related to security policies and guidelines and where possible incorporate those standards and recommendations into revised security practices. We believe the previously mentioned online learning management system may be an ideal vehicle for the conveyance of additional information to all Trial Court personnel regarding security policies, responsibilities and standards. We agree that an aspect of all IT-related training in the future should include security awareness, password protection, etc.

#16, Page 33 & 34, with regard to inventory controls.

Please refer to response #6. The Trial Court is committed to improving its physical inventory practices through a variety of methods outlined above.

#17, Page 35, with regard to "Given the extent of the MassCourts Project, strict inventory control to support a higher level of IT configuration management is a critical success factor to the overall project"

Although we agree that greater inventory controls would be helpful, as it relates to the impact on *MassCourts* we believe the configuration management component considerations are minimal. Because the *MassCourts* application is web-based, the overall client configuration is minimal. A properly configured browser and acrobat reader are the only client components necessary to support the use of *MassCourts*. Obviously the presence of proper anti-virus software and other infrastructure considerations are important as well. We believe information available from the LanDesk tool already being utilized can provide any needed information in support of this finding.