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. 2003-1221-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE SUFFOLK PROBATE AND FAMILY COURT

JULY 1, 2002 THROUGH MAY 8, 2003

OFFICIAL AUDIT REPORT

SEPTEMBER 30, 2003

2003-1221-4T

TABLE OF CONTENTS

	Page
INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	3
AUDIT SUMMARY	5
AUDIT RESULTS	7
1. IT-related Organization and Management	7
2. Business Continuity Planning	9
3. Appendix	13

INTRODUCTION

The Probate and Family Court Department, Suffolk County Division, is authorized by Chapter 211B, Section 1, of the Massachusetts General Laws. The Court, which is located in the Edward W. Brooke Courthouse, 24 New Chardon Street, Boston, Massachusetts, serves three cities and one town in eastern Massachusetts. The Court has jurisdiction over family-related matters such as divorce, child support, paternity establishment, family abuse prevention, elderly abuse prevention, abuse of the disabled, and adoption proceedings. The Court maintains exclusive jurisdiction over probate matters, such as wills, trusts, guardianships, and conservatorships. The Court consists of a First Justice, three Associate Justices, the Register of Probate, and seventy-eight employees.

Through the Court Reform Act, Chapter 478 of the Acts of 1978, the Administrative Office of the Trial Court (AOTC), previously entitled the Office of Chief Administrative Justice, was established to provide management and fiscal oversight to the seven trial court departments, including the Probate and Family Court Department and the Office of the Commissioner of Probation. The AOTC's Information Technology Department is located in Boston and provides technical support to individual courts. The AOTC also provides the courts with information technology (IT) resources, as well as guidelines for IT policies and procedures. The AOTC administers the Court's IT infrastructure, including mission-critical applications installed on AOTC's file servers located in Cambridge. In addition, at the time of our audit, the AOTC was in the process of establishing inventory records of IT equipment for the courts under its jurisdiction. At the Chief Justice's direction, the Fiscal Affairs Department has promulgated accounting policies and procedures that comprise the Trial Court Standard Accounting System.

At the time of our audit, the Court's computer operations included 70 workstations in the Register of Probate's Office and 27 in the Probation Department, two workstations in a courtroom, and two workstations in a public area in the Clerk's Office. The Court also had two routers and switching networking equipment functioning as the center of communication activity through which all 101 workstations were connected in the courthouse. A line-of-site laser on the roof of the Courthouse beams a signal to the AOTC's Information Technology Department data center in Cambridge allowing connectivity to the AOTC wide area network.

The application systems used by the Court reside on AOTC file servers located in Cambridge. The application systems used by the Court are the Basic Court Operation Tools (BasCOT) system, which is used to record docket information; the Warrant Management System (WMS), which is used to track outstanding warrant information; and the Probation Receipts Accounting (PRA) system, which includes an account for court-ordered alimony payments. In addition, the Probation Department uses the Criminal

Activity Record Information (CARI) system to access information on all cases involving guardianship or restraining orders. The Court's Register of Probate maintains an Internet web site, www.probatecourtiannella.com, which includes downloadable forms, interactive surveys, and a virtual tour of the Court.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the Court's IT environment.

AUDIT, SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

From January 27, 2003 through May 8, 2003, we performed an audit of certain information technology (IT) related controls at the Suffolk Probate and Family Court for the period covering July 1, 2002 through May 8, 2003. Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security and environmental protection for areas housing IT resources, business continuity planning, generation of on-site and off-site backup copies of magnetic media, and the backup and storage of hardcopy files.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control environment, including policies, procedures, practices, and organizational structure provided reasonable assurance that control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to provide a clean and secure environment and to prevent damage to, or loss of, computer equipment or IT-related assets.

We also sought to determine whether an effective business continuity plan had been implemented to provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period should a disaster render the automated functions inoperable and whether adequate provisions were in effect for on-site and off-site backup media to assist recovery efforts. We also sought to determine whether hardcopy files were being backed up.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, interviewing senior management regarding the Court's IT control environment and performing a preliminary review and evaluation of certain IT-related internal controls. To obtain an understanding of the Court's activities and internal control environment, we reviewed the Court's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT general controls.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation, and assessed relevant IT-related internal controls. Although our

review was limited to the Court's IT operations, we reviewed the degree of documentation the Court had received from AOTC regarding IT policies and procedures.

To determine whether adequate physical security and environmental protection were in place and in effect within the Court to prevent damage to or loss of IT-related equipment, we inspected the telecommunication and server room and areas where IT resources and workstations were located. We also interviewed the Director of Security and inspected the security office where closed circuit television cameras are located. We also interviewed the Director of Facilities Management, observed and evaluated the adequacy of certain environmental protection controls, such as water and smoke detectors, fire suppression measures, an uninterruptible power supply, and general housekeeping for all areas housing IT resources, including the Fire Command Center and fuel storage area for the backup generator. We confirmed the existence and functionality of the main and local controls of the heating, ventilation, and air conditioning system (HVAC). We also observed the water shutoff valves for the water flow alarm system and sprinklers located in the stairwells (North, South, East, and West) of each floor in the courthouse.

To assess the adequacy of business continuity planning, we determined whether any formal recovery planning had been performed to resume computer operations supported through AOTC's data center should access to, or processing capabilities for, the BasCOT, PRA, WMS, and CARI systems be lost for an extended period. With respect to business continuity planning, our interviews were limited to management and staff from the Court and AOTC. We interviewed the Court's and AOTC's senior management as to whether the criticality of application systems had been assessed, risks and exposures to computer operations had been evaluated, and a written, tested business continuity plan was in place and in effect. Although we did not review business continuity planning with AOTC staff, we inquired whether the Court had been provided a strategy from AOTC regarding recovery and processing of AOTC-supported mainframe applications and data. In addition, to evaluate the adequacy of controls to protect data and information through the backup of on-site and off-site magnetic media and hardcopy files, we interviewed Court staff, as well as AOTC, regarding the generation and storage of backup copies of computer-related media and hardcopy files.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry practices.

AUDIT SUMMARY

Based on our audit at the Suffolk Probate and Family Court, we found that adequate controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to physical security, environmental protection, and generation of backup copies of magnetic media for on-site and off-site storage. However, our review of the controls over IT organization and management and business continuity planning at the Court indicated that controls should be strengthened by documenting IT-related control policies and procedures and by developing and implementing a comprehensive business continuity strategy in conjunction with the central office of the Administrative Office of the Trial Court (AOTC).

Our review of the Court's organization and management over IT-related activities disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC. Although job descriptions for staff existed at the Court, they did not include reference to IT-related responsibilities where applicable. Our examination of the Court's organization and management revealed that there was an established chain of command and adequate segregation of duties among Court employees. Our review of IT-related activities disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC. Although there was no established IT function at the Court, two employees served, in addition to maintaining their regular Court responsibilities, as the liaisons between the Court and AOTC regarding IT-related issues. Given that AOTC had not defined IT-related areas of responsibility for the Court or communicated required IT policies and procedures, Court personnel were unaware of certain responsibilities and control practices and did not have clear operational standards and guidance on which IT related tasks and activities should be performed. We found that although certain control procedures did exist, there was a general absence of documented IT policies and procedures and IT general controls to address IT functions performed at the Court.

We determined that adequate physical security controls were in place to safeguard IT-related resources in both the Register of Probate's Office and the Probation Department. All visitors must pass through a metal detector and a hand-held wand inspection when entering the Court. All packages must pass through an X-ray machine, and all activities are under closed circuit surveillance. We found that areas housing computer equipment were inaccessible by the general public and were staffed by Court employees. The only exception was that two workstations were located in the Clerk's Office from which docketing information is made available to the general public.

Our review revealed that there were adequate environmental protection controls in place and operating within the Court's offices and the area housing the computer room with respect to general

housekeeping, heating, ventilation, and air conditioning, emergency lighting, smoke, heat, and water detectors, and a fire alarm system that was connected to the local fire department.

Our review of business continuity planning indicated that the level of planning needed to be strengthened. Our audit revealed that the Court, in conjunction with AOTC, had not documented a formal and comprehensive business recovery strategy for mission critical and essential application systems residing on AOTC's file servers in Cambridge. In addition, we found that the Court in conjunction with AOTC, had not performed a criticality assessment of application systems and assessed their associated risks.

Although backup procedures appear to be in place for the mission-critical applications operating on the AOTC's file servers and mainframe computer in Cambridge, we found that backup procedures for certain hardcopy standard forms and Court-related documentation were not in place. Although we realize the Court has microfiche and imaging capacity for most current Court documents, older documents and other Court materials supporting case management may not be recoverable if originals are destroyed or lost. As a result, important documents could not be recovered if they were destroyed, and added costs would be required to recreate these standard forms or reconstruct related information. Importantly, the Court needs to address the risks of not being able to recover and process information within an acceptable period of time or incur unnecessary data or system reconstruction costs. The Court, in conjunction with AOTC, should implement a comprehensive business continuity strategy and disaster recovery plan to help ensure system availability and resumption of IT operations within an acceptable time frame should IT processing be rendered inoperable or inaccessible.

AUDIT RESULTS

1. IT-related Organization and Management

Although our audit revealed that the Court had certain IT-related general controls in place, control practices needed to be strengthened by having IT-related policies and procedures formally documented to provide sufficient guidance for performing certain functions and operations. Since IT operations are limited and are supported by centralized AOTC-based systems, the extent of required documentation for IT-related functions should be evaluated and prepared in conjunction with AOTC. While we acknowledge the Court's difficulty in allocating limited staff resources to document IT-related policies and procedures, we believe that overall control practices would be strengthened by documenting policies and procedures regarding physical security, environmental protection, business continuity planning, system access and password security, and hardware and software inventory control. Although we found that the Court did provide policies and guidelines regarding authorized and acceptable use of IT resources, the Court would benefit from having a comprehensive set of written IT policies and procedures to ensure that important operational and control objectives would be met. Documented procedures might also cover information technology planning, risk assessment and risk management, data management for the various application systems, virus protection, access security, training, monitoring and IT reporting activities.

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

In the absence of formal standards, policies, and procedures, employees may rely on individual interpretation of what is required to be performed or how to best manage and control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result, and key control objectives may not be adequately addressed. Also, management may not be adequately assured that desired actions will be taken. Furthermore, the absence of documented policies and procedures undermines management's ability to monitor and evaluate IT operations and application systems because of the absence of stated internal controls and required audit or management trails. In addition to generally

accepted control practices, documented and approved control procedures are required of all state agencies under Chapter 647 of the Acts of 1989.

Recommendation

We recommend that the Court, in conjunction with AOTC, should begin documenting its IT-related policies and procedures to provide sufficient, formal guidance for IT-related tasks and activities. Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken and that undesired events are prevented and detected and, if detected, that corrective action is taken in a timely manner. Control practices would be strengthened by written IT-related policies and procedures regarding physical security, environmental protection, access security and password administration. Since documented policies and procedures provide guidance for functions and activities and a basis for evaluation, they help to ensure that important operational and control objectives would be met.

Auditee's Response

> *…the Suffolk Registry relies on the AOTC and the IT Division, as part of their core missions, to ensure that such plans are in place and to share them with all court divisions.(The) Chief Information Officer has been fran kand honest in stating that no disaster recovery plan exists… and that formal documentation of many IT-related policies and procedures is lacking. He has accepted responsibility, and is currently drafting these policies as quickly as possible.*
> *(The) Chief Information Officer has been made fully aware of the findings and recommendations included in the draft audit report, and we are confident that his commitment to resolving each of these issues in a timely fashion is a solid one. In our discussions, he has agreed that the AOTC and the IT Division have the ultimate responsibility for most of the deficiencies listed in the audit report, and has agreed to keep the Registry informed as he works to correct these and other problem areas.*

Auditor's Reply

Documented controls, policies, and procedures provide a framework to guide and direct staff in the discharge of their responsibilities. The nature and extent of the documented control procedures also needs to accommodate staff experience, competency and knowledge. It is our hope that the development of documented policies and procedures for the Court's IT environment would be done in conjunction with implementing the new MassCourts application.

2. Business Continuity Planning

Our audit revealed that the Court and AOTC had not collaborated sufficiently to develop and test a formal business continuity plan that would provide reasonable assurance that critical data processing operations could be regained effectively and in a timely manner. Further, the Court had not assessed the relative criticality of the automated systems to determine the extent of potential risks and exposure to business operations. Although we realize the Court has microfiche and imaging capacity for most current Court documents, older documents and other Court materials supporting case management may not be recoverable if originals are destroyed or lost. We also found electronic data files for the CARI, WMS, and PRA applications were maintained and backed up through the central AOTC office. In the Register of Probate's Office, although certain hardcopy files were being backed up through imaging or scanning, not all hardcopy files would be recoverable. Our audit revealed that the Court, in conjunction with AOTC, had not developed a comprehensive business continuity strategy, including user-area contingency plans for the Court, testing of the plan, and recovery strategies to the extent possible to recover hardcopy court files in the event of a loss of automated processing.

We acknowledge that AOTC is responsible for developing and testing a formal business continuity and contingency plan to restore automated functions in a timely manner. Without a comprehensive, formal, and tested recovery and contingency plan, including required user area plans, the Court's ability to access information related to the Warrant Management System and BasCOT applications operating on the AOTC's file servers, and the CARI and PRA systems operated by the Commissioner of Probation would be impeded. Without access to these applications, the Court would be hindered from obtaining information regarding outstanding warrants related to court cases and case docketing information, the Court would be unable to confirm that fines, fees, and penalties were being collected by the Probation Department or to access all trial court dispositions regarding criminal cases. Given the absence of recovery plans, a significant disaster impacting the Court's automated systems would seriously affect the Court's ability to regain critical and important data processing operations. Business continuity and contingency planning has taken on added importance given the potential processing disruptions that could be caused by man-made events.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe

the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

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 Court, in conjunction with 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.

Generally accepted practices and industry standards for computer operations support the need for each entity to have an ongoing, business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. Therefore, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

We believe that AOTC management has not emphasized to each court the importance of developing an individual business continuity plan to detail steps to be taken should automated systems become unavailable for an extended period of time. In addition, according to Court management, sufficient resources were unavailable to make business continuity planning a priority.

Recommendation

The Court, in conjunction with AOTC, should document their disaster recovery strategy and prepare a written disaster recovery and business continuity plan that incorporates user area plans. The disaster recovery plan should focus first on those automated systems that are mission-critical to the business objectives and operations of the Court.

Management should establish an ongoing contingency planning process that periodically reassesses the relative criticality of automated systems and the IT infrastructure and their associated risks, and update recovery and business continuity plans accordingly. We recommend that a risk analysis be performed on the Court’s information technology environment on an annual basis, or upon major changes to systems or the IT environment. An impact analysis of the denial of processing functions should be performed in conjunction with the risk analysis.

The Court should develop appropriate policies and procedures to support disaster recovery and business continuity planning, which address recovery and operational objectives, procedures, assignments of responsibilities, controls, monitoring and evaluation, and security measures. We further recommend that the disaster recovery and contingency plan be periodically reviewed and tested to ensure that it is current, accurate, and complete. The results of all tests should be documented and maintained and copies of the recovery and business continuity plan, including user area plans, should be stored in the off-site location. The plans should be communicated to all responsible parties and those individuals who are assigned disaster recovery and business continuity responsibilities and have sufficient skills and knowledge to carry out their responsibilities.

Lastly, to ensure that sufficient recovery plans and procedures are in place for continued availability of mission-critical and essential IT-supported services, we recommend that a policy statement be documented and distributed outlining management's commitment regarding disaster recovery and business continuity planning. AOTC should communicate to each court the importance of establishing an individual continuity plan for their critical business functions. In addition, AOTC should provide the necessary resources to ensure that business continuity plans are developed and implemented. The plan should also be periodically assessed and amended as the technology changes.

Auditee Response:

> *The Suffolk Registry relies on the AOTC and the IT Division, as part of their core missions, to perform such functions and ensure that such plans are in place. In turning to (The new) Chief Information Officer for assistance in responding to the audit findings, the Registry learned that no such disaster recovery plan exists. Just six weeks on the job, (the)CIO has made the development and implementation of an IT disaster recovery plan a top priority, and is expected to have this plan completed within days. He will communicate this information to all court divisions in writing and through the Court's Intranet site to ensure that the plan is implemented as quickly as possible.*
> *In order to perform court functions and serve the public should a disaster result in the closing of the Edward Brooke Courthouse, the Suffolk Registry would turn to the Middlesex Registry of Probate for assistance and support. Little more than a mile from our current location, the Cambridge courthouse would serve as a temporary office for essential Suffolk Registry staff and the public. We will work with the Middlesex Register of Probate to further detail and formalize this business continuity plan.*

Auditor's Reply:

We acknowledge that the need to have recovery and contingency plans in place has been recognized to assist in regaining mission-critical operations should technology be significantly damaged or be inoperable for an extended period of time. Considering that the primary processing capabilities are

external to the Court, business continuity efforts must take into consideration what will be provided to, or required of, the Court for each of AOTC's business continuity strategies.

Although a formal and comprehensive business continuity plan for all IT operations across the courts would have to be developed by the AOTC in conjunction with the courts, much of the preliminary evaluations of the criticality of IT processing and on-line availability of data and the impact on operations resulting from a loss of IT capabilities should be assessed within each court. While we acknowledge the existence of some procedures encompassed within a business continuity strategy, a formally documented comprehensive plan is necessary to ensure system availability due to loss of IT processing capabilities. At the start, business continuity planning requires a series of evaluations, including a criticality assessment and risk assessment for all operations that are enabled or supported by technology. The development of recovery or contingency strategies to address the Court's operations will require a collaborative effort between the Court and AOTC's IT Department. Recovery strategies may involve using locally-generated backup media and an alternate processing site. The Court should also identify and assess the importance of hardcopy files and adopt monitoring procedures to identify the age of documents and to consider placing documents in State Archives when applicable. The Court, in conjunction with AOTC, should evaluate the risk of being unable to retrieve essential original Court-related documents.

Although we acknowledge that the court is making a good effort to create backup copies of current hardcopy files, we feel there is still a danger of losing original documents for older case management information.

Appendix

August 25, 2003

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

Dear Mr. Beveridge,

I write to present the Suffolk County Probate and Family Court Registry's response to your draft audit report, and welcome the scrutiny that such a detailed review and independent evaluation of our operations provides.

When I first arrived at the Registry six years ago, there were only four outdated computers in our office and no electronic method to track cases. Much of the court's work was still being done using typewriters. With some vision and determination, the turnaround was remarkable as we quickly joined modern times. Our computerized indexes now go back thirty years, all court forms are generated electronically, and BasCOT performs multiple functions including judge's scheduling. Taking the next major step forward, the Trial Court has contracted with Maximus Justice Solutions of Canton, Ohio to develop and implement *MassCourts* - an Internet-based system that will provide Court administrators with one unified system to track cases as they progress through the system. The Boston Municipal Court will be the first to launch the new system this fall.

Despite little in the way of resources and support from the IT Division in the past, the Registry has been able to make numerous independent advances that are of great benefit to the court and the public. (These technological advances will be listed in detail in our response.) From scanning and digitizing all recent case files to development and maintenance of a popular Internet Web site, we are clearly light years ahead of other court divisions in Massachusetts.

As 96% of the Suffolk Registry's overall budget is specifically earmarked for employee salaries, it is difficult, if not impossible, for the Registry to act alone in putting many of your recommendations in place. We do not have the on-site expertise to develop IT-related policy and procedure, nor do we have the ability to hire additional staff for that purpose. I am also concerned that your report suggests that the Registry is responsible for deficiencies when, in fact, the Registry is at the will and mercy of the AOTC and the IT Division. From the start, it has been my belief that the audit report should be directed to these authorities rather than to me as a Register of Probate. After all, with over 150 separate court divisions, it only makes sense that the system be unified rather than asking each division to formulate its own set of policies and procedures.

In preparing this response, I asked the IT Division's new Chief Information Officer for copies of disaster recovery plans, daily backup procedures and other documents deemed critical by the audit team.(The) CIO admitted that they simply do not exist. He is currently drafting these policies and has vowed to make compliance with audit findings a top priority. Since (the CIO) was appointed six weeks ago, we have noticed a remarkable change in the manner and approach taken by the IT Division. We have had open and frank discussion of various issues including the draft audit report, and I am confident that (the) CIO will act quickly and decisively to resolve your concerns.

In turn, I ask the state to provide me with copies of disaster recovery and business continuity plans that would be used if a large-scale disaster befalls the Commonwealth. I question whether or not such documentation exists on this level, and firmly believe that the state's Information Technology Division should be charged with developing and implementing such plans instead of asking each state agency to act independently of the other.

Once again, I commend the Office of the Auditor of the Commonwealth and the audit team for their professionalism and attention to detail throughout the audit process. I am confident that your report, coupled with new leadership and new lines of communication between the Registry and the IT Division, will benefit the Trial Court, court employees and the taxpayers of the Commonwealth in the future.

Very Truly Yours,

Richard Iannella, Register

cc: Chief Justice Sean M. Dunphy
First Justice John M. Smoot
CIO John Beaton, Jr.

Appendix

INTRODUCTION

- "*The Court consists of a First Justice, three Associate Justices, The Register of Probate and seventy-eight employees."*

The Audit Team has included the Probation Department / Family Services Office within this count, and included the Probation Department as part of the Registry's information technology audit. The Probation Department falls under the jurisdiction of the Office of the Commissioner of Probation and is not answerable to the Register of Probate. Any existing ties between the Registry and the Probation Department (shared payroll and purchasing functions, etc.) were officially severed as of July 1, 2003.

- *"The court's Registrar maintains an Internet Web site, www.probatecourtiannella.com, which includes downloadable forms, interactive surveys and a virtual tour of the court."*

Because the Trial Court has not permitted individual court departments to develop or maintain Internet Web sites, I have privately funded the Suffolk Registry site in order to provide the public with helpful resources and information. Simply by scanning and posting several dozen of the most commonly used court forms on-line, attorneys and pro se litigants are able to save a trip to the courthouse, while the state saves on printing costs. Self-help kits, brochures and other detailed information about various aspects of probate and family law are also available on the popular site (so popular, in fact, that more than 15,000 'hits' were recorded the first day after announcing that a list of 'missing heirs' was available on the site).

For several years now, various Trial Court committees have discussed expansion of the existing Trial Court Web site to include information more useful to court clients. While the issue continues to be studied and an interactive form isn't anywhere to be found, a new brochure or pamphlet trickles onto the existing site once or twice a year. Facing this frustration, many other Registers of Probate have used the Suffolk example as a model and are also using personal funds to maintain a Web site for their court.

AUDIT SUMMARY

- *"Our review…disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC at Two Center Plaza, Boston, Massachusetts."*

The Registry believes that the level of management provided by the AOTC and the IT Division is clearly understated here. The Division's sole function is the total management and oversight of computers, software and other information technology resources used by the Trial Court and its various divisions. As detailed below, the Director of the Trial Court's IT Division admits as much and accepts responsibility for many of the deficiencies listed in the draft audit report.

- *"Although job descriptions for staff existed at the Court, they did not include reference to IT-related responsibilities."*

- *"Although there was no established IT function at the court, two employees served, in addition to maintaining their regular Court responsibilities, as the liaisons between the court and AOTC regarding IT-related issues. Given that AOTC had not defined IT-related areas of responsibility…personnel were unaware of certain responsibilities and control practices and did not have clear operational standards and guidance on which IT-related tasks and activities should be performed."*

The Suffolk Registry is fortunate to employ several staff members who are technically savvy and skilled in computer installation, repair, etc. Without them, our operations would have come to a standstill on numerous past occasions because of the IT Division's inadequate response to problems. The current, unwritten policy for these 'liaisons' is basically one of "Call the Help Desk." Unfortunately, the resulting response has been one that is of no help, and our employee is on his or her own in solving a problem or making a repair.

In one recent instance, we asked for assistance with several desktop computers that had failed and were unusable. (This also meant that there were several employees who had no ability to perform their job functions.) The Help Desk reported that vacations and other priorities meant we wouldn't receive a visit from a technician for three weeks. In another instance, an employee's Word Perfect program became corrupted. We offered to walk the two blocks to the IT Division offices to borrow a copy in order to reinstall the program. We were denied access to the disc, and instead, waited several weeks for a technician to come in and perform this very simple task.

In a recent discussion with the Registry, the newly appointed IT Division Chief Information Officer … agreed that wait times of several weeks for technician visits are absolutely inexcusable. He is committed to correcting the problem by ensuring a faster, more thorough response from IT technicians. He is also in the process of compiling the specific responsibilities of IT liaisons in order to share this information with all court divisions.

- *"We found that areas housing computer equipment were inaccessible by the general public and were staffed by Court employees. The only exception were two workstations located in the Clerk's Office from which docketing information is made available to the general public."*

Only those employees specifically needing editing capabilities (Index Department, Trial Department, etc.) are given clearance to edit information contained within BasCOT. Most do not have this capability, ensuring limited access to BasCOT files. Meanwhile, the two computers located in public areas are 'lookup only,' and files contained within cannot be edited in any way.

- *"Our audit revealed that the Court, in conjunction with the AOTC, had not documented a formal and comprehensive business recovery strategy for mission critical and essential application systems..."*

- *"We found that formal planning had not been performed for restoring Court-based computer operations in the event that automated systems were inoperative or were damaged or destroyed. In addition, we found that the Court, in conjunction with AOTC, had not performed a criticality assessment of application systems and their associated risks."*

- *"The Court, in conjunction with AOTC, should implement a comprehensive business continuity strategy and disaster recovery plan to help ensure system availability and resumption of IT operations within an acceptable time frame should processing be rendered inoperable or inaccessible."*

The Suffolk Registry relies on the AOTC and the IT Division, as part of their core missions, to perform such functions and ensure that such plans are in place. In turning to the Chief Information Officer for assistance in responding to the audit findings, the Registry learned that no such disaster recovery plan exists. Just six weeks on the job, the(sic) CIO has made the development and implementation of an IT disaster recovery plan a top priority, and is expected to have this plan

completed within days. He will communicate this information to all court divisions in writing and through the Court's Intranet site to ensure that the plan is implemented as quickly as possible.
In order to perform court functions and serve the public should a disaster result in the closing of the Edward Brooke Courthouse, the Suffolk Registry would turn to the Middlesex Registry of Probate for assistance and support. Little more than a mile from our current location, the Cambridge courthouse would serve as a temporary office for essential Suffolk Registry staff and the public. We will work with the Middlesex Register of Probate to further detail and formalize this business continuity plan.

- **"…***we found that there were no backup procedures for many hardcopy standard forms and Court-related documentation. As a result, important documents could not be recovered if they were destroyed, and added costs would be required to recreate these standard forms."*

The Registry clearly disagrees with this finding. In terms of the preservation and protection of court files, legal forms and other important paperwork, the Suffolk Registry of Probate is light years ahead of other court divisions for a multitude of reasons. To begin, all case files are kept in a secure, state-of-the art fireproof and waterproof room to ensure their protection. In addition, the Registry maintains a $28,000 microfilm machine that photographs and indexes all legal paperwork – that which contains a judge's signature – as the law requires and within a day of it being signed. The Registry has contracted with Donnegan Systems of Northboro to develop this microfilm, provide the Registry with a copy, and store the original roll in a secure off-site facility. The Registry also uses the Trial Court's BasCOT system to electronically docket all case files, and a backup of BasCOT files is performed daily by the IT Division. Even further, the Court retains docket books containing manual entries in older cases.

It should also be noted that documents of historical significance and cases ordered impounded by a judge are segregated from general case files and maintained in a separate locked vault to ensure their safety and security.

These steps alone ensure that copies of legal paperwork will always be available, but a pilot program brings even greater dependability to the process. Late last year, the Suffolk Registry was the first court in the state to employ scanning technology to digitize court papers. This digital paperwork is then stored on an 'E-Cabinet' for later recall by simply searching these PDF files under the case docket number. These files are also backed up onto a DVD disc immediately upon scanning. The eventual goal is a paperless courthouse that eliminates the need for case folders to travel from attorneys and litigants to the courtroom and other Court divisions. It also means that, in addition to microfilming and the BasCOT system, there is yet another system in place to ensure that important legal documents cannot and will not be lost.

The use of an E-Cabinet is another example of a move taken by the Registry because of inaction on the part of the Trial Court. While the Trial Court has spent years mired in studies of new technology and ways to improve court operations, the Suffolk Registry has taken its own major steps forward in this regard.

AUDIT RESULTS

- **"***For the Probation Department, we found that hardcopy files of court proceedings were maintained by the Court office with no recovery strategy in place to recover these files if damaged or destroyed, while electronic data files for the CARI, WMS and PRA applications were maintained and backed up through the central AOTC office."*

All issues regarding the electronic data files of the Probation Department fall under the jurisdiction of the Office of the Commissioner of Probation and not the Register of Probate.

- *"In the Register of Probate's Office, although certain hardcopy files were being backed up through imaging or scanning, not all hardcopy files would be recoverable."*

The multitude of measures taken by the Registry and already described make the recoverability of legal documentation a certainty. Under the law, only those documents that include a judge's signature are needed to recreate a case file, and those documents (or information about those documents) can easily be retrieved from multiple sources.

AUDIT RECOMMENDATIONS

- *"We recommend that the court, in conjunction with the AOTC, should begin documenting its IT-related polices and procedures to provide sufficient, formal guidance for IT –related tasks and activities."*

As stated earlier, the Suffolk Registry relies on the AOTC and the IT Division, as part of their core missions, to ensure that such plans are in place and to share them with all court divisions. (The) Chief Information Officer … has been frank and honest in stating that no disaster recovery plan exists, and that formal documentation of many IT-related policies and procedures is lacking. He has accepted responsibility, and is currently drafting these policies as quickly as possible.

- *"The Court, in conjunction with the AOTC, should document their disaster recovery strategy and prepare a written disaster recovery and business continuity plan that incorporates user-area plans."*

- *"We recommend that a risk analysis be performed on the Court's information technology environment on an annual basis, or upon major changes to systems or the IT environment."*

- *"The results of all tests should be documented and maintained and copies of the recovery and business continuity plan, including user area plans, should be stored in the off-site location."*

The Chief Information Officer … has been made fully aware of the findings and recommendations included in the draft audit report, and we are confident that his commitment to resolving each of these issues in a timely fashion is a solid one. In our discussions, he has agreed that the AOTC and the IT Division have the ultimate responsibility for most of the deficiencies listed in the audit report, and has agreed to keep the Registry informed as he works to correct these and other problem areas.

In turn, I would ask the state for copies of its plans for disaster recovery and business continuity should a large scale disaster befall the Commonwealth. I would suggest that the state itself is lacking in this area and question whether or not such documentation exists on this level. Should it not be the role of the state's Information Technology Division and the Chief Technology Office to work with state agencies and divisions to develop and implement such plans?