A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

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

No. 2007-1137-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS AT THE SOUTH BOSTON DIVISION OF THE BOSTON MUNICIPAL COURT DEPARTMENT

July 1, 2004 through January 25, 2007

OFFICIAL AUDIT REPORT
MAY 2, 2007

TABLE OF CONTENTS

INTRODUCTION

The South Boston Division of the Boston Municipal Court Department, which was organized under Chapter 218, Section 1, of the Massachusetts General Laws, has jurisdiction for all criminal and civil matters for the district of South Boston. The Court's organization and management structure consists of the Judge's Lobby, Clerk Magistrate's Office, and the Probation Department. For the fiscal years 2005 and 2006, the Court processed $667,000 and $767,000, respectively, from cash bail receipts, fines, fees, and penalties. For the first two months of fiscal year 2007, the Court processed $92,946.

Chapter 478, of the Acts of 1978 reorganized the courts into seven Trial Court departments, including the District Court. The 1978 statute created a central administrative office supervised by the Chief Justice for Administration and Management responsible for the overall management of the Trial Court. Since the implementation of Chapter 478, the central administrative office has been referred to as the Administrative Office of the Trial Court (AOTC). The Boston Municipal Court Department was reorganized under Chapter 393 of the Acts of 2003 to administratively oversee the seven court divisions within Suffolk County, including the South Boston Division.

From an information technology (IT) perspective, the AOTC supports the mission and business objectives of the court system by administering the IT infrastructure, including mission-critical applications installed on the file servers and mainframes located at the AOTC's Information Technology Division in Cambridge. In addition, the AOTC provides IT services and technical support to individual courts and maintains master inventory records for the courts under its jurisdiction.

At the time of our audit, the South Boston Division of the Boston Municipal Court Department's computer operations were supported by 23 microcomputer workstations, with nine located in the Clerk-Magistrate's Office, 11 in the Probation Department, two in the Judge's Lobby, and one in the courtroom. The workstations were connected through a 3-COM router and two 3-COM switches to the AOTC's wide area network (WAN) to provide access to a file server located at the AOTC data center in Cambridge.

The AOTC implemented the first phase of the MassCourts application system at the South Boston Division in March 2006. The application, known as MassCourts Lite, which is a limited version of the MassCourts application, is used by the Clerk-Magistrate's Office and the Probation Office to issue and document criminal complaints, provide identity information, and track warrant information. The Probation Department also uses the Criminal Activity Record Information (CARI) system to access information on dispositions from courts regarding criminal offenses and restraining orders and uses the Probation Receipt Accounting (PRA) system to account for fines and fees. Court management also utilizes the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS) applications for administrative purposes.

The Office of the State Auditor's examination focused on an evaluation and review of certain IT-related general controls and financial-related items related to cash management and cash receipts for bails, court fees, fines, and penalties.

AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) and financial-related controls at the South Boston Division of the Boston Municipal Court Department covering the period of July 1, 2004 through January 25, 2007. The audit was conducted from July 24, 2006 through January 25, 2007.

The scope of our audit included an evaluation of IT-related controls pertaining to documented IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and off-site storage of backup copies of magnetic media. Our audit scope included a review of user satisfaction of the recently-implemented MassCourts Lite application system. We also examined financial-related controls regarding the management of cash receipts for bails, court fees, fines, and penalties.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control framework, including policies, procedures, and practices, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. Specifically, we sought to determine whether the Court, in conjunction with AOTC, had documented IT-related policies and procedures to provide sufficient, formal guidance for IT-related tasks and activities. We determined whether adequate physical security and environmental protection control policies and procedures were in place and in effect to prevent unauthorized access, damage to, or loss of, IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to the MassCourts Lite system. Furthermore, we sought to determine whether Court management, in conjunction with the AOTC, adequately monitored password administration and user account activity.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's computer equipment was properly accounted for and safeguarded against unauthorized use, theft, or damage. Regarding system availability, we sought to determine whether business continuity or user area plans were in place for use in conjunction with AOTC's disaster recovery efforts to regain business operations supported by technology. We also sought to determine whether business continuity plans included recovery strategies should IT resources at the Court be lost or

damaged. Furthermore, we sought to determine whether the Court had adequate procedures for off-site storage of backup media to regain business operations should IT systems become inoperable or inaccessible. For our review of user satisfaction of the MassCourts Lite application system, we sought to determine the degree of overall satisfaction regarding response time, functionality, support, and training.

With respect to financial-related areas, we sought to determine whether the Court had adequate controls over the management of cash receipts for bail funds, fines, fees and penalties. We sought to determine whether these funds collected by the Court were properly recorded and deposited in a timely manner for the period of July 1, 2004 through August 31, 2006.

Audit Methodology

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

Regarding our review of documented policies and procedures, we interviewed senior management, reviewed and analyzed documentation, and assessed relevant IT-related internal controls. Since our audit work was limited to the Court's IT-related operations, we determined whether relevant IT policies and procedures, either issued by the AOTC or developed by the Court, were promulgated and provided to Court staff. We determined whether Court staff were aware of AOTC's IT-related policies and procedures. Although our audit did not encompass a review of AOTC's IT operations, we reviewed AOTC's IT-related policies and procedures pertaining to access security and inventory control.

To evaluate physical security at the Court, we interviewed management personnel from the Clerk-Magistrate's Office and the Probation Office and security personnel assigned to the Court. We conducted walk-throughs, observed security devices, and reviewed procedures to document and address security violations and/or incidents. We requested a list of key holders to the Court's office areas and verified whether the individual key holders were current employees. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees of the Court. Through observation, inspection, and interviews, we determined whether adequate physical security controls were in place over areas housing IT equipment. We examined controls, such as office door locks, key management, remote cameras, and intrusion alarms.

To determine the adequacy of environmental protection controls, we conducted walk-throughs, evaluated controls in selected areas, and assessed the sufficiency of relevant documented policies and procedures. We examined the areas housing IT equipment at the Court to identify controls and to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; and emergency lighting. Audit evidence for environmental protection was obtained through interviews, observation, photos, and a review of relevant documentation.

To determine whether the Court's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access security. Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the MassCourts application system used by the Court. To determine whether only authorized employees were accessing the MassCourts Lite application system, we obtained system-generated lists from AOTC and the Office of the Commissioner of Probation for individuals granted access privileges and compared the lists to the Court's current personnel listing. We reviewed user profiles and access privileges for all employees at the Court having access to the MassCourts Lite application and compared this information to their individual job functions and responsibilities. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to Court personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly safeguard and account for computer equipment, we reviewed inventory control policies and procedures. Since AOTC is responsible for maintaining fixed-asset inventory records and promulgating policies and procedures for all courts, the AOTC master inventory was considered the official system of record for IT inventory. We conducted a complete test of the Court's inventory listing of computer equipment dated March 2006, and compared the information to the AOTC master inventory record. We further examined the inventory record for identification tag number, location, description, and historical cost. Furthermore, we compared the computer equipment listed on the Court's fixed asset inventory record to the master inventory record maintained by the AOTC for completeness and accuracy. We determined whether all microcomputer workstations and printers were accurately and completely recorded on the Court's inventory and the AOTC's master inventory record. In addition, we determined whether IT resources recorded on the inventory lists could be located at the Court and verified the descriptive information regarding those resources. We also determined whether any IT resources had been lost or stolen over the audit period.

To assess the adequacy of business continuity planning, we identified the extent to which the Court had assessed the impact of the loss of processing capabilities to its automated systems. We examined whether the Court, in conjunction with the AOTC, had performed a formal risk assessment to address the impact on processing capabilities should IT operations be disrupted for an extended period of time. With respect to business continuity planning, we interviewed management from the South Boston Division as to whether a written, tested business continuity or user area plan was in place, whether the criticality of application systems used by the Court had been assessed, and whether risks and exposures to computer operations had been evaluated. To evaluate the adequacy of controls to ensure the availability of electronic documents and data files prepared by the Court for the MassCourts Lite application, we considered audit results from prior and current IT audit work performed in regard to AOTC's procedures for the generation and off-site storage of backup copies of computer-related media and hard copy files.

To determine the level of user satisfaction with degree of training, ease of use, and functionality of the MassCourts Lite application system, we conducted a user survey review to determine whether the system was meeting user needs. We accomplished this through personnel interviews and user surveys with a total of nine employees from the Clerk-Magistrate's Office and the Probation Department at the Court.

To determine whether adequate controls were in place and in effect for cash receipts activity in the Clerk-Magistrate's Office and the Probation Department for the period July 1, 2004 through August 31, 2006, we examined the timeliness of deposits of cash receipts and the status of the reconciliation process. For the bail fund activity, we reviewed the adequacy of internal controls regarding the recording and reconciliation of bail funds and examined 26 months of bail receipt activity totaling $921,000, bail distributions totaling $981,000, and bail forfeiture totaling $29,000.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by Comptroller General of the United States and generally accepted industry practices. The criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association in July 2000.

AUDIT CONCLUSION

Our audit disclosed that the Court, in conjunction with AOTC, had internal controls in place and in effect for inventory control of computer equipment located at the Court and system access security and off-site storage of backup computer media for the MassCourts Lite application system. However, certain controls pertaining to the Court's IT environment needed to be strengthened. Specifically, our review indicated that controls pertaining to physical security, environmental protection, and business continuity planning for the Court needed to be strengthened. Regarding our examination of financial-related controls, we found that adequate controls were in place and in effect for the management of cash receipts and disbursements and bail fund activity.

Our review of IT-related policies and procedures disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC. We found that IT policies and procedures promulgated by AOTC were available and in effect at the Court. We found that documented IT policies and procedures provided sufficient guidance regarding IT-related tasks and activities performed at the Court. Our audit revealed that the Boston Municipal Court Department had a designated employee to serve as the formal liaison between the South Boston Division and AOTC to resolve technical issues related to the automated systems at the Court.

We determined that physical security controls and environmental protection over IT-related equipment at the courthouse needed to be strengthened. We found that security to the entrance of the courthouse was adequate, as all visitors were required to pass through a metal detector, and all packages were required to be scanned through an X-ray machine. However, we observed that cameras were not in place to allow monitoring of security to help protect public and employee safety in the areas that are in front of, and adjacent to, the courthouse. Court management indicated that security would be greatly enhanced by the installation of additional security cameras in the areas directly outside the courthouse. Regarding security over IT resources, we found that although access to the areas housing the microcomputers and printers was limited to Court employees, management did not maintain a list of key holders for office areas throughout the courthouse. As a result, the Court could not be assured that access to areas housing computer equipment was limited to only authorized personnel.

Regarding environmental controls, we observed that the area housing electronic switches used by the Court to connect to the AOTC file servers was not located in an environmentally suitable area in the Clerk-Magistrate's Office. We found that the equipment was located in an open, unprotected, and cluttered area, adjacent to a hot air radiator and water pipes. Because the equipment was not located in a separate controlled area, such as a dedicated telecommunications closet, it was at risk of being damaged. We also observed that due to the poor physical conditions within the only courtroom, the Court was

unable to install a computer terminal in the courtroom to provide online access to information and enhance the efficiency of the processing of daily court activity.

Our review of system access security controls for the MassCourts Lite application system revealed that adequate control practices were in place to provide reasonable assurance that only authorized users from the Court were granted access privileges. Our audit tests revealed that all individuals having access privileges to the MassCourts Lite application were current employees at the Court, and that the levels of access granted to these individuals were appropriate for their job responsibilities. However, we found that Court personnel were not required to change their passwords for a one-year period during the implementation stages of the MassCourts Lite application system. We recommend that the Court, in conjunction with AOTC, require that passwords be changed at least every 60 days and monitored for compliance.

With respect to inventory control for computer equipment, we found that the AOTC was responsible for maintaining the master inventory listing for all courts under its jurisdiction and that AOTC's Fiscal Systems Manual requires each court to maintain a perpetual inventory and verify the inventory on an annual basis. We found that the Court was adhering to the AOTC policies and procedures and had conducted an annual physical inventory and reconciliation in compliance with AOTC policies. Our tests indicated that hardware items were locatable, properly accounted for, and tagged. We found that the Court's inventory record of IT resources contained appropriate information that was found to be accurate and complete for each item listed. We acknowledge that because purchases of IT equipment are made centrally by AOTC, the Court's inventory record did not include historical cost figures. We noted that AOTC's inventory system of record for the Court's IT resources did include historical cost.

Our audit revealed that the Court did not have contingency or user area plans to be used in conjunction with disaster recovery plans that would be initiated by AOTC should automated systems residing on AOTC file servers be rendered inoperable or inaccessible. In addition, we found that the Court had not assessed the impact on business operations should automated systems, or network capabilities, be unavailable for an extended period of time, nor had the Court performed a risk assessment from a business continuity perspective. On the basis of our examination, we believe that the Court needs to address the risks of being unable to regain business operations within an acceptable period of time for functions or processes dependent upon technology. Although we found through interviews with South Boston Division senior management that the Court had certain procedures in place in the event of a disaster or emergency, the Court had not formally documented these procedures in a comprehensive user area plan that would include the loss of IT processing capabilities. According to audit work conducted on both prior and current IT audits at AOTC, evidence indicated that backup copies of magnetic media

were being generated and stored off-site for mission-critical application systems, including MassCourts Lite, residing on AOTC's file servers.

Our review of user satisfaction of the MassCourts Lite application system installed by the AOTC indicated that the application was supporting the primary business functions of the Court. However, our interviews and user satisfaction surveys indicated that improvements in the system's functionality and reliability may be warranted. At the time of our audit, we found that users had difficulty maneuvering through the system menus and screens and indicated that accessing required forms was cumbersome and time consuming. Users further stated that they had experienced processing delays and system disruptions on a daily basis. However, our review indicated that users were satisfied with the MassCourts training provided by the AOTC and pleased with the responsiveness of the technical support provided by the AOTC liaison to the Court. The Court should continue to work with AOTC to communicate any operational concerns or identify areas where the reliability or efficiency of the MassCourts Lite application can be addressed through AOTC technical assistance or modifications to the system or its supporting technology.

Our examination of financial controls revealed that the Court had controls in place and in effect to provide reasonable assurance that the management of cash bail was adequate and that fees and fines were being deposited in a timely manner. Our audit tests on cash bail activity revealed that the bail was being properly recorded, accounted for, and reconciled in compliance with AOTC regulations. We found that bail forfeitures were classified correctly and transmitted to the Office of the State Treasurer in a timely manner and that bails were returned to sureties after appropriate case resolution. Our audit test also revealed that Notification of Surety Letters were kept on file at the Court. Our examination of the cash receipt activity at the Court revealed that the daily activity was handled in a timely manner with appropriate segregation of duties. Our tests revealed that deposits were made on a daily basis into the Court's bank account and daily wire transfers were made to the Office of the State Treasurer. Our review indicated that monthly bank statements were being reconciled by the Court in a timely and accurate manner.

AUDIT RESULTS

1. Physical Security and Environmental Protection Controls

At the time of our audit, physical security and environmental controls at the South Boston Division of the Boston Municipal Court needed to be strengthened. We observed that the courthouse was staffed with security personnel and public entrances were equipped with metal detection and X-ray screening equipment. However, our audit revealed that security for the perimeter areas outside the courthouse needed to be strengthened. We observed that there were no surveillance cameras to monitor activities in the areas adjacent to the courthouse where defendants and the general public often congregated. According to Court management, prior incidents outside the courthouse have jeopardized public safety and that security enhancements, such as the installation of security cameras, must be undertaken for the safety of the general public. We also found that Court management did not maintain a list of key holders and could not account for every key distributed. As a result, the Court was unable to provide adequate assurance that only authorized employees had access to courthouse offices.

Regarding environmental controls, we observed that there were serious deficiencies throughout the building. We found that the communications equipment used for connections to the AOTC file servers were located on the floor in the Clerk-Magistrate's Office. The electronic switching equipment was located adjacent to a hot air radiator and water pipes. We also found the area to contain water bottles and office supplies. We found that the telecommunications equipment was at risk of being damaged due to its placement in an environmentally unsafe location instead of in a dedicated telecommunication closet.

Due to the absence of controls regarding physical security and environmental protection controls, we found that the Court could not provide reasonable assurance that computer equipment and access to AOTC's network would be safeguarded from unauthorized use, damage, loss, or theft. We believe that the age and the deteriorating condition of the building, as well as budgetary constraints, contributed to the difficulty in implementing controls to safeguard IT equipment. Generally accepted computer industry standards advocate the need for sufficient physical security and environmental protection controls to provide reasonable assurance that damage to, or loss of, IT-related assets will be prevented.

Recommendation:

We recommend that the South Boston Division management, in conjunction with the Boston Municipal Court Department and the AOTC, seek the means to improve the physical and environmental protection controls at the courthouse. As a first step, we recommend that court management establish a written policy concerning the distribution and control of keys to authorized personnel. We urge management to compile a list of current key holders and, if feasible, consider re-keying the building and

office areas. Further, we urge AOTC management to consider the installation of security cameras to provide perimeter surveillance of the courthouse building.

Regarding environmental controls, we urge court management to re-locate the computer switching equipment to a dedicated telecommunications closet.

Auditee's Response:

> *To help ensure the security of IT equipment, after consultation with the Chief Court Officer, the Chief Probation Officer and the Clerk Magistrate, a master key list has been compiled and is now on file in the Judges Lobby here at the South Boston Court. Security of the outside perimeter areas of the courthouse continues to be a problem. A request for remote outside surveillance cameras to monitor front, back, and adjacent areas of the courthouse where defendants and the public congregate will be made again. Previous requests were denied because of budgetary considerations. We are well aware that the age and deteriorating conditions of the building, as well as budgetary constraints, contribute to the difficulty that we have had in establishing a safe area for the IT switching equipment. We will work closely with AOTC to improve the housing (and security) of all telecommunication equipment at the South Boston Division.*

Auditor's Reply:

We commend the initial actions being taken by Court management to improve physical security controls with the compilation of a master key list. We continue to urge the Court to work in conjunction with AOTC to seek a more appropriate location for the placement of the telecommunications equipment in order to reduce the risk of damage to equipment and the loss of processing capabilities. The Court should continue to seek the means to enhance physical security controls for the perimeter areas at the courthouse.

2. Business Continuity Planning

Our audit revealed that the South Boston Division had not developed user area contingency plans, including an evacuation plan and contact list, to address a potential loss of automated processing. We noted that user area plans and contingency plans should be developed with input and consultation with the AOTC's Information Services Department. We found that Court staff were unfamiliar with AOTC's strategy for business continuity planning and were unaware of their responsibilities with respect to the development of appropriate user area and contingency plans to address a loss of IT processing capabilities. Although we acknowledge that the Court's plan is to contact AOTC for instructions should IT processing capabilities be lost, the Court should have a detailed user area plan to address various disaster scenarios to support the timely restoration of mission-critical business operations.

Without adequate disaster recovery and contingency planning, including user area plans, the Court is at risk of not being able to perform mission-critical business functions should the automated systems be

disrupted or rendered inoperable or inaccessible for an extended period. A loss of processing capabilities could result in significant delays in processing cases. The environmental protection issues presented in this audit report place increased emphasis on the Court's need to develop a detailed business continuity plan should mission-critical applications become unavailable for an extended period of time. Without access to the MassCourts Lite, CARI, and PRA application systems, the Court would be hindered from obtaining case management information. The Court would also be unable to confirm that fines, fees, and penalties were being collected by the Probation Department and would be unable to access all Trial Court dispositions regarding criminal cases.

Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the Court'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 IT resources and render the systems inoperable or inaccessible, and the likelihood of the threat and frequency of occurrence and the cost of recovering the systems.

Generally accepted practices and industry standards for IT 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.

AOTC and Court management should clearly identify the responsibilities associated with developing viable user area plans to address the loss of automated systems for an extended period of time. Court administrators should be responsible for identifying and formally documenting key personnel, alternate staff, and emergency contact information; describing and documenting roles and responsibilities for a disaster recovery team at the Court; formally assessing potential Court impact based on various disaster or emergency scenarios; formally identifying Court-based files and records; and detailing a strategy or process for the recovery of these records and files. The Court-based files and records would include hardcopy documents vital to the Court's daily case processing activities, including docketing and scheduling information. The Court, in conjunction with AOTC, needs to identify the nature and extent of Court or business activities that can be conducted in the absence of AOTC-supported systems or damage to the Court facilities.

Recommendation:

We recommend that the South Boston Division of the Boston Municipal Court Department, in conjunction with the AOTC, assess the relative criticality of its automated processing environment and develop and test appropriate user area plans to address business continuity. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to Court operations or the IT environment. We further recommend that the South Boston Division and the Boston Municipal Court Department request information from AOTC as to the status of disaster recovery and business continuity plans for application systems and network capabilities critical to the Court's operation.

The business continuity plan, or user area plan, should document the Court's recovery and contingency strategies with respect to various disaster scenarios, and outline any necessary contingencies. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities, needed to effectively and efficiently recover critical operations within the needed time frames. We recommend that business continuity and user area plans be tested and periodically reviewed and updated, as needed, to ensure their viability. The completed plans should be distributed to all appropriate staff, who should be trained in the execution of the plans under emergency conditions.

Auditee's Response:

> *We recognize the use of a business continuity/Disaster Plan for the Court. We plan to work with the Administrative Office of the Boston Municipal Court Department and Administrative Office of the Trial Court to develop and implement a detailed user area plan/continuity plan for the Court.*

Auditor's Reply:

The Court, in conjunction with AOTC, should collaborate in developing user area plans to ensure continuity or timely restoration of Court activities should the Court facility become inaccessible or should IT systems become inoperable for an extended period of time.