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. 2003-1162-4T

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

July 1, 2002 through June 30, 2003

OFFICIAL AUDIT REPORT
DECEMBER 30, 2003

TABLE OF CONTENTS

INTRODUCTION

The Wrentham District Court (WDC) is organized under Chapter 211, Section B and Chapter 218, Section 1 of the Massachusetts General Laws. The Court's organization and management structure consists of the Judge's Lobby, the Clerk-Magistrate's Office and the Probation Department. The Court has jurisdiction for all criminal, civil, and juvenile matters for the towns of Foxborough, Franklin, Medway, Millis, Norfolk, Plainville, Walpole and Wrentham. The Court received approximately $1.55 million of state funds and processed revenue of approximately $950,000 from sources such as cash bail receipts, fines, fees, and penalties for the 2003 fiscal year.

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). From an information technology perspective, the AOTC supports the mission and business objectives of the District Courts 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 Court's computer operations were supported by 34 microcomputer workstations of which 17 were in the Clerk-Magistrate's Office, four in the Judge's Lobby and court rooms, and 13 microcomputer workstations in the Probation Department. The workstations were connected by a router and two switches to the AOTC's wide area network (WAN) through the IBM Netfinity file server located at the AOTC data center in Cambridge. The Court utilizes the Warrant Management System (WMS) which is maintained by the AOTC, the Probation Receipt Accounting System (PRA) maintained by the Office of the Commissioner of Probation, and the Criminal Activity Record Information System (CARI) which is also maintained by the Office of the Commissioner of Probation. In addition, the Court utilizes the Human Resources Compensation Management System (HR/CMS) payroll system maintained by the State Comptroller's Office.

The Clerk-Magistrate's Office uses the Warrant Management System to track warrants issued from all courts under the jurisdiction of the AOTC. The Probation Department uses the Criminal Activity Record Information (CARI) system to access information on all dispositions from courts regarding criminal offenses and restraining orders and the Probation Receipt Accounting System (PRA) to account for fines and fees.

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

SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

We performed an information technology (IT) related audit at the Wrentham District Court (WDC) from June 2, 2003 through September 8, 2003. The audit covered the period of July 1, 2002 through June 30, 2003.

The scope of our audit included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, logical access security, inventory control over IT-related assets, disaster recovery and business continuity planning, and off-site storage of backup copies of magnetic media. In addition, we examined controls over the security and disposal of confidential records, and assessed user satisfaction regarding the application systems utilized at the Court.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Court's IT-related internal control framework, including policies, procedures, practices, and organizational structure provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding logical access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access into the Court's automated systems. Further, we sought to determine whether the WDC, in conjunction with the AOTC, was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. In addition, we sought to determine whether the Court had adequate procedures for off-site storage of backup media to support system and data recovery objectives. Further, we determined whether the Court had an effective business continuity plan that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. A further objective was to determine whether adequate controls over the security and disposal of confidential records were being exercised at the Court to meet the regulations

promulgated by the Office of the Secretary of State. Finally, we reviewed the level of satisfaction of the users of the Warrant Management, CARI and PRA application systems.

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 court personnel. To obtain an understanding of the internal control environment, we reviewed the Court's organizational structure and primary business functions. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

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

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

To determine the adequacy of environmental controls, we conducted walk-throughs and evaluated controls in selected areas in order to assess the sufficiency of documented control-related policies and procedures. We examined the areas housing IT equipment at the Court to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of logical access security included a review of procedures used to authorize, activate, and deactivate access privileges to the AOTC file servers through the microcomputer workstations located at the Court. To determine whether only authorized employees were accessing the automated systems, we

obtained system-generated lists from AOTC and the Office of the Commissioner of Probation for individuals granted access privileges to the automated systems used by the Court and compared it to the Court's current personnel listing. We performed a test of user profiles and access privileges for all employees versus 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 the WDC personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

We reviewed inventory control procedures for IT-related items, by determining whether adequate controls were in place and in effect to properly safeguard and account for IT resources. We found that the AOTC was responsible for maintaining fixed-asset inventory records and promulgating policies and procedures for all courts, and therefore the AOTC master inventory was considered the official system of record. We conducted a 100% test of the Court's inventory listing of IT-related items 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. Further, we compared the IT-related items listed on the Court's fixed-asset inventory record to the master inventory record maintained by the AOTC for completeness and accuracy.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the PRA or the WMS application systems be inoperable or inaccessible. With respect to business continuity planning, we interviewed management from the Wrentham District Court as to whether user area plans were in existence at the court and a written, tested business continuity plan was provided by AOTC to the court. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. In addition, to evaluate the adequacy of controls to protect data files through the backup of off-site magnetic media and hardcopy files, we interviewed Court staff regarding the creation of backup copies of computer-related media.

To determine whether adequate controls were in place to safeguard and dispose of confidential records, we examined policies and procedures, conducted interviews with WDC employees and observed the areas used by the Court to store confidential records.

To determine whether Court employees believed they were adequately trained in the use of the Warrant Management system and were satisfied with the level of performance of the application, we interviewed staff members of the Clerk-Magistrate's Office. We also determined through interviews and the use of questionaires the degree to which Probation Department staff members were satisfied with the PRA and CARI application systems.

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

AUDIT CONCLUSION

Our audit disclosed that although the Court, in conjunction with AOTC, had internal controls in place over physical security, logical access security, off-site storage of backup computer media and the retention and disposal of confidential records, certain controls pertaining to the accounting of IT resources, provision for an appropriate processing environment and continuous availability of processing needed to be strengthened. Specifically, our review indicated that the controls over IT-related inventory, environmental protection for the Courthouse, and business continuity planning needed to be strengthened.

Our examination of the Court's organization and management revealed that there was an established chain of command, adequate segregation of duties among court employees, and clear points of accountability. Our review of IT-related activities disclosed that the primary IT functions were supported and maintained by the IT Department of the AOTC. Due to the nature and limited extent of the IT environment at the Court, there was no established IT department, although there was an employee who served as the informal liaison between the Court and AOTC. Although the AOTC had limited IT-related policies and procedures, we found that certain controls over the use of IT-related resources needed to be strengthened, documented and communicated to court personnel.

Our audit revealed that physical security controls provided reasonable assurance that WDC's IT-resources and personnel would be adequately protected. We found that security to the entrance of the courthouse was adequate as all visitors were required to pass through a metal detector, and all packages were required to be scanned through an X-ray machine. We observed that the WDC employed remote cameras and intrusion alarms throughout the courthouse. Court management maintained a list of individuals having keys for office areas throughout the courthouse, and our review of the list revealed that access was limited to authorized persons. Our observations of the Court's telecommunication room, which contains equipment that enables access to the mission-critical application systems utilized by the Court, indicated that access was limited to three court employees and that the door to its room was kept locked.

Our review revealed that there were certain environmental protection controls in place such as an evacuation plan for the entire building, an emergency lighting system, air conditioning for areas housing microcomputer workstations, and fire extinguishers on each floor. However, we determined that environmental protection controls needed to be strengthened to provide reasonable assurance that the Court's IT operations would not be disrupted. We observed that the telecommunication room, which houses the router and switches allowing connectivity to networked application systems, was also being used for storage of maintenance supplies. Furthermore, we observed that environmental protection

needed to be strengthened in the telecommunication room to regulate the room temperature. In addition, there were no provisions for an emergency generator in the event of a temporary loss of electrical power.

Our review of logical access security controls revealed that adequate control practices were in place to provide reasonable assurance that only authorized users were granted access privileges to the applications residing on the AOTC's file servers and the Court's microcomputer workstations. Our audit revealed that access privileges for individuals no longer employed by the Court were being removed by AOTC in a timely manner. However, we found that Court personnel were not required to change their passwords, and there was little indication that password administration was being monitored. There were limited written policies and procedures contained in the AOTC's "Internal Control Guidelines section 2.3.1" that outline parameters for password administration. In addition, during our audit and subsequent to the audit period, the AOTC issued Information Technology Policy #1 on August 13, 2003, which formalizes certain policies regarding IT-related security policies and procedures for all court employees. We believe that, due to the confidential nature of the information residing on the Court's application systems, policies and procedures for password administration should be strengthened and communicated to appropriate court personnel. Court management should ensure that the levels of access to certain application systems be appropriate for individual job classifications and responsibilities. We recommend that passwords for all systems be changed at least every sixty days and monitored for compliance.

Our review of IT-related equipment revealed that controls needed to be strengthened to provide for the proper accounting of information technology assets. The AOTC is responsible for maintaining the master inventory listing for all courts under its jurisdiction. We found that the AOTC's Fiscal Systems Manual requires each court to maintain a perpetual inventory, verify the inventory on an annual basis and reconcile the record to the AOTC master inventory listing. Our audit tests revealed that two IT-related inventory listings were not in agreement and needed to be reconciled, and that both listings lacked essential information, such as historical cost and acquisition dates. Our audit test of the master inventory record disclosed that certain hardware items sampled could not be located. As a result of our inventory tests, we concluded that a further reconciliation of the inventory lists and physical assets was necessary and that both the AOTC master inventory record and the Court's inventory were not accurate and current. We determined that the last physical inventory taken at the Court was on June 30, 1998 and there was no evidence of any recent reconciliation of the inventory listings.

At the time of our audit, the AOTC had not provided the Court with a business continuity plan regarding system availability in the event of a disaster. Our audit revealed that the Court, in conjunction with the AOTC, had not documented a formal business recovery strategy for critical applications residing on AOTC's file servers. We found that formal planning had not been performed to restore computer operations in the event that automated systems were damaged or destroyed. In addition, we found that

the Court, in conjunction with the AOTC, had not performed a criticality assessment of application systems and their associated risks. On the basis of our examination of business continuity plans, we believe that the Court needs to address the risks of not being able to recover critical data within an acceptable period of time. The Court, in conjunction with AOTC, should implement a comprehensive business continuity plan to help ensure system availability and resumption of IT operations within an acceptable time frame should processing be rendered inoperable or inaccessible. It is our understanding that the AOTC has taken steps to address disaster recovery and business continuity planning. However, the plan has neither been formalized and tested nor communicated to the individual courts. We found that backup procedures were in place for the mission-critical applications operating on the AOTC's file servers, which support the Warrant Management System. The PRA and CARI application systems have backup procedures administered by the Office of the Commissioner of Probation in Boston.

Our examination of the security and disposal of confidential records indicated that the Court had established policies and procedures to ensure that all records would be safeguarded. We examined the areas in which the records were being stored and found the room to be secure and that access was limited to only the Office Manager and the Clerk-Magistrate. Regarding the disposing of confidential records, we found that the Wrentham District Court is following established policies and procedures promulgated by the Office of the Secretary of State as well as the Administrative Office of the Trial Court. Specifically the Court is adhering to M.G.L. C. 221, sec.27A permitting the destruction of records as well as the disposal of records policy no.17/76 promulgated by the Secretary of the Commonwealth.

Based on our review of user satisfaction regarding various application systems used by the Court, we found that the users were generally satisfied with the integrity of the data received, but had concerns about accessing the information requested in a timely manner. Specifically, we found that users had concerns regarding system availability, password administration, and the lack of up-to-date hardcopy system manuals. In addition, users indicated a need to implement an automated system to improve case management tracking. The users indicated that when they needed assistance, AOTC's Help Desk personnel were very responsive.

AUDIT RESULTS

1. Environmental Protection

At the time of our audit, environmental controls at the Wrentham District Court needed to be strengthened. Our audit revealed that although there were hand-held fire extinguishers and emergency lighting throughout the Courthouse, we observed environmental control deficiencies that could impact the Court's availability of mission-critical applications systems. We found only limited written policies in place for the environmental controls of the mission-critical and essential IT-related systems at the courthouse.

We observed that the telecommunication room, which serves as the center through which all computer lines are routed to the AOTC file servers, had several deficiencies. Our audit revealed that the room was being used to store potentially flammable materials such as office paper products, cleaning supplies, and paint. We observed that the room was cramped, poorly ventilated, contained exposed cabling, and that general housekeeping procedures needed to be strengthened. The room did not contain any environmental controls such as heat, water or temperature monitoring equipment.

Our audit revealed that, although there was an emergency evacuation plan in place, the Court had not made any provisions for an emergency generator in the event of a temporary loss of electrical power. The lack of environmental controls places the Court at risk of being unable to access critical information from the WMS, PRA and CARI applications should the connection to these systems be disrupted or damaged.

Generally accepted computer industry standards advocate the need for sufficient environmental protection controls to provide reasonable assurance that damage to, or loss of, IT-related assets will be prevented.

Recommendation:

We recommend that the Court consider relocating the telecommunication equipment, specifically the router and switches, to an area that affords better environmental protection. If the most cost-effective approach is to use the existing telecommunication room until a more appropriate solution can be implemented, then we suggest that non-essential materials be removed, that the storage of general office supplies and building materials be relocated and that the room be equipped with environmental control devices such as heat, smoke, humidity and temperature controls. Removal of non-essential materials and office supplies should assist the Court in maintaining good housekeeping efforts.

We also recommend that the Court, in conjunction with AOTC, develop policies and procedures to improve environmental protection controls over IT-related assets including mission-critical applications.

At the conclusion of our audit period, the relocation of the utility lines to the Courthouse facility was about to begin. We believe this will provide the Court an opportunity to address some of the environmental concerns raised in this audit.

Auditee's Response:

The auditor's observations of the basement-level telecommunication room are most perceptive. Not only is the ground-level location of the room problematical in the event of a casualty, but its present condition renders the IT controls most vulnerable, as to this, there is no question. The difficulty in taking any remedial action is that the room, as is the building, is under the care and control of Norfolk County. The Trial Court is merely a tenant at 60 East Street. Recommendations should be made, however, and will be as to the further configuration and care of this room. There should be the construction of a wall separating the IT operations from the county storage area. The IT area should be filled with the necessary controls to regulate humidity, heat, ventilation and power. At this time, it would also be advisable to install an emergency generating system to guard against the casualty of loss of electricity. Ideally, the IT room should be relocated to the first floor. This should alleviate the threat of damage through a flood and would assist in keeping the equipment at a constant temperature and humidity level. Unfortunately, there is no room on the first floor.

Success in obtaining the necessary changes to the telecommunication room will depend largely on the amount of money available to the county in this area and how this money will be allocated. The auditors make a very good point, however, that this may be the time to pursue such changes as new utility lines are currently being finished to the building in conjunction with a recently upgraded electrical service. A telephone call will be made to the Facilities Maintenance for Norfolk County requesting the recommended changes to the telecommunication room.

Auditor's Reply:

We acknowledge that the courthouse facility is owned and operated by the Norfolk County. We recommend that requests for assistance to Norfolk County be made in writing. In addition, management should consider either relocating the telecommunication room or strengthening environmental protection controls over the existing room.

2. Inventory Control of IT Resources

At the time of our audit, we found that IT-related fixed-asset controls needed to be strengthened to provide for the proper accounting of the Court's inventory record. Our audit review of the AOTC master inventory record for hardware items and the WDC fixed-asset inventory indicated they were not in agreement and needed to be reconciled. Our audit revealed that IT-related equipment at the Court had vendor serial numbers and state asset tag numbers. However, our audit test revealed that the inventory record was not current and accurate.

Although the AOTC is responsible for maintaining the Court's IT-related fixed asset inventory records, the AOTC's Fiscal Systems Manual requires each court to maintain a perpetual inventory, verify the inventory on an annual basis and reconcile the record to the AOTC master record listing. At the time we began our audit, the Court could not provide a current and complete record for all IT-related items. Subsequently, the Court performed a physical inventory of IT hardware assets to assist in verifying the inventory record. The last annual physical inventory taken by the Court prior to the initiation of our audit was June 30, 1998.

Our examination of the inventory record of the Wrentham District Court provided by AOTC, consisting of 72 IT-related items, revealed that there was incomplete data, such as historical cost, acquisition dates, and location of the equipment. As a result of our initial inventory test, we concluded that a further reconciliation of the inventory lists and physical assets was necessary and therefore we conducted a complete physical inventory of the WDC's IT-related assets. Our test of the AOTC master inventory record disclosed that 12 IT-related items could not be physically located and 13 items were on the AOTC master inventory record, but not on the WDC perpetual inventory listing. We found that there were a total of 93 IT-related assets on the WDC inventory record, of which 16 could not be physically located. In addition, there were 19 IT-related items physically located at the Court that were not located on the AOTC master listing. Due to the lack of accurate and complete cost amounts on the inventory records, an accurate total value for the inventory could not be determined.

Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained to properly account for all IT-related assets and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

The AOTC's "Internal Control Guidelines" states, "All assets with a value over $100 must be inventoried on an annual basis and submitted to the AOTC, Fiscal Affairs Department." The Court should, in conjunction with AOTC, develop written procedures, maintain a perpetual inventory record, and perform an annual physical inventory and reconciliation of the Court's property and equipment to the AOTC's inventory record. From an IT configuration management perspective, all IT resources should be inventoried.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989, states, in part, that "…the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts."

Shortcomings in inventory control were the result of a lack of management attention and proper assignment of inventory control responsibilities. The absence of an accurate inventory record may hinder the Court's ability to manage IT-related resources and to detect theft and unauthorized use of IT-related assets. The lack of an up to date and accurate inventory hinders the Court's ability to assess its future technology and configuration management needs.

Recommendation:

The Court, in conjunction with AOTC, should enhance controls over its record-keeping to provide for maintenance of a perpetual hardware inventory record. We recommend that the perpetual inventory include historical cost data, acquisition dates, and specific locations of equipment. Based on the results of the review, the Court, in conjunction with the AOTC, should implement formal policies and procedures to include compliance with all state reporting requirements for fixed assets. Additionally, the Court should include practices regarding the maintenance of a perpetual inventory, and perform an annual reconciliation of all physical assets.

We believe that the Court should comply with the policies and procedures documented in the AOTC "Internal Control Guidelines" pertaining to inventory control. Specifically, the Court should maintain a perpetual inventory that is periodically reconciled to the physical assets and records of purchased and surplus or lost equipment. To maintain proper internal control, a staff person who is not responsible for maintaining the inventory record of property and equipment should perform the periodic reconciliation. Further, the inventory record once reconciled should be used as the basis for documenting the Commonwealth's required asset-management reports.

We recommend that the Court enter all property and equipment into the fixed-asset inventory record at the date of acquisition or date of installation. The Court should work, in conjunction with the AOTC, to ensure that the inventory records are current, accurate, and complete.

Auditee's Response:

> *Per the recommendation of the auditors, a perpetual inventory of IT related fixed assets, as they are allocated to the Clerk-Magistrate, can and will be performed and maintained on an annual basis. This data shall be reconciled, from time to time, as recommended in the audit and in accordance with AOTC internal control guidelines that pertain to inventory control.*
>
> *The perpetual hardware and software inventory has already been performed in conjunction with the recent pertinent memorandum of October 1, 2003 from John Beaton, Director of the Information Technology Department. This inventory has been sent to the AOTC.*

The auditor's recommendations regarding historical cost data and acquisition dates may refer to the person in the First Justice's office that historically has kept that information. If necessary, that information could be reconciled with our data.

Auditor's Reply:

We are pleased that the Court is taking steps to strengthen the integrity of the fixed-asset inventory record. We believe that once the Court's inventory has been reconciled and updated to the AOTC's master list, the Court should maintain a perpetual inventory record that is reconciled periodically with AOTC's master inventory record. We will examine the progress made to the fixed-asset inventory record during our follow-up audit.

3. Business Continuity Planning

Our audit revealed that the Court, in conjunction with the AOTC, had not developed 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 supporting Court operations to determine the extent of potential risks and exposures to business operations. Although the AOTC provided backup copies of magnetic media for the business functions processed through its file servers, our audit revealed that the Court, in conjunction with AOTC, had not developed user-area contingency plans to address a potential loss of automated processing. Without adequate disaster recovery and contingency planning, including required user-area plans, the Court is at risk of having their automated systems be disrupted or lost. A loss of processing capabilities could adversely affect the Court's ability to perform its functions and could result in significant delays in processing caseloads.

The environmental deficiencies existing at the Courthouse place even more emphasis on the need to develop a detailed business continuity plan should mission-critical applications become unavailable for an extended period of time. 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 application 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 warrant information. The Court would also be unable to confirm that fines, fees, and penalties were being collected by the Probation Department; and it would be unable to access all trial court dispositions regarding criminal cases. Given the fact that the Court will be moving to an automated case management system by the end of 2003, it is imperative that disaster and contingency plans be developed and implemented. The absence of a comprehensive recovery strategy could seriously affect the Court's ability to regain critical and important data processing operations should significant disruptions impact the Court's automated systems.

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 the Court the importance of developing an individual continuity plan should automated systems become unavailable for an extended period of time. In addition, it is our understanding that sufficient resources were not available to Court management to make business continuity planning a priority.

Recommendation:

In conjunction with the AOTC, the WDC should implement procedures to provide reasonable assurance that the criticality of automated 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 automated systems. Based on the results of the

assessment, the Court should proceed with the development of a written business continuity plan for its critical and essential functions. If feasible, the Court, at a minimum, should develop user area plans should mission-critical applications be unavailable.

The business continuity plan should document the Court's recovery strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. We further recommend that the business continuity plan be tested, then periodically reviewed and updated, as needed, to ensure that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members who must be trained in the execution of the plan under emergency conditions.

Auditee's Response:

Due to the anticipated high cost of a comprehensive business continuity plan, the AOTC would have to be the chief architect of such a plan. Where the Attleboro District Court maintains the server for the Warrant Management System of the Wrentham District Court, perhaps it would be prudent to design a continuity plan focusing more on those courts where the Warrant Management servers are located. The Clerk-Magistrate's office will be most helpful in implementations of such a continuity system once a basic design and direction are established by the AOTC. We firmly agree that such a plan is necessity of the future.

With regards to a recovery plan, this should also be directed to the location of the server rather than the District Court itself. The server is the conduit by which the court accesses the Warrant Management operations.

The relocation of the telecommunication room, as discussed in topic #1, would also assist this Court in its development of a continuity plan (as) most major casualties associated with a basement level operation would be eliminated. Unfortunately room on the first floor of this building is very limited and it is unlikely that the County Commissioners would vote such a change.

Auditor's Reply:

We understand that the Court is aware of the need for business continuity planning for its mission-critical and essential applications. We acknowledge that the Attleboro District Court houses the file server utilized by Wrentham District Court. However, we urge WDC management to work in conjunction with AOTC and the Attleboro District Court in developing a comprehensive business continuity plan. We recommend that plans and procedures be established to address business continuity planning, and are periodically reviewed and updated as necessary. This is especially critical in the future as the Court increases its reliance on information technology in performing its primary business functions.