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. 2003-1198-4T

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

July 1, 2001 through November 7, 2003

**OFFICIAL AUDIT REPORT**
**MAY 21, 2004**

2003-1198-4T

TABLE OF CONTENTS

# INTRODUCTION

The Brockton District Court (BDC) is organized under Chapter 211B, Section 1 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 and most civil matters for the City of Brockton, and for the towns of Abington, Whitman, Bridgewater, West Bridgewater, and East Bridgewater. The Court also provides office space for staff members of the Administrative Office of the Trial Court (AOTC) including the Security Department and the Court Facilities Bureau as well as the Office of the Plymouth County District Attorney. The Court, during the period from July 1, 2001 to October 2003, processed revenues of approximately $8,976,000 from various sources and assessments, court costs, restitution, and fines.

Chapter 478 of the Acts of 1978 reorganized the courts into seven Trial Court departments, including the District 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 the individual courts, provides internal control guidelines, 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 115 microcomputer workstations, of which 46 were in the Clerk-Magistrate's Office, 44 in the Probation Department, 17 in the courtrooms and 8 in the Judge's Lobby. In addition, there were 21 network printers located in the Court. The workstations and the network printers were connected to an AS/400 server located in a server room at the Court. In addition to providing network access to AOTC's application systems the AS/400 supports the Judicial Management System (JMS), which is a comprehensive application system used for processing and managing information concerning criminal cases that flow through the Brockton District Court. The major components of the JMS are Criminal, Probation, Cashiering, and Accounting.

The Court is linked through T1 lines to file servers in Cambridge and AOTC's wide area network (WAN). The WAN allows connectivity to the IBM Netfinity file server located at the AOTC data center in Cambridge. Other than the in-house JMS system, the primary application

systems used by the Court are the Basic Court Operations Tool application (BasCOT) and the Warrant Management System (WMS), which are maintained by AOTC, and the Criminal Activity Record Information (CARI) system, which is maintained by the Office of 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 JMS to manage information concerning criminal cases and the accounting and cashiering of funds collected, WMS to track warrants issued from all courts under the jurisdiction of the AOTC, and the BasCOT system to record docket information for all civil cases and generate various civil forms. The Probation Department also uses the JMS System's Probation Module and the CARI system to access information on all dispositions from courts regarding criminal offenses and restraining orders.

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

We performed an audit of selected information technology (IT) general controls at the Brockton District Court (BDC) from June 12, 2003 through November 7, 2003. The audit covered the period of July 1, 2001 through November 7, 2003. The scope of our audit included an evaluation of IT-related controls pertaining to the adequacy of documented IT-related policies and procedures, physical security, environmental protection, logical access security, inventory control of IT-related assets, business continuity planning, and on-site and off-site storage of backup copies of computer media.

### 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 to the Court's automated systems. Further, we sought to determine whether the BDC, 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 sought to determine 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.

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 an IT-related risk analysis and assessed the strengths and weaknesses of the IT control environment, and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To evaluate the IT internal control environment, we assessed the extent to which BDC had developed, implemented, and documented formal IT-related internal control policies and procedures. We interviewed senior management, reviewed and analyzed documentation, and assessed relevant internal controls. We reviewed BDC's organizational structure and primary business functions, and documented overviews of internal control areas for selected IT activities identified in our audit scope and audit objectives. Our work was focused on the Court's IT facilities and did not include a review of AOTC's IT-related management structure, IT operations or facilities. We requested and received AOTC's formal IT-related internal control guidelines that included policies and procedures. We also downloaded policies and procedures memos that were available on the Trial Court's website.

To evaluate physical security, we interviewed management and security personnel, requested written policies and procedures, and performed walkthroughs of the Courthouse, the server room, and selected telecommunication closets. We examined the existence of controls, such as the Simplex keycard system, motion detectors, and intrusion alarms. To evaluate physical security over the Simplex keycard system, we completed a keycard system questionnaire and interviewed Court personnel regarding the procedures used in gaining a simplex card to access the Courthouse. We obtained a Simplex cardholder listing and compared all of the BDC cardholders to an employment listing from the Brockton District Court to verify that all cardholders were current employees of the Court. Our review of cardholders was limited to BDC employees, not other employees located at the facility.

To determine the adequacy of environmental protection controls, we performed a walk-through and evaluated controls in the file server room, communication closets, and areas housing microcomputer workstations to assess the adequacy of controls. Through observation, documentation review, and selected tests, we determined the adequacy of environmental controls over areas housing IT equipment. We examined environmental controls over microcomputer workstations and closets that house telecommunication equipment including hubs and routers

located throughout the courthouse. Our examination included a review of general housekeeping, fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting; water detection; and humidity controls and air conditioning. In addition, we completed an environmental protection questionnaire with the appropriate Court staff.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume operations should the JMS, BasCOT, WMS, or CARI systems be inoperable or inaccessible for an extended period. With respect to business continuity planning and disaster recovery, we interviewed management from the Court to determine whether written, tested business continuity and disaster recovery and appropriate user area plans were in place and in effect; whether or not 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 generation of on-site and off-site storage of backup copies of magnetic media and hardcopy files, we interviewed the Court's staff regarding the creation of backup copies of computer-related media and hardcopy files pertaining to the JMS application system. We requested and reviewed the Court's documentation of their strategy for backup and restoration, which was included in the "AS/400 Disaster Recovery of the System" handbook. We interviewed auditee personnel responsible for full back-up procedures in place for the JMS application system to assess the adequacy and completeness of the procedures.

Our test of logical access security included a review of procedures to authorize, activate and deactivate access privileges to the JMS system and to the systems residing on the AOTC file servers. To determine whether only authorized employees could access the automated systems, we analyzed a list of current access accounts for individuals authorized to access JMS, WMS, CARI, and BasCOT, and compared them to current BDC personnel records. We performed the test by cross-referencing JMS, WMS, CARI, and BasCOT users to the personnel listing to determine whether users were current employees of BDC. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to BDC personnel. In addition, 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 IT-related resources were being properly safeguarded and accounted for, we reviewed and determined whether BDC had complied with the Administrative Office of the Trial Court's "Internal Control Guidelines" regarding inventory control and whether generally accepted inventory controls were in place. To assess compliance with AOTC's guidelines, we

obtained a listing of IT-related assets from AOTC and compared it to BDC's listing for accuracy and completeness. We also examined the Court's in-house inventory record to determine whether it contained the appropriate data fields to identify and describe IT resources, such as the value, location, date of purchase, date received, tag number, and whether the IT resource was in use.

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 had certain IT-related controls in place, controls pertaining to physical security, inventory control of IT resources, system access security, and business continuity planning needed to be strengthened. Although there was a general absence of documented policies and procedures to address IT-related functions performed at the Court, we found that adequate environmental protection controls were in place to provide reasonable assurance that IT resources and IT operations were operating in a proper environment to safeguard IT equipment, software, and data files. Our examination indicated that although IT control objectives regarding system access security would be met with respect to the Court's in-house application, the Judicial Management System (JMS), business continuity planning needed to be strengthened for the system.

Our review of controls over IT-related activities disclosed that the Court's primary IT functions were supported and maintained by the Information Technology Department of the AOTC, and by an AS/400 server running the Judicial Management System that was maintained by the Court. Although the Court did not have an established IT department, an employee having the job title of Operation Supervisor was responsible for supporting the JMS application and performing trouble-shooting with respect to IT-related issues regarding the AOTC applications. We found that the staff member's job description needed to be expanded to refer to these IT-related functions. In addition, although we determined that BDC had policies and procedures pertaining to the AS/400 and the JMS application, AOTC had provided only limited IT-related policies and procedures to the Court for the systems that it supported. We recommend that control documentation regarding IT-related activities and the use of IT resources be strengthened and that control requirements be communicated to court personnel. We further recommend that the Operation Supervisor's job description be updated to encompass assigned IT responsibilities.

With respect to physical security, our audit revealed that there were certain controls in place such as an intrusion detection system, surveillance cameras for public areas and the exterior of the building, and that all visitors were required to pass through a security checkpoint upon entering the courthouse. A Simplex keycard system was used for employees to gain admittance to court offices throughout the facility. In addition, only Court staff occupied areas where the microcomputer workstations, telecommunications closets, and the server room were located. However, we determined that the Court needed to document policies and procedures related to physical security controls and to strengthen controls over the maintenance of keycards for the

Simplex access security system to provide reasonable assurance that only authorized employees would have access into courthouse offices and restricted areas. We found that employees who were no longer employed by the Court were never required to turn in their access keycards.

We found that adequate environmental protection, such as smoke detectors and alarms, emergency lighting, fire extinguishers, and air-conditioning were in place throughout the courthouse. Our audit disclosed that the file server room, telecommunication closets, and the areas housing the microcomputer workstations were neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels were monitored and controlled by a computerized climate control system. We also found that the courthouse had a generator to provide emergency backup power. In addition, we found that the fire alarm system rings inside and outside the building, and is transmitted directly to the local fire department. We also found that the courthouse has enunciator panels to show the location of the fire. However, our audit disclosed that the uninterruptible power supply for the AS/400 was inoperable since the system's batteries had expired. Therefore, in the event of a power outage or surge, a managed shutdown of the AS/400 may not be possible, placing at risk the loss of critical information. To improve environmental protection, we recommend that the Court, in conjunction with AOTC, replace the batteries for the UPS system periodically.

At the time of our audit, the Court had not developed an adequate business continuity plan to provide reasonable assurance that access to on-line data and processing for the JMS application could be regained within an acceptable period of time should the Court's system be rendered inoperable or inaccessible. We determined that Court had implemented procedures for generating backup copies of magnetic media and storing the backup copies in secure on-site and off-site locations. Although the Court had a disaster recovery plan dated August 27, 2003 for restoring JMS operations, the plan was not adequately detailed and did not designate an alternate processing site.

We found that formal business continuity planning had not been performed to develop recovery strategies to restore computer operations in the event that automated systems were damaged or destroyed. In addition, we found that the Court, either on its own or 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. In addition,

the Court should develop user area plans to be implemented in concert with AOTC-managed recovery plans to address the loss of AOTC-based systems. In that regard, the Court had not been informed as to what procedures AOTC would follow or provided with a copy of AOTC's business continuity plan regarding system and network availability in the event of a disaster.

Our review of logical access security controls revealed that adequate control practices were in place to provide reasonable assurance that only authorized users were initially granted access privileges to the applications residing on the AOTC's file servers and the Court's AS/400 system. However, system access administrative procedures needed to be strengthened to ensure timely change or deactivation of access privileges no longer required or authorized. We determined that although BDC had written policies and procedures for system access security for the Judicial Management System (JMS), they had not been formally approved. Although access privileges for individuals no longer employed by the Court were being removed from the JMS system and the CARI application, we found that access privileges to the WMS and BasCOT were not being deactivated in a timely manner when Court employees were transferred from BDC or were no longer employed by the court. Our tests revealed that at the time of our audit, five BasCOT users and four WMS users were no longer employed at the Court. In addition, we disclosed that there were five generic access accounts to BasCOT for which an individual user had not been assigned to ensure accountability.

We found that Court personnel were not required to change their passwords and that 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. Furthermore, during our audit, the AOTC issued "Information Technology Policy #1" on August 13, 2003, which formalized certain policies regarding IT-related security for all court employees. However, due to the limited aspect of the technology policy and the confidential nature of the information residing on the Court's application systems, policies and procedures for password and user account administration should be strengthened and communicated to appropriate court personnel. Court management should ensure that the levels of access to the 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 that access security controls be monitored for compliance.

Our review of inventory control of IT resources revealed that controls needed to be strengthened to ensure the proper accounting of the IT resources. 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 the AOTC's master inventory and the Court's inventory of IT resources were not in agreement and needed to be reconciled, and that both listings lacked essential information, such as historical cost, acquisition dates, and status of equipment use. We determined that the Court's inventory list of IT assets, dated June 19, 2003, did not include 47 items and had not been reconciled to AOTC's master inventory list. In addition, the Court had not performed a physical inventory of its IT hardware items. We also found that nine IT resources installed at the Court and listed on the Court's inventory record did not appear on AOTC's master inventory listing. As a result of our inventory tests, we concluded that both the AOTC master inventory record and the Court's inventory were not sufficiently accurate and complete for BDC and that a complete reconciliation of the inventory lists to the physical assets and procurement and disposition records was necessary. In addition, the Court's management indicated that they were unaware of Chapter 647 of the Acts of l989 and its requirements for internal control, including inventory control. The Court was unable to provide us with any record of items received or disposed of during the period of July 1, 2001 to November 7, 2003, and did not maintain an inventory record of its furniture and equipment.

## AUDIT RESULTS

1. Physical Security

At the time of our audit, although the Brockton District Court did have certain physical security controls in place, physical security controls needed to be strengthened with respect to electronic keycard management. We found that all visitors were required to enter the courthouse through the main entrance and pass through a metal detector and that all packages were required to be screened by an x-ray machine. Motion detector and magnetic contact door alarms were activated during non-business hours to protect the courthouse. We determined that courthouse windows were alarmed and could not be opened from either inside or outside the courthouse. All intrusion and fire alarms were installed to sound at the nearby fire department and police station. We determined that the BDC had keycard security in place at all egress points throughout the courthouse. We observed that BDC security officers checked all bags and personal ID's in order to allow individuals access into the Court. However, we found that Court management had not established written physical security policies and procedures. In addition, although key cards were issued to authorized Court personnel, we found that temporary visitor cards had not been returned and that keycards for prior employees had not been deactivated to prevent unauthorized physical access. Furthermore, the default deactivation date for all users had been set for December 31, 2010, too far in advance at this time to provide any security value.

Our review of the Simplex keycard listing revealed that duplicate keycards had been issued and that a number of cards had not been deactivated for individuals no longer employed by the court. We determined that out of the 646 issued cards, 74 former court employees had 95 active simplex key cards, representing an error rate of 15%. Of the 74 former employees, 12 had two active keycards, three had three active keycards, and one had four active keycards. We also determined that out of the 646 active key cards, 51 keycards were assigned as “temporary” keycards with no associated user name, representing an error rate of 8%. Furthermore, we found that 54 keycards were assigned to 24 current employees. Of these employees, 18 staff members had two cards and six had three cards assigned to them.

During the audit, after our concern regarding keycard management was brought to the auditee’s attention, the Court promptly initiated corrective action. Our review of the modified access listing indicated that out of the 74 former court employees that had 95 active Simplex keycards, 91 of the keycards had been deactivated, leaving four unknown or transferred employees with active keycards. Regarding the 51 “temporary” keycards, after the Court’s

corrective action, only 19 had been deactivated, leaving 32 temporary cards in active status. Concerning the 24 current employees with duplicate cards, the Court had deactivated 20 cards out of the 30 duplicate keycards. Our review disclosed that former employees still have custody of keycards that could provide access to areas housing microcomputer workstations and that some former employees may still have access to the server room and the telecommunication closets. As a result, the Court must enhance their physical security policies and procedures to more adequately restrict physical access to only authorized individuals to prevent loss, damage, or theft of IT resources housed in various courthouse locations.

Generally accepted computer industry practices indicate that appropriate physical security controls need to be in place to ensure that the information technology assets are operating in a safe and secure operating processing environment and that IT-related resources be protected from unauthorized access, use, damage, or theft. Those control measures need to include preventive controls, such as authorization, locked areas, and identification and authentication, and detective controls, such as intrusion detection and alarms. Both the review of personal IDs and the keycard system rely on certain elements of authentication. By more closely administering the validity of keycard access, the Court will strengthen its authentication controls in this area.

Recommendation:

We recommend that further effort be made to fully address the keycard access deficiencies noted during the audit. We recommend that the Court establish documented administrative procedures for managing the keycard access system. The procedures should include requirements that prompt notification be made to the Chief Court Officer of all required changes in security access, including transfers of staff to other court facilities and terminations of employment, as well as prompt notification of lost or stolen keycards to enable timely deactivation of the access cards. The procedures should also require periodic reconciliation of the active access cards to current employees to identify any cards requiring deactivation. We recommend that individuals be assigned only one access card and that generic group access cards not be used. We recommend that steps be taken to ensure that no unauthorized “temporary” keycards remain active. In that light, we recommend that the Court consider deactivating all “temporary” access cards and then reactivate cards on an as needed and authorized basis with an appropriate time limit.

Auditee’s Response:

*The Auditee agreed with our audit recommendations, but chose not to respond in writing.*

Auditor's Reply:

We expect that Court management will initiate corrective measures to improve physical security by developing and implementing the recommended policies and procedures regarding keycard access and implement appropriate procedures to continuously monitor compliance with the established security requirements and standards.

2. System Access Security

Our audit revealed that system access security over the application systems used by the Court needed to be strengthened to ensure that only authorized users have access. We found that although adequate procedures were being followed in conjunction with AOTC to authorize and activate user privileges to the Court's automated systems, no documented policies and procedures regarding access security controls existed at the Court, and that password administration control procedures needed to be strengthened to ensure that user accounts no longer required were deactivated in a timely manner.

Although control practices regarding authorization and activation of access privileges were in place, procedures for changing or deactivating user privileges needed to be improved. At the time of the audit, we found there was no formal process, or standard electronic form, for notifying the AOTC of changes in employment status or terminations that would require user account access privileges to be changed. We found that access privileges to BasCOT and the WMS applications were not being deactivated in a timely manner when a Court employee was transferred or terminated employment from the Brockton District Court. Our tests revealed that access privileges had not been deactivated for five out of the thirty-three BasCOT users and for four out of thirty-eight WMS users who were no longer employees at the Court. Furthermore, we obtained evidence that the Court had submitted requests to AOTC to delete users or deactivate user accounts for individuals no longer employed at the Court. We found that the Court was unaware whether the user accounts had been deactivated. The Court was never provided with a confirmation that the user accounts were deactivated.

We determined that because management had not established a mandatory time frame for changing passwords, passwords had not been changed on a regular or frequent basis for the AOTC-supported applications. For application systems available through Court workstations, we found that passwords had not been changed in some cases for periods ranging from five to ten years. Furthermore, access security functions were not being used to prompt users to change their passwords for access to the BasCOT and WMS applications. In addition, there was no minimum length of characters for passwords. We found that password composition, length, and

frequency of change needed to be reevaluated, formally documented, and communicated to all users. Generally accepted access security procedures and password syntax rules require that passwords be comprised of at least eight alpha/numeric characters, not be easy to guess, be of sufficient length, and be changed periodically. In addition, authorization and authentication mechanisms should be reviewed and maintained to support security administration.

Access to computer systems, program applications, and data files should be authorized on a need-to-know, need-to-perform, and need-to-protect basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact the individual's level of authorization. Appropriate notification procedures should be in place to ensure that access privileges are modified in a timely manner when changes occur in job responsibilities or employment status.

The Commonwealth of Massachusetts' Internal Control Guide for Departments, promulgated by the Office of the State Comptroller, states in part " . . . an employee's password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility." In addition, computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for security administration and proper protection of information assets. The policies and procedures should address authorization for system users, establishing and activating user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access. Lastly, appropriate mechanisms need to be in place to provide assurance that security policies and procedures are in effect to ensure that only authorized users have access to automated systems and on-line data files.

The failure to fully document and implement appropriate system access security policies and procedures places critical systems and data files at risk to unauthorized access, modification, deletion, or loss of confidentiality. Given the nature of the Court's activities and operations and the sensitivity of information captured, stored and processed by the computer systems, access security to IT resources and systems is a critical IT-related function. As such, the viability of authorization and authentication mechanisms is extremely important to ensuring that only appropriate access is provided. In addition, access security and user accounts should be reviewed on a relatively frequent basis.

Recommendation:

We recommend that the Court, in conjunction with AOTC, document and formalize policies and procedures regarding access security controls. We recommend that the Court's department

heads determine whether access privileges granted to Court staff are appropriate to their job responsibilities. The review should be conducted in conjunction with AOTC's security administrator on a periodic basis. We also recommend that the Court, in conjunction with AOTC, establish a formal mechanism to notify AOTC's Help Desk or security staff of changes in the status of BDC employment or employee responsibilities that requires timely deactivation or changes to user privileges. In addition, we recommend that policies and procedures regarding deactivation of access privileges be extended to address other changes in employee status that would impact and provide access, such as leaves of absence and job transfers.

We recommend that procedures for creating, assigning, monitoring, and deleting of passwords be formalized, and that the frequency of password changes regarding all Court applications be established and communicated to all users. We recommend that access procedures and password syntax rules be established or enhanced to include password composition, rules of use, password confidentiality, password length, frequency of changing passwords, responsibility for safeguarding passwords, authorization procedures, and timely notification in changes in employment or authorization status. Procedures should also be established to ensure that access security is appropriately monitored and evaluated. Policies should advise users not to write down passwords and prohibit the sharing of passwords.

Auditee's Response:

*The Auditee agreed with our audit recommendations, but chose not to respond in writing.*

Auditor's Reply:

We encourage the Court to work with the AOTC's IT Department to evaluate security and implement and enhance system access security controls. We believe that efforts in this area will strengthen password administration and user account management.

3. Business Continuity Planning

Our audit revealed that the Court, in conjunction with the AOTC, had not developed a formal business continuity or user area 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, including the JMS application system, to determine the extent of potential risks and exposures to business operations should automated systems be rendered inoperable or inaccessible.

Although we found that procedures for both on-site and off-site storage of backup media for the JMS application system were in place, the existing disaster recovery plan did not adequately outline a viable recovery strategy for restoring operations at a designated alternate processing site. In addition, although the AOTC generated and stored backup copies of magnetic media off-site for the business functions processed through its file servers, the absence of an alternate processing site places AOTC recovery efforts at risk should the AOTC primary data center be render inoperable or inaccessible. However, our audit revealed that the Court, in conjunction with AOTC, had not developed user area contingency plans and a comprehensive recovery strategy 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 processing at a degraded level and not being able to recover their systems. A loss of processing capabilities could adversely effect the Court's ability to perform its functions and could result in significant delays in processing caseloads.

We found that backup procedures were in place for the mission-critical applications operating on the AOTC's file servers which support the WMS and the BasCOT. The CARI application systems have backup procedures administered by the Office of the Commissioner of Probation in Boston.

Since there was no clear recovery strategy for networked application systems running through AOTC, our review focused on the Court's procedures to ensure the availability of information residing on the in-house AS/400. Although the Court was able to provide us with a documented, but unapproved, disaster recovery plan for the JMS application, the plan did not adequately address alternate site processing, and had not been formally reviewed, tested, and approved. The Court had not included in the plan an alternate processing site to be used in case of a disaster. At the time of our audit, the Court indicated the possibility of Barnstable District Court as an alternate processing site, since they had the same JMS system and IT platform.

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 BasCOT and Warrant Management application systems operated by AOTC's file servers, and the CARI system operated by the Commissioner of Probation, would be hindered. Without access to these applications, the Court would be delayed from obtaining critical information, such as outstanding warrant information. The Court would also be unable to access all Trial Court dispositions regarding criminal cases.

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 and senior management and system user involvement with IT functions to help ensure a clear understanding of information system requirements, determinations of system criticality, and associated risks and exposures. Well communicated and cooperative efforts are necessary to ensure 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 assess the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could render systems and networks inoperable or inaccessible, the cost of recovering the systems, and the likelihood of occurrence of the threats.

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. The entity should assess the extent to which it is dependent upon the continued availability of information systems for all processing or operational requirements and should develop its recovery plans based on potential disaster scenarios and 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 Court should implement procedures to provide reasonable assurance that the criticality of automated systems is evaluated and that business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the IT environment. The procedures should require that, if warranted, appropriate business continuity or contingency plans are developed for automated systems. We recommend that the

Court enhance the existing disaster recovery plan for the JMS application system and develop user area plans to be used in concert with AOTC's recovery efforts for AOTC-based systems.

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 required time frames. We further recommend that the business continuity plan be tested and periodically reviewed and updated, 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:

*The Auditee agreed with our audit recommendations, but chose not to respond in writing.*

Auditor's Reply:

We believe that the Court will be able to strengthen its business continuity plan for JMS and develop appropriate user area plans in concert with AOTC's IT Department. Efforts in this area will help ensure adequate system availability and provide reasonable assurance that critical data processing operations could be regained effectively and in a timely manner.

4. Inventory Control

At the time of our audit, we found that IT-related inventory control needed to be strengthened to provide for the proper accounting of the Court's IT resources. Our examination of the AOTC master inventory record for computer equipment and the BDC inventory of IT resources indicated that the inventory listings were not in agreement and needed to be reconciled. Although our audit revealed that IT-related equipment at the Court had a description of the IT resource, location, vendor serial numbers, and state asset tag numbers, our audit tests revealed that the inventory record was not current, accurate, and complete.

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 of our audit, the Court had performed a physical inventory of IT hardware assets to assist in verifying their inventory record. The Court could not provide any evidence of taking an annual physical inventory of all fixed assets.

Our examination of the inventory record of the Brockton District Court provided by AOTC, consisting of 167 IT-related items, revealed that there was incomplete data, such as historical cost, acquisition dates, installation dates, and status of IT resources. Our test of the AOTC master inventory record disclosed that 47 IT-related items were not included on the Court's in-house list, and nine items from a total of 129 items on the Court's in-house inventory list were not found on the AOTC master inventory record. 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 that, "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 with appropriate information on the location and the status recorded.

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 and complete inventory record may hinder the Court's ability to manage IT-related resources and to detect loss or theft of IT-related assets. In addition, the lack of an up-to-date and accurate inventory hinders the Court's ability to assess its future technology and configuration needs.

Recommendation:

The Court, in conjunction with AOTC, should enhance controls over its inventory records to ensure that a perpetual inventory of fixed assets, including IT resources, is maintained. We

recommend that the inventory of IT resources include historical cost, acquisition dates, location of equipment, and equipment status. Additionally, the Court should include control practices regarding the maintenance of a perpetual inventory, and perform an annual reconciliation of all physical assets.

We recommend that the Court comply with the policies and procedures documented in the AOTC "Internal Control Guidelines" pertaining to inventory control. Specifically, the Court should periodically reconcile their inventory 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.

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

Auditee's Response:

*The Auditee agreed with our audit recommendations, but chose not to respond in writing.*

Auditor's Reply:

The Court should follow the recommendations noted above to ensure adequate inventory controls for IT resources.