The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

NO. 2007-0045-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT
THE MASSACHUSETTS COMMISSION AGAINST DISCRIMINATION

June 1, 2003 through October 30, 2006

OFFICIAL AUDIT REPORT

JUNE 30, 2008

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Commission Against Discrimination (hereinafter referred to as MCAD) is organized under Chapter 6, Section 56 of the Massachusetts General Laws (MGL), as amended, and operates under the purview of the Executive Office for Administration and Finance (EOAF) under Chapter 7, Section 4G of the MGL. The MCAD traces its origins to the mid-nineteenth century when the Commonwealth enacted laws prohibiting discrimination in education and public housing. The modern Commission was established in 1946 when the Massachusetts Legislature passed the Fair Employment Practices Act and created the Fair Employment Practices Commission to enforce the legislation. In 1950, the Commission's name was changed to the Massachusetts Commission Against Discrimination.

As of April 2007, Section 56 of Chapter 6, as amended, of the Massachusetts General Laws placed MCAD under the purview of the Office of the Governor. The MCAD is comprised of three Commissioners appointed by the Governor for three-year overlapping terms, and is staffed by the equivalent of 65 full-time employees, nine outsourced staff, and 10 interns hired to assist the staff throughout the year. An Advisory Board, currently consisting of three members, appointed by the Governor, counsels the Commission and the Governor regarding policy issues and reports on the implementation of MCAD programs and policies.

The MCAD's primary mission is "to ensure equality of opportunity by enforcing the Commonwealth's anti-discrimination laws in employment, housing, public accommodations, access to bank and retail credit, mortgage lending, and education"." The Commission works to eliminate discrimination and advance the civil rights of the Commonwealth's citizens through law enforcement activities, including filing of complaints, investigations, mediations, hearings, and litigation and outreach, such as training sessions and testing programs. According to the MCAD, the Commission's authority to enforce anti-discrimination laws was strengthened through changes to its statutory authority that allowed the Commission to charge fees for training services for workplace and housing discrimination prevention programs. Regarding the adjudication of cases during the 2007 calendar year, 3,413 new cases were filed, 2,845 cases were closed, and 2,928 remained active.

For the 2007 fiscal year, MCAD's appropriation was $4,175,386 including a direct budgetary appropriation of $2,274,386 and retained revenue of $1,901,000. The retained revenue account, capped at $2,482,071, allowed the MCAD to retain and spend revenues for services provided to the United States Department of Housing and Urban Development and the Equal Employment Opportunity Commission. The federal monies were used to pay the salaries of one-half the Commission's staff. Further, the MCAD's fiscal year 2007 appropriation included a retained revenue account, capped at $14,089, obtained

from fees charged for training and certification of diversity trainers in conjunction with its discrimination prevention certification program. The MCAD maintains an administrative office in Boston and a satellite office in Springfield. Citizens can also file complaints at the Worcester City Hall.

At the inception of our audit, MCAD's IT operations consisted of Management Information Services (MIS) and database operations related to the Case Management System (CMS). MIS was staffed by the network administrator and an assistant network administrator, and database operations were managed by a program coordinator and one additional staff. In July 2006, MCAD signed an agreement with the Executive Office for Administration and Finance's Information Technology Division's (ITD) to manage the Commission's network in Boston. Subsequent to the agreement between MCAD and ITD, a part-time Commission staff member continued to address database functions for the CMS. At the close of our audit, the Commission's agreement with ITD was in effect.

MCAD's computer operations were supported by two file and print servers, a SQL (Standard Query Database) server, and a PowerVault storage device used for backup of magnetic media installed in the file server room in Boston. The three servers and storage device were connected to 88 microcomputer workstations, of which 60 were leased and approximately 28 were purchased, configured in a local area network (LAN). A Dynamic Host Configuration Protocol (DHCP) server installed at the field office in Springfield was connected through a dedicated T-1 line to the servers in Boston. The DHCP server assigns Internet Protocol (IP) addresses to hardware connected to the network, authenticates logon IDs and passwords, and extracts data from the databases in Boston so that Case Management System users can view cases online and perform appropriate functions. The ITD's domain controller authenticates logon IDs and passwords for all state agencies, including MCAD. A standalone Simplex file server installed in the Boston file server room controlled physical access to the Commission's business offices and hearing rooms. MCAD's Housing Unit interfaced electronically with the federal government's Housing and Urban Development database server on which housing discrimination complaints reside. The file servers installed in Boston were connected through a wide area network (WAN) to ITD's mainframe, which provides connectivity for access to the Web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system.

The primary application used by MCAD to support its mission-critical business functions is the Case Management System (CMS). According to MCAD's Annual Report, as of 2003, the CMS "came on-line at the end of 2001, and it was first used for intake in 2002. . . ." . The CMS is comprised of two components, document processing that enables a user to view documents on-line, retrieve, and review files, and an automated process that tracks and monitors active cases. The CMS is used to manage and

control MCAD cases, and improve document imaging and workflow. In May 2007, MCAD completed the modification of the CMS to accept scanned-in documents, convert them to Portable Document Format (PDF), and store them in a dedicated server. Furthermore, the Commission used business-related applications, such as word processing to process daily administrative functions.

Our Office's examination of controls focused on selected general controls, such as physical security, environmental protection, system access security, inventory control over IT resources, and business continuity planning, including on-site and off-site storage of backup copies of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Massachusetts Commission Against Discrimination for the period June 1, 2003 through October 30, 2006. The audit was conducted from June 13, 2003 to November 5, 2004 and from December 15, 2005 to October 30, 2006. The scope of our audit included a review of the organization and management of IT operations. We examined control practices, procedures, and devices regarding physical security and environmental protection at the administrative offices and the file server rooms in Boston and the Commission's satellite office in Springfield. We reviewed and evaluated system access security to MCAD's automated systems. In addition, we examined inventory control practices for computer equipment and software.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the automated systems. With respect to normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning, including the provisions for on-site and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT-related resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion. We sought to determine whether adequate physical security controls were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of IT assets. In addition, we determined whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to network resources, including the Case Management System, which is the Commission's primary application used to process complainants' cases, and other business-related office applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. We determined whether sufficient environmental protection controls were in place to provide a proper IT environment and to prevent and detect damage or loss of IT resources. Another objective was to review and evaluate control practices regarding the accounting for and, when appropriate, reporting on computer equipment and software.

We sought to determine whether adequate business continuity planning had been performed and whether disaster recovery and business continuity plans were in place to restore mission-critical and essential business operations in a timely manner should the automated system be unavailable for an extended period. In conjunction with our examination of business continuity planning, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of MCAD's mission and business objectives. Through pre-audit interviews with the managers and staff and reviews of statutory authority, Commission's website, business operations, and selected documents, such as the annual reports for 2003 through 2006, we gained an understanding of the primary business functions that were supported by the automated systems. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. Furthermore, we gained an understanding of the significant manual components of the Commission's business functions, such as interviewing complainants and conducting hearings.

As part of our audit work, we reviewed and evaluated the organization and management of IT operations at the administrative office in Boston. In that regard, we reviewed relevant policies and procedures, reporting lines, and IT-related job descriptions. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives, such as the Commission's "Internal Control Plan," dated September 2001.

We interviewed MCAD management to discuss internal controls regarding physical security and environmental protection over and within the administrative offices and file server rooms housing the automated systems and the on-site and off-site storage areas in Boston and in Springfield. We inspected the administrative office and the file server room in Boston, reviewed relevant documents, and performed selected preliminary audit tests. In conjunction with our review of internal controls, we performed a high-level risk analysis of risks and threats to selected components of the IT environment. In addition, we observed a demonstration of selected functions of the Case Management System.

To determine whether physical access over computer equipment was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the administrative offices in Boston and Springfield. We reviewed physical security and environmental protection over IT equipment through inspection and interviews with MCAD management and staff. To determine whether adequate controls were in effect to prevent and detect unauthorized access to the offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, intrusion detection systems, the presence of a security officer at the entrance to the buildings housing MCAD offices, a receptionist at the entrance point to the administrative offices, and whether visitors were required to sign in and out. We reviewed access control procedures, such as the list of staff authorized to access the administrative offices and file server rooms in Boston and Springfield, and control practices regarding the management of card-key access to the building housing MCAD offices, file server rooms and other restricted areas within the administrative offices in Boston and Springfield. Furthermore, we reviewed physical access controls to the network closet that provides connectivity to MCAD offices and file server room in Springfield. In conjunction with our review of physical access security, we reviewed control procedures associated with the Simplex system that controls access to the administrative office and hearing rooms in Boston.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS), surge protectors for automated systems, and emergency power generators and lighting installed in the administrative offices and file server rooms in Boston and Springfield. Moreover, we reviewed selected environmental protection controls within the network closet located in Springfield. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer-related equipment. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the file server room. Furthermore, we reviewed control procedures to detect and prevent water damage to automated systems, official records, and on-site storage for backup copies of magnetic media.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer workstations. To determine whether MCAD's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the Director of Administration and the

Network Administrator and evaluated selected access controls to the network and applications available through the network and microcomputer workstations. In addition, we reviewed MCAD's control procedures regarding remote access privileges to the network. We determined whether MCAD's internal control documentation included control practices, such as a risk assessment, an acceptable use policy for IT resources, and security awareness training. We interviewed MCAD managers and staff and ITD personnel regarding control and monitoring of the Commission's network, including security procedures regarding system access to the automated systems.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the Network Administrator responsible for access to the automated systems on which the Commission's Case Management System and other business-related applications operate. In addition, we reviewed control practices used to assign MCAD staff access to network resources, including the CMS. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. Because MCAD did not maintain documentation authorizing users to be granted access to automated systems until December 2003, we determined whether the Commission was providing proper authorization to employees and outsourced staff hired after December 2003. To determine whether all users with active privileges were current employees or outsourced staff, we obtained the list of individuals granted access privileges to network resources, such as the CMS and other business-related applications, and compared all users with active access privileges, as of September 30, 2003 and June 30, 2006, to the personnel roster of current employees and outsourced staff. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so required, we reviewed the frequency of the changes.

Regarding inventory control over IT resources, we first reviewed formal policies and procedures promulgated by the Massachusetts Office of the State Comptroller (OSC) regarding inventory control. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed the roles of the Director of Administration and the Network Administrator regarding the accounting for computer equipment and software, reviewed the inventory control procedures for IT resources, and performed selected tests. During our initial fieldwork, we obtained the hardware inventory record, as of September 30, 2003, from the Network Administrator. We determined whether computer equipment installed at the administrative offices in Boston and Springfield was tagged with state identification numbers and whether the Commission's inventory record accurately reflected tag

numbers and equipment serial numbers. We reviewed the inventory record to determine whether appropriate "data fields," such as state identification number, manufacturer's model number, serial number, location, and cost were included for each piece of equipment listed in the record and whether the record provided sufficient information to identify and monitor computer equipment. We determined whether appropriate information, such as version number and cost were listed on the software inventory record whether the software record was current, accurate, and complete.

We reviewed Generally Accepted Accounting Principles (GAAP) Fixed Asset reporting requirements for state agencies and departments required by the Office of the State Comptroller (OSC), as of the date of our audit, and determined whether MCAD had complied with the requirements. GAAP Fixed-Assets are comprised of property and equipment, including hardware and software, with an historical cost of $49,999 or more and an economic life of one year or more.

To determine whether the IT-related inventory record, as of September 30, 2003 accurately reflected computer equipment installed in Boston and Springfield, we initially reviewed the 305 pieces of computer equipment listed on the record. We selected 226 (100%) workstations, servers, and printers listed on the record, located in Boston and Springfield, for review. Of the 305 pieces of equipment listed on the inventory record, eight consisted of duplicate items and 71 consisted of a variety of electronic and communication equipment. We compared the tag numbers and serial numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record, and determined whether serial numbers were accurately recorded. Furthermore, we confirmed selected pieces of equipment installed at the Boston office to the hardware inventory record. In addition, we confirmed file servers and workstations listed on the hardware inventory record to the actual equipment installed at the field office in Springfield.

Prior to our review of the June 30, 2006 inventory record, we determined whether any significant changes had been made to OSC regulations. We compared computer equipment; specifically workstations, servers, and notebook computers listed on the September 30, 2003 inventory record to the equipment listed on the June 30, 2006 inventory record and noted any changes in the records. We also compared the hardware record to additional lists provided by the Commission that documented workstations installed at the Boston and Springfield offices and noted discrepancies between the two documents. We confirmed a judgmental sample of tag numbers for seven workstations listed on the hardware record, as of June 30, 2006 to the workstations installed in the Springfield office. We did not test the 60 leased workstations installed in Boston. We reviewed the software inventory records, as of September 30, 2003, January 1, 2006, and June 30, 2006 provided to us by the Commission. To determine whether all software

purchased for use by the Commission during the 2000 through 2003 fiscal years and the 2006 fiscal year, was listed on the records, we compared software listed on the MMARS records and selected purchase documentation to the software inventory records. Moreover, we compared the software listed on the inventory system of record, as of June 30, 2003 and September 30, 2003 to the inventory system of record, as of June 30, 2006.

To determine whether the hardware inventory records, as of September 30, 2003 and June 30, 2006, respectively, accurately reflected computer equipment purchased during the 2000 through 2003 fiscal years and the 2006 fiscal years we initially selected judgmental samples of purchases from both periods. We selected purchase documentation that included computer equipment, such as servers, workstations, and notebooks, purchased during fiscal years 2001, 2002, and 2003, with total listed values of $61,32, and $12,706, and a videoconferencing system, with a listed value of $140,529, purchased during fiscal year 2006, and compared computer equipment listed on the purchase documentation to items listed on the hardware inventory records, as September 30, 2003 and June 30, 2006, respectively.

We reviewed the MCAD's "Declaration of Surplus Personal Property," as of June 23, 2005 and April 26, 2006. We compared five pieces of equipment identified as file servers and one item listed as a tape drive on the inventory record, as of September 30, 2003 to the inventory record, as of June 30, 2006 and the surplus property records, as of June 23, 2005 and April 26, 2006. In addition, we compared notebook computers listed on the hardware inventory records, as of September 30, 2003 and June 30, 2006, to the notebooks listed on the surplus property records and noted discrepancies between the surplus property and hardware inventory records. Furthermore, we reviewed control procedures regarding the disposition of surplus property.

With respect to notebook computers, we initially determined the role of the Network Administrator regarding the management and control of the computers. To gain an understanding of control procedures regarding the distribution to and return of the computers from Commission staff, we interviewed the network administrator and reviewed control procedures for assigning notebook computers to Commission staff. We reviewed and evaluated instructions regarding the process of sign-out and sign-in for the notebooks. We reviewed the notebook computers listed on the inventory records, as of June 30, 2003 through September 30, 2003, and June 30, 2006.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to restore mission-critical and essential operations in a timely manner should the automated systems be inoperable or unavailable for an extended period. We interviewed the Director of

Administration and the Network Administrator to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We reviewed and evaluated MCAD's Continuity of Operations (COOP) plan, as of January 2006. According to the Massachusetts Emergency Management Agency (MEMA), "the COOP was prepared in accordance with Department of Homeland Security Headquarters COOP Guidance Document, as of April 2004, that provides a structure for formulating a COOP plan; Presidential Decision-67, 'Ensuring Constitutional Government and Continuity of Operations,' and Commonwealth of Massachusetts Executive Order No. 144 that requires all Commonwealth agencies and local communities to prepare for emergencies and disasters, and to provide emergency liaisons to MEMA for coordinating resources, training, and operations." We determined whether the COOP and other business continuity documents included sufficient information to support the resumption of the Commission's normal business operations in a timely manner.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we initially interviewed the Network Administrator responsible for generating backup copies of magnetic media. Moreover, we reviewed the adequacy of provisions for on-site and off-site storage of backup copies of mission-critical and essential magnetic media at the administrative offices in Boston and Springfield. We reviewed procedures for transferring to and retrieving backup media from the off-site storage location. During our subsequent audit work, we interviewed ITD personnel responsible for generating backup copies of magnetic media and we gained an understanding of ITD's plans for electronic transfer of backup to the Massachusetts Information Technology Center located in Chelsea, Massachusetts. We did not review ITD's backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting system (MMARS) and the Human Resources Compensation Management System (HR/CMS).

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

AUDIT CONCLUSION

Based on our audit of the Massachusetts Commission Against Discrimination, we determined that, except for written documentation, adequate physical security and environmental protection controls were in place at the administrative office in Boston and the satellite office in Springfield. We determined that although physical security and environmental protection controls over and within the file server room in Boston were adequate, certain environmental controls at the Springfield office's file server room needed improvement. We determined that, although appropriate controls regarding logon ID and password administration were in place, controls regarding authorization of users to access automated systems needed to be strengthened. We found that adequate controls were not in effect to provide reasonable assurance that IT resources would be properly accounted for and that IT processing could be regained within an acceptable period of time. We determined that there were significant weaknesses regarding inventory control over IT resources and in addressing business continuity planning.

Our audit revealed that appropriate physical security controls had been implemented over and within the administrative office in Boston to provide reasonable assurance that only authorized persons would have access to IT resources and that damage or loss would be prevented. For example, State Police were stationed at the main entrance to the building and card-key access was required for all employees to enter the building. With respect to the MCAD administrative office, a receptionist was located at the front entrance to the administrative office and unique card-keys were required to access the administrative office. The file server room in Boston was located in a non-public area, the room could not be accessed from outside the building, the door to the room was locked at all times, and access to the room was restricted to the Commission's IT staff and contracted staff from the Commonwealth's Information Technology Division.

Regarding the satellite office in Springfield, we found sufficient control practices regarding physical access security, such as security officers on duty within the State office building housing the administrative office, a receptionist on duty within the administrative office, and requirements that visitors sign in prior to admittance. The file server room was located in a non-public area.

We found that adequate environmental protection controls, such as smoke detectors and fire alarms, sprinkler systems, and an emergency power supply were in place in the building housing MCAD's administrative office in Boston to help prevent damage to, or loss of, IT resources. Our audit indicated that the file server room was neat and clean, temperature and humidity levels within the room were appropriate, and two uninterruptible power supply (UPS) devices were in place to permit a controlled shutdown and to prevent a sudden loss of data and hand-held extinguishers were located within the server

room. With respect to the satellite office in Springfield, we found that important environmental controls were in place, such as a UPS, appropriate temperature controls in the administrative office and file server room, a sprinkler system, and file servers were kept elevated to prevent water damage. We found that conditions within the network closet housing the Commission's network connections had improved since the inception of our audit. To strengthen controls, we recommend that MCAD install a fire extinguisher and smoke detector in the file server room.

Regarding inventory control practices, we found that MCAD did not provide reasonable assurance that IT resources were properly accounted for in the Commission's inventory system of record and, when appropriate, reported on, as required by statutory authority and associated regulations promulgated by the Office of the State Comptroller. We found that the Commission's system of record for hardware and software, as of September 30, 2003 lacked integrity and, as a result, could not be relied upon as a current, accurate, complete, and valid representation of the computer equipment on hand or software installed on automated systems. We could not estimate the value of the hardware record because costs were not entered for all the equipment; equipment was omitted from the record, and incorrect cost information was listed for certain items. We found that these deficiencies existed throughout the subsequent stages of our audit work. It is our understanding that the Commission initiated new inventory records for hardware and software in January 2006 that were not based on a review of actual equipment on hand or software installed on the systems. As a result, we determined that the inventory records for hardware and software, as of June 30, 2006 were not reliable. With respect to notebook computers, we determined that MCAD was not properly accounting for the distribution and return of computers from staff.

We acknowledge that the Commission complied with Operational Services Division requirements regarding designation of surplus property. To strengthen inventory control over IT resources, we recommend that MCAD gain an understanding of OSC requirements regarding proper accounting for and reporting on IT resources, maintain a perpetual inventory record, and conduct a physical inventory and reconciliation at least annually.

With respect to availability of systems, our audit disclosed that MCAD had not documented sufficient recovery strategies in order to provide reasonable assurance that normal business operations could be resumed in a timely manner should automated systems be unavailable for an extended period. Our audit indicated that the Commission had performed certain initial steps regarding business continuity planning, such as documenting procedures within the Continuity of Operations Plan, as of January 2006, to provide for essential functions at the alternate processing site, should its administrative office in Boston be inaccessible. To strengthen controls over business continuity planning, MCAD should conduct a risk analysis and criticality assessment; document various disaster scenarios and instructions to follow for

each occurrence; compile vendor lists; and address restoration of network resources. The plan should be distributed to appropriate Commission officials and staff, staff should be trained in the plan's use, and the plan should be periodically tested and modified when needed. We determined that, as of July 2007, MCAD, in conjunction with the Executive Office for Administration and Finance's Information Technology Division (ITD), had provided adequate off-site storage for backup copies of magnetic media residing on file servers.

With respect to system access security, we determined that although appropriate controls were in place and in effect to provide reasonable assurance that only current employees and outsourced staff were granted access to network resources, including the Case Management System, MCAD could not provide sufficient documentation indicating that all users granted access privileges to automated systems had been properly authorized. We found that although a framework for authorizing activation of access privileges to automated systems had been documented, with few exceptions, the procedures had not been formally implemented. To strengthen access security controls, we recommend that MCAD document control practices regarding authorization to access automated systems, activation of logon IDs and passwords, and deactivation of access privileges.

Our review of the Commission's internal control documentation revealed that MCAD's most current "Internal Control Plan" as of September 2001, needed to be updated. Specifically, documented control practices regarding physical access security, environmental protection, and systems access security needed to be developed and control practices regarding inventory control over IT resources enhanced. At the inception of our audit, the Commission had an appropriate and defined organizational structure for IT operations, assigned reporting responsibilities, and documented job descriptions for IT staff. During our audit, key IT staff, such as the Network Administrator and staff responsible for CMS database functions terminated employment at the Commission and their positions were left unfilled or filled with temporary replacements for a considerable period. Furthermore, we determined that the position of Director of Administration and Finance was filled on a part-time basis for the period June 13, 2003 to July 1, 2004. A full-time Director was hired in December 2004. We believe that the turnover in key IT staff and the absence of a full-time Director of Administration and Finance for an extended period contributed to the inability of MCAD to develop and maintain appropriate IT-related controls practices. In July 2006, the Commission contracted with ITD to manage the file servers installed in Boston. MCAD retained one part-time database administrator. At the close of our audit, the agreement with ITD remained in effect. We believe that this agreement will facilitate appropriate management and control over network resources and help maintain the availability of the Case Management System.

AUDIT RESULTS

1. Business Continuity Planning

Our audit revealed that MCAD had not implemented sufficient, documented recovery strategies or developed adequate resources to resume normal business operations in a timely manner should automated systems be rendered inoperable or unavailable for an extended period. We determined that MCAD had not documented related control practices, such as a risk analysis and criticality assessment, descriptions of various disaster scenarios and detailed instructions to follow regarding each potential disruption, user area plans, and procedures to restore automated systems. We noted that, at the beginning of our audit, MCAD stored backup copies in an off-site location. However, during our audit period the Commission suspended off-site storage of backup copies of magnetic media. Subsequent to the close of our audit, we found that as of July 2007, Executive Office for Administration and Finance's (EOAF) Information Technology Division was providing electronic backup of magnetic media residing on Commission file servers in Boston.

We believe that the Commission understood the need for business continuity planning and had documented certain control practices required by the Continuity of Operations Plan (COOP), as of January 2006. The purpose of the COOP was to "provide for the immediate continuity of essential functions of an organization at an alternate facility for up to 30 days in the event an emergency prevents occupancy of its primary facility." The COOP was prepared according to Department of Homeland Security guidance, Presidential directives for federal departments, and the Commonwealth's Executive Order No. 144 requiring agencies to prepare for emergencies and disasters and provide liaisons to the Massachusetts Emergency Management Agency. We found that the COOP addressed important elements integral to business continuity planning, such as a listing of essential business functions, designation of the Case Management System as the MCAD's mission-critical system; general requirements for relocation to and use of the emergency relocation site in Springfield (hereinafter referred to as the alternate processing site), and delegation of duties and responsibilities for continuity of operations to Commission officials and selected managers. However, control practices documented in the COOP needed to be significantly enhanced to provide sufficient support for the resumption of mission-critical and essential business functions. According to MCAD management, the COOP was designated as the Commission's business continuity plan.

We found that although the COOP had documented a series of potential disruptions to MCAD's business operations and had designated the Springfield office as the Commission's alternate processing site, a formal criticality assessment and risk analysis had not been performed. A risk analysis should identify the relevant threats that could damage the systems, the likelihood of the threat and frequency of

occurrence, the impact of the occurrence on the automated systems and related business functions, and the cost of recovering the systems. The risk analysis should be based on the Commission's current IT configuration and processing environment at the administrative office in Boston and satellite office in Springfield. In addition, we determined that that the list of disruptions identified in the COOP, such as severe winter storms, power outages, multiple explosions, civil disturbance, and credible threats that would force closure of MCAD offices, did not note other potential disruptions, such as fire or flood; did not differentiate between disruptions in the administrative offices in Boston and Springfield; and did not refer to risks to the IT environment or loss of automated systems, including network failure. Furthermore, the COOP did not include descriptions of service disruptions ranging from partial interruptions to major system failures; detailed instructions to address different types of service disruptions and time requirements to address recovery steps; or procedures to prevent or mitigate the potential damage.

Our audit indicated that although the Commission had designated the satellite office in Springfield as the alternate processing site to be used in the event that the Boston office was damaged or destroyed, no alternate site had been designated for the Springfield site should that office be unavailable for normal business functions for an extended period. According to the COOP "In general, the telecommunication and information system support provided at MCAD locations is available independently at the alternate processing site. It is imperative that the Senior COOP Official ensures that unique or critical information system requirements are considered in planning and, if appropriate, identified as capabilities to be provided by support organizations at the alternate site. MCAD offices shall maintain all necessary and up-to-date files, computer software, and databases required to carry out essential functions." We found that although the COOP included general instructions regarding preparation of, relocation to, and restoration of normal business functions, neither the plan nor any other documentation included detailed procedures regarding restoration of communication components for network operations, a schedule for the restoration of automated functions, written "user area" contingency plans for resuming critical and essential applications, and detailed training plans for appropriate staff for both the Boston and Springfield sites. Further, the Commission had not documented a vendor list or a contact list, including MCAD employees and ITD personnel, to be used in the event of an emergency.

We found little evidence that MCAD had tested recovery strategies documented in the COOP. According to the COOP, "a changing threat environment and recent events emphasize the need for COOP capabilities that enable the MCAD to continue its essential functions across a broad spectrum of emergencies. Federal Preparedness Circular No. 66 states that, " testing, training, and exercising of COOP capabilities are necessary to demonstrate and improve the ability of agencies to execute their

essential functions. The MCAD Tests, Training, and Exercises (TT&E) Program incorporates the three functional areas of testing systems and equipment, training personnel, and exercising plans and procedures." Contrary to these statements regarding testing, MCAD was unable to provide documentation regarding specific schedule of tests, test results, or any corrective action taken to address weaknesses in the plan. Tests should include the restoration of business functions not only at the Springfield office, but also at any additional alternate sites. Manual procedures should be included in the plan, the procedures should be tested, and appropriate staff trained in their use. Failure to adequately test a comprehensive business continuity plan hinders MCAD from attaining reasonable assurance that the recovery plan will effectively address various disaster scenarios. Moreover, the lack of tests of recovery strategies may impede the periodic review and modification of the plan. If the plan was not modified when needed, the Commission may not be able to rely upon the plan's current viability due to factors, such as changes in the risks and threats to the IT environment, IT infrastructure vulnerabilities, IT application systems, network and communication changes, security requirements, electronic interfaces, personnel, logistics, and organizational changes.

In June 2006, MCAD contracted with EOAF's Information Technology Division to maintain the Commission's file servers installed in the Boston Office. According to ITD management, as of July 2007, an electronic system was developed to transmit backup copies of magnetic media from Commission servers to servers at the Massachusetts Information Technology Center and, subsequently, to move physical tapes to an off-site location. Prior to July 2007, MCAD was storing backup tapes in an unlocked, non-fire proof cabinet in the file server room in Boston and was not providing off-site storage. Electronic transfer of backup copies and distribution of physical tapes to an off-site location reduces the risk that backup will be damaged or destroyed and provides reasonable assurance that, when needed during an emergency, will be available to support the Commission's mission-critical and essential functions.

The objective of business continuity planning is to provide reasonable assurance of the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for 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. Business continuity plans need to be developed to effectively address short, medium, and long-term recovery requirements. In the short term, mission-critical systems and services should be restored. Medium-term plans address

recovery of systems and services on a temporary basis; long-term plans involve the total recovery of the IT processing environment.

The business continuity plan should also incorporate detailed user area plans describing the procedures for user departments and their staffs to follow when changing to alternate-processing activities should a disaster render the automated systems inoperable. Further, the recovery plan should identify contingency procedures that could be used during an interim recovery period. The recovery plan should address procedures for the restoration of critical IT functions and should indicate the logical order of system implementation and integration. The plan should be distributed to appropriate staff, such as MCAD officials, senior management, and selected IT staff, and ITD staff. A copy of the plan should be stored in a secure off-site location and should be available in electronic and hardcopy form. MCAD should consider whether additional copies of the business continuity plan should be stored in other secure locations.

Recommendation

The Commission should strengthen business continuity planning by:

- Gaining an understanding of generally accepted computer industry standards, such as Control Objectives for Information Technology (CobiT) regarding a business continuity planning framework outlining business continuity, recovery and contingency objectives, and procedures for mission-critical and essential business operations. The business continuity planning framework includes a criticality assessment and risk analysis, policies; procedures; defined responsibilities; documented management control practices; organizational controls, such as steering committee, recovery teams, and oversight functions; and assurance mechanisms. Assurance mechanisms would include internal reviews, testing, and independent examination and verification. The framework should also include senior management assignment of enterprise responsibility for additional recovery strategies and adequate provisions for on-site and off-site storage.
- Performing an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes are evaluated and updated, if necessary. The risk analysis and criticality assessment should include all external partners, such as the federal government and outsourced services, such as ITD.
- Reviewing the list of disaster scenarios already documented by MCAD to determine whether all potential scenarios have been identified, and update the list accordingly with respect to the likelihood and impact of the scenarios at the administrative offices in Boston and Springfield, and the loss of the generation and storage of backup media performed by ITD. Ensure that recovery and business continuity strategies are documented or documented for each of the disaster scenarios identified.
- Reconfirming MCAD's understanding of the relative importance of business functions and the potential impact of a loss IT processing support. MCAD should formally rank mission-critical, essential, and less essential business process functions and IT processes for the development and update of disaster recovery, business continuity and contingency plans.

- Obtaining an understanding and adequate level of assurance of disaster recovery and business continuity plans for required services and support from all mission-critical and essential business partners, including and OSC, and third-party providers.
- Establishing a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, MCAD should establish targets for acceptable time periods by which mission-critical IT operations need to be recovered.
- Ensuring that appropriate resources are available at alternate processing sites, such as suitable hardware and communication equipment; supplies; adequate space in which to resume operations; backup copies of all required application programs, data files and system utilities; documented policies and procedures; and accommodations for sufficient personnel.
- Developing and performing appropriate levels of testing to provide MCAD with sufficient assurance as to the viability of recovery and business continuity plans. Once tests are completed, test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.
- Reviewing business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. We recommend that subsequent to testing the business continuity plan, the plan should be updated when needed to provide reasonable assurance that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members, including MCAD officials, senior management, IT staff, and ITD administrators and staff.
- Training MCAD staff in the execution of the business continuity plan under emergency conditions. Ensure that all key business process and IT management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.
- Maintaining on-site storage of backup copies of magnetic media in a physically secure location that is protected from environmental hazards.

Auditee's Response:

> *Recovery and Business Continuity Plan: MCAD will review its current plan to ensure that it is current and that all key personal have adequate skill and knowledge to carry out the tasks and activities outlined in the plan.*

Auditor's Reply:

We acknowledge that MCAD is aware of the need for business continuity planning for its mission-critical and essential application systems and are pleased management will review its current plan. However, we urge MCAD management to work toward developing a comprehensive business continuity strategy that will allow the restoration of systems in an acceptable period of time under various disaster scenarios. We recommend that recovery plans and procedures are established to address business continuity planning, and that the plans be periodically reviewed, tested, and updated as necessary.

2. Inventory Control over IT Resources

Our audit revealed that, with few exceptions, although physical security over automated systems at the administrative office in Boston and satellite office in Springfield was adequate, the MCAD could not provide reasonable assurance that sufficient control practices were in place and in effect to properly account for and, when appropriate, report on IT resources. Although staff had been assigned to maintain the inventory of IT resources and a significant number of pieces of computer equipment had been tagged with state identification numbers, we found significant weaknesses regarding the accounting for and reporting on MCAD's IT resources, as of June 30, 2006.

Deficiencies pertaining to asset-related control practices included, but were not limited to MCAD's failure to:

- develop formal policies and procedures regarding fixed-asset management, regarding an annual physical inventory and reconciliation, tagging of computer-related equipment, accounting for and monitoring of notebook computers, and accounting for surplus property;
- maintain a current, accurate, and complete inventory record for IT resources, including software;
- include appropriate fields such as cost, date of acquisition, or date of last update in its inventory system of record;
- enter appropriate IT-related GAAP Assets for MCAD into the MMARS Fixed Asset Subsystem, resulting in inaccurate and incomplete GAAP Reports and GAAP-related information reported to the Office of the State Comptroller for inclusion in the Commonwealth's Comprehensive Annual Financial Report;
- demonstrate that an annual physical inventory and reconciliation of IT-related assets had been performed;
- comply with the Internal Control Act, Chapter 647 of the Acts of 1989 regarding safeguarding of Commission's assets;
- comply with Office of the State Comptroller's asset-related internal control requirements, such as the "Internal Control Guide for Departments" and "MMARS Fixed Asset Subsystem User Guide";
- safeguard and properly account for notebook computers assigned to staff;
- comply with all Operational Services Division (OSD) requirements regarding designation and disposition of surplus property, and
- maintain a current, comprehensive internal control plan, including IT control practices, as required by state law.

We found that deficiencies regarding MCAD's system of record for hardware and software identified during our initial audit work conducted from June 13, 2003 through November 5, 2004 had not been corrected, as of June 30, 2006. Comprehensive controls were not in place and in effect to properly

account for IT assets. According to MCAD management, a lack of staff contributed to MCAD's inability to develop and implement control practices regarding the monitoring and control of its IT resources. We believe that MCAD management had not demonstrated sufficient understanding regarding the accounting for and reporting of IT assets.

a. Record-keeping Practices

Our audit indicated that, contrary to Office of the State Comptroller's written internal control guidelines for fixed-asset management, promulgated under the authority of the Internal Control Act, Chapter 647, of the Acts of 1989, MCAD's inventory system of record for IT resources, as of September 30. 2003 and June 30, 2006 lacked integrity and, as a result, could not be relied upon as a current, accurate, complete, and valid representation of the computer equipment and software. Furthermore, we found that the Commission was not properly accounting for notebook computers.

Regarding computer equipment, we found the hardware inventory record, as of September 30, 2003 was not current, accurate, or complete. Of the 305 items listed on the record, we tested 226 pieces of equipment, including servers, workstations, and printers to the actual equipment installed in the administrative office in Boston and satellite office in Springfield. The additional 71 pieces of equipment consisted of electronic and communication components, such as routers. (Eight pieces of equipment were duplicate entries.) We found that cost figures were not recorded for 88 (28.9%) of the 305 hardware items. As a result, we were unable to state the total value of the Commission's inventory. Furthermore, we found that "dates of service" were not listed for 87 of the 88 items. In addition, MCAD staff could not state definitively whether "dates of service" referred to 'date of acquisition," "installation date," or "date equipment placed in service."

Our test of computer equipment listed on the inventory record to the actual pieces of equipment revealed that tag and/or serial numbers for 19 (8.4%) of the 226 pieces of equipment reviewed did not match the numbers affixed to the actual equipment. Regarding the administrative office in Boston, we found that the description listed on the inventory record for four workstations did not match the pieces of equipment located at the office. We found that one notebook computer and one workstation that were listed on the record could not be located. Moreover, we found that one workstation that was located at the administrative office was not listed on the inventory record. With few exceptions, we could not confirm file servers listed on the hardware record to the actual equipment, because the information on the inventory record was insufficient to differentiate between various types of computer equipment, including servers and workstations.

Our audit disclosed that deficiencies regarding the Commission's system of record persisted through June 30, 2006, the completion date for our examination of inventory control practices. We determined that the inventory record, as of June 30, 2006 was also not current, accurate, and complete. We determined that the Commission did not maintain the inventory system of record on a perpetual basis. According to MCAD management, the Commission initiated a new inventory record in January 2006 that did not include equipment previously installed in the administrative offices and listed on the inventory record, as of September 30, 2003. We determined that three servers that were installed in Boston, as of June 15, 2006, were not listed on the June 30, 2006 inventory record. Furthermore, our review of purchase documentation indicated that a videoconferencing system, with a listed price of $140,529, purchased on June 22, 2006, was omitted from the record. The OSC requires that the initial entry of a fixed-asset record should be entered into the MMARS Fixed Asset Subsystem must be recorded onto the system within seven days of acquisition. In addition to equipment not being listed on the record, we found that, similar to the prior inventory record, sufficient information regarding equipment costs was not included on the record. Of the 28 workstations listed on the record, we found that 12 items (42.9%) did not include a corresponding cost.

In conjunction with our review of the hardware inventory, we compared workstations listed on the hardware record, as of June 30, 2006 with additional lists of computer equipment provided by the Commission. We found discrepancies between the 26 Dell Optiplex GX270 workstations listed on the inventory record and a separate list of these workstations located in the Boston and Springfield administrative offices. Of the 26 workstations listed on the hardware record, the record indicated that 23 workstations were located at the Springfield office. However, the supplemental inventory list of workstations indicated that 18 workstations were installed at Springfield. Contrary to the hardware record that noted that no workstations were located at the Boston office, the supplemental list indicated that six workstations were installed in Boston. Although three of the 26 Dell GX 270 workstations listed on the inventory record lacked information regarding location, we found that the three workstations were installed in Boston. MCAD staff could not explain the discrepancies between the inventory record and the supplemental list.

As additional audit tests, we reviewed selected pieces of computer equipment purchased during the fiscal years 2000 to 2003 and during the 2006 fiscal year. We initially compared purchase documentation, such as purchase orders and vendor invoices, to the equipment listed on the inventory record, as of September 2003. Our audit disclosed discrepancies between purchase documentation and computer equipment listed on the inventory record. We found that a vendor invoice, dated February 26, 2001, indicated that MCAD had purchased 41 DELL 733 central processing units (CPU) with a listed value of

$25,256. However, the inventory record, as of September 2003, listed 39 DELL 733 CPUs, with a service date of February 26, 2001. (Two were duplicate entries). MCAD could not explain the reasons for the discrepancies between the pieces of equipment listed on the invoice and the items listed on the inventory record.

Our audit revealed additional discrepancies between information recorded on the purchase documentation and the hardware record for one file server and 15 workstations. We found that although the serial numbers for the pieces of equipment listed on the inventory record and payment vouchers were identical, the purchase dates and costs were different. For instance, we found that one file server was listed on the inventory record with a purchase date of June 20, 2000 and a stated cost of $5,086; however, the payment voucher listed the date of receipt as November 19, 2001 and a stated cost of $4,948. We also found that 15 DELL workstations were listed on the inventory record, each with a purchase date of July 15, 2003 and a stated unit cost of $863.50; however, the payment voucher listed the purchase date as June 16, 2003 and unit cost of $1,402.80. MCAD could not explain reasons for the discrepancies between purchase and cost information listed on payment vouchers and the inventory record.

In conjunction with our examination of inventory control, we determined whether the Commission could account for computer equipment listed on the inventory record, as of September 30, 2003 to subsequent the inventory record, as of June 30, 2006 or to surplus property records. As shown below, a test of selected hardware listed on the inventory records, as of September 30, 2003 to the inventory record, as of June 30, 2006 and to surplus property records, as of June 23, 2005 and April 26, 2006 indicated that five items described as file servers and one tape drive were not listed on the inventory record, as of June 30, 2006 or listed on the surplus property records, as of June 23, 2005 and April 26, 2006.

Equipment Listed on Inventory Record, as of September 30, 2003,
Omitted from Surplus Property Records, as of June 23, 2005 and April 26, 2006
and Inventory Record, as of June 30, 2006

Type of Equipment	Date of Service	Description	Cost
Server*	03.13.01	Compaq	$ 9,443
Server*	09.13.01	HP	$ 3,876
Server*	03.13.01	Compaq	$ 3,068
Server*	06.4.01	Simplex	$ 29,591
Server*	06.19.01	HiQ	$ 3,820
Tape Drive	03.13.01	Compaq	$ 3,668

*Identified on hardware record as a server

With respect to notebook computers, we determined that MCAD could not provide reasonable assurance that all notebook computers purchased or used by the Commission were properly accounted for in inventory and other accounting records, adequately safeguarded from theft, loss, or damage, and used only for their intended purpose. As shown below, there were significant differences regarding the number of notebook computers listed in the various inventory records from June 30, 2003 through June 30, 2006. As of June 30, 2006, we could not determine the actual number of notebook computers maintained by the Commission. MCAD could not provide any explanation for the differences in the number of notebooks included in the various inventory records.

Notebook Computers Listed on Inventory Records
June 2003 to June 2006

Date of Inventory Record	Number of Notebooks
June 2003	12
July 2003	8
August 2003	14
September 2003	19
June 2006	11

Regarding the declaration of surplus property, we found discrepancies between notebook computers listed on inventory records, as of September 30, 2003 and June 30, 2006 and computers listed on surplus property records, as of June 23, 2005 and April 26, 2006. For example, we found that four notebook computers listed on the September 2003 inventory record were not listed on either the surplus property record, as of June 23, 2005 or April 26, 2006, or listed on the June 30, 2006 inventory record. The Commission could not explain the discrepancies between the information listed on the various inventory records and surplus property lists. Furthermore, MCAD did not provide documentation regarding the actual disposition of notebook computers declared surplus property and recorded on the surplus property record.

We determined that MCAD had not complied with statutory requirements, such as “The Internal Control Act”, Chapter 647 Acts of 1989, OSC internal control guidelines for state departments, or its own control procedures regarding the maintenance of and periodic performance of a physical inventory and reconciliation of the inventory record. Because the MCAD could provide little evidence that an annual physical inventory and reconciliation for IT resources had been performed, it could not be determined whether all items declared surplus property had been removed from the inventory record and properly

disposed of. OSD regulations require that "(items declared as surplus, salvage or scrap under the appropriate code will remain the responsibility of the declaring agency until disposal, as authorized by the State Surplus Property Office." Furthermore because records of surplus property are developed in conjunction with inventory records of fixed assets, the lack of adequate inventory control procedures regarding fixed assets could result in inaccurate records of surplus property. As a result, assets may be subject to greater risk of loss or theft or their detection in the absence of being recorded on the inventory record and/or surplus property records. Identification of costs and dates of acquisition are important for proper accounting of assets and appropriate disposal of property and equipment.

b. Distribution and Return of Notebook Computers

Our audit indicated that the Commission's control procedures for the distribution and return of notebook computers and for periodic monitoring of the status of the equipment assigned to staff needed to be strengthened. We determined that the Commission had not developed formal policies and procedures regarding the distribution to and return of notebook computers from staff; did not maintain a comprehensive record of all staff who had been provided notebook computers or had returned them and the dates of these actions. Furthermore, the Commission had not implemented a schedule to periodically monitor the status of the computers that had been distributed to personnel. We found that although MCAD had 19 notebook computers listed on its hardware inventory record, as of September 30, 2003, and had 11 computers listed on its inventory record, as of June 30, 2006, the Commission could not provide reasonable assurance that these computers were properly accounted for, adequately safeguarded from theft, loss, or damage, and used only for their intended purpose.

We found that for the 19 notebook computers listed on the inventory record, as of September 30, 2003, identification of the staff to whom the equipment had been assigned had not been listed for 10 computers. In addition, cost information, in the amount of $37,064 was listed for 14 of the 19 computers. Regarding the inventory record, as of June 30, 2006, although 11 notebook computers were listed, only two Commissioners were recorded as having been assigned computers. Costs, in the amount of $22,229 were listed for nine of the 11 notebook computers listed on the record. The Commission could not provide any sign-out/in forms for MCAD officials or staff recorded on the inventory record as having received a computer or staff to whom a notebook computer had been assigned, but was not listed on the inventory record. Furthermore, MCAD could not provide any documentation indicating that any notebook computers had been returned.

The absence of consistent policies and procedures, a comprehensive set of documented sign-out/in forms, and a schedule for the periodic monitoring of notebook computers hindered designated managers responsible for safeguarding of computers and monitoring their use, specifically ensuring that staff to

whom notebooks have been assigned were aware of their responsibilities regarding appropriate use of the equipment. The absence of a comprehensive set of forms impeded the ability of managers responsible for monitoring the use and safeguarding of computers from carrying out their duties in this regard. In addition, due to the lack of appropriate recordkeeping procedures, notebook computers may be placed at increased risk of loss or theft.

Good management practices advocate that comprehensive control practices regarding the distribution to and return of notebook computers from individuals be implemented. Control procedures should include written instructions regarding distribution and return of equipment, sign-out/in forms, supervisory approvals, and periodic monitoring of the status of computers.

c. GAAP Reporting

Our audit indicated that MCAD had not entered Generally Accepted Accounting Principles (GAAP) Fixed Assets into the MMARS Fixed Asset Subsystem, as required by the Office of the State Comptroller's regulations. At the inception of our audit, we found that the Case Management System, with a listed value of $1,011,345 as of the October 2001 acceptance date, had not been entered into the MMARS Fixed Asset Subsystem. We determined that, as of December 2003, the CMS was properly recorded in the MMARS Subsystem. Furthermore, we determined that, as of October 31, 2006, the Commission had not entered the videoconferencing system, purchased on June 22, 2006, with a listed value of $140,529, into the MMARS Fixed Asset Subsystem.

The OSC requires that state departments and agencies properly account for all fixed-asset transactions, including the proper recording and reconciliation of GAAP Fixed Assets. GAAP Fixed Assets are defined as all land, regardless of cost, and buildings and equipment with a useful life of one year or more, and an original cost of $50,000 or more. GAAP Fixed Assets also include computer software, with a useful life of one year or more, and an original cost of $50,000 or more. According to the OSC, all GAAP Fixed Assets must be recorded at the time of acquisition in the MMARS Fixed Asset Subsystem. The Office of the State Comptroller's "MMARS Fixed Asset Subsystem User Guide" states that "all assets entered into the MMARS Fixed Asset Subsystem must be recorded onto the system within seven days of acquisition." Further, the OSC requires that "all acquired assets entered into the Fixed Asset Subsystem be verified by the department that the information entered into the system is correct and appropriate for that particular asset."

d. Accounting for Software Inventory

Our audit revealed that adequate controls were not in place and in effect to properly account for software installed on MCAD's automated systems. We determined that although the MCAD had documented software inventory records, as of June 30, 2003, September 30, 2003 and June 30, 2006, none of the records was accurate or complete. The software record, as of September 30, 2003 did not include cost information for a significant number of items listed on the record. During our initial audit work, we compared selected software packages listed on MMARS records, dated from the 2000 through 2003 fiscal years, and compared these items to the inventory records, as of June 30, 2003 and September 30, 2003 provided by the Commission. We found many discrepancies between software purchases listed on MMARS records and the software records, as of June 30, 2003 and September 2003. For example, 31 software packages, purchased June 7, 2000, were listed on the inventory record, as of June 30, 2003. However, only 13 packages were listed on the inventory record, as of September 30, 2003. In addition, we found that 40 Microsoft licenses related to the CMS were not listed on either the inventory records, as of June 30, 2003 or September 30, 2003.

We determined that MCAD initiated a new inventory record in 2006. Because the Commission had not maintained a perpetual inventory nor performed a detailed reconciliation regarding IT resources, the record as of June 30, 2006 was not accurate and complete. Our audit indicated that, although 883 software packages were listed on the record, as of September 30, 2003, only 342 packages were listed on the record, as of June 30, 2006. We found that licenses related to the CMS listed on the prior record were not listed on the 2006 record. The Commission could not provide an explanation for the disposition of the 541 software packages no longer listed on the inventory record, as of June 30, 2006.

Sound management practices and generally accepted industry standards advocate that a perpetual inventory be maintained for all property and equipment, including hardware and software, and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. Further, in accordance with Massachusetts General Laws Chapter 7, Subsection 4A, each state agency is required to record and to report on state-owned assets to certain control agencies, such as the OSC. Chapter 647 of the Acts of 1989 states that, "The agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose, and 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." Moreover, the OSC's Internal Control Guide for Departments requires that "fixed assets be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to provide control of inventories."

The OSC internal control documentation requires that "non-GAAP Assets be maintained in accordance with the department's internal control plan." Non-GAAP Fixed Assets are buildings and equipment including computer software with a useful life of more than one year and an original cost between $1,000 and $49,999.99, and all electronic and computer components. The OSC requires that, at a minimum, all non-GAAP Assets be recorded at the time of acquisition in the MMARS Fixed Asset Subsystem or in a system housed and maintained by the department. State departments have the option of using the MMARS Fixed Asset Subsystem to record non-GAAP fixed assets that the OSC does not require to be entered into the Subsystem.

The lack of an accurate and complete inventory record for computer equipment hindered the Commission's ability to account for IT resources, detect lost or stolen items, and to ensure that IT resources were being used for their intended purpose. In addition, without an accurate, complete, and valid inventory record, the Commission cannot be assured that all IT resources, including Generally Accepted Accounting Principle (GAAP) assets have been entered into the MMARS Fixed Asset Subsystem. Because MCAD had not performed a physical inventory and reconciliation for IT resources, it could not be determined whether all acquisitions had been entered into the inventory and all items designated as surplus and no longer installed had been removed from the inventory record. Because surplus property records are developed in conjunction with the inventory record, the lack of adequate inventory control procedures regarding IT resources could result in inaccurate records of IT-related surplus property. Assets may be placed at greater risk of loss or theft being detected because equipment was not listed on the inventory record or a list of surplus property. Further, due to the absence of cost information, the Commission did not have a readily available accurate total value of computer equipment as of the date of the inventory record and could not ensure that all GAAP Assets were properly recorded. Further, the absence of information regarding "date of acquisition" impedes the Commission's ability to identify, monitor, and track equipment. The software inventory should identify software currently installed or available for use on MCAD's computer systems. In addition, the identification of cost per software product needed to reflect actual cost of software. The inventory record of IT-related assets did not identify the status of equipment, or whether equipment was under warranty or a preventive maintenance agreement.

It appears that a lack of a thorough understanding of fixed-asset accounting requirements and the absence of detailed policies, standards, and guidelines for fixed-asset management impeded the implementation and exercise of inventory control procedures.

Recommendation:

We recommend that MCAD senior management obtain a sufficient understanding of the Internal Control Act, Chapter 647 of the Acts of 1989, and the management and control policies, standards and procedures required for the safeguarding of, accounting for, and reporting on property and equipment, including IT-related resources. We recommend that the MCAD strengthen current practices to ensure compliance with policies and procedures documented in the OSC's Internal Control Guide for Departments, and its associated internal control policies and procedures, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment.

The MCAD should strengthen formal policies and procedures regarding the safeguarding of, accounting for, and reporting on its fixed assets. The formal policies and procedures should include, but not be limited to, the following items: maintaining an inventory record; performing, at minimum, an annual physical inventory and reconciliation; tagging procedures for computer-related equipment; accounting for and monitoring of property and equipment; and the declaration and disposal of surplus property. In conjunction with the development of policies and procedures, the MCAD should include procedures regarding the maintenance of a perpetual inventory, which should be reconciled, at least annually, to the physical assets. The perpetual inventory should indicate dates last updated and reconciled. The policies and procedures, once approved by MCAD officials and senior management, should be distributed to the appropriate staff, and the staff should be instructed in their use.

MCAD should record new purchases, donations, and transfers of equipment and delete items, as needed, in a timely manner. To maintain proper internal control, staff members who are 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 generating the Commonwealth's required asset-management reports (e.g., GAAP reports). The inventory record should be amended to reflect inter-office transfers of computer equipment. Further, we recommend that the process of transferring equipment and updating the inventory record be monitored. To help ensure the integrity of the inventory record, we recommend that the MCAD ensure that the location, cost amounts, and dates of acquisition are included on the inventory records.

We recommend that the MCAD ensure that all computer equipment, including leased equipment accounted for as capital assets, according to the OSC regulations, be tagged with state identification numbers. We recommend that MCAD enter all property and equipment, regardless of how acquired, into the fixed-asset inventory record at the date of acquisition. Further, we recommend that the MCAD perform an inventory record reconciliation, concurrent with its annual physical inventory, and make any required adjustments to its inventory record. The MCAD should establish controls, including monitoring

and evaluation procedures, to provide reasonable assurance that the inventory records of all property and equipment, including IT-related assets, are accurate, complete, valid, and verifiable, and are maintained on a current basis.

MCAD should document procedures regarding the sign-out and sign-in of notebook computers. Users should be required to formally sign-out and/or sign-in each notebook computer and record the actual date of transfer of responsibility. Further, the designated fixed-asset manager for IT-related resources should periodically review the status of notebook computers, especially those that have been signed out. Given that the Commission has a number of notebook computers signed out to employees to assist them in their work, we recommend that, on at least a quarterly basis, the Commission perform a file comparison of the list of staff to whom computer equipment or software has been assigned to the master list of current MCAD employees. This would serve as a detective control to identify any instances when IT-related resources had not been returned to MCAD upon employee termination, transfer or leave of absence. Further, once the IT resource has been transferred to another party, MCAD should require that the transfer be formalized by the completion of a new sign-out form.

The MCAD should ensure that all software is properly accounted for in its IT-related inventory record and that accurate and complete records are maintained for all software no longer in use. The software inventory should identify all software products installed and available for use on all MCAD IT platforms. With respect to information that should be included in the software inventory record, the record should identify the name of the software product, date of installation, type of license (e.g., workstation or LAN version), version number, date of acquisition, license period (if applicable), and the cost or annual license fee per item. The MCAD should establish monitoring and evaluation procedures and mechanisms to ensure that controls are in place and in effect and provide reasonable assurance that control objectives are addressed. The MCAD should take full advantage of the training regarding fixed-asset management provided by the OSC and from other sources.

Auditee's Response:

> *I am pleased to report that several items you mentioned in your audit have already been changed, improved, or are currently being addressed:*
>
> *Notebook computers: approximately a year ago we implemented a new form that requires employees to sign out the equipment, and sign it back in. Additionally, all IT equipment is kept in a locked room with access allowed only by the Fiscal Officer and myself.*
>
> *Inventory: The Fiscal Officer maintains an accurate and up-to-date inventory on IT resources, including software.*

Auditor's Reply:

We acknowledge that MCAD has initiated steps to strengthen the integrity of the inventory system of record for IT resources and improve inventory control policies and procedures. Strengthening inventory control procedures will enhance resource knowledge for IT infrastructure management decisions. MCAD should as noted in their reply maintain a master inventory system of record for all IT resources. We believe that controls to ensure adequate accounting of IT resources will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory and records of acquisitions and deletions (trade-in, loss, etc.) to the system of record. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for lost or missing IT equipment.

Massachusetts Commission Against Discrimination
Summary of Internal Control Practices
as of October 30, 2006

Pg Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
11	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, file server room, microcomputer workstations, and client records in hardcopy form to prevent unauthorized use, loss or damage	Control over access to offices, computer rooms, file servers, and microcomputer workstations; designated facilities manager; intrusion detection devices; locked doors, foot patrols	In effect, administrative offices in Boston and Springfield	No	N/A
11,12	Environmental Protection	Provide reasonable assurance that IT-related resources operate in an appropriate environment and are adequately protected from loss or damage	Proper ventilation, temperature control, fire alarms, fire suppression mechanisms, water sprinklers, posted emergency procedures	In effect, except for file server room in Springfield needs improvement	No	N/A
13	System Access Security	Provide reasonable assurance that only authorized users are granted access to the automated systems and that logon IDs and passwords are deactivated for users no longer needing access	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	In effect	No	N/A
12,19	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	None	Yes	Inadequate
12,14	Business Continuity Planning	Provide reasonable assurance that mission-critical and essential functions can be restored in a timely manner should file servers and microcomputer workstations be rendered inoperable or be inaccessible.	Current, formal, tested business continuity plan; alternate processing site; periodic review and modification of plan; plan implemented and distributed; and staff trained in its use	Insufficient	Yes	Inadequate

Massachusetts Commission Against Discrimination
Summary of Internal Control Practices
as of October 30, 2006

Pg. ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation.
16,18	On-site storage	Provide reasonable assurance that backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location			
14	Off-site storage	Provide reasonable assurance that critical and important backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Same as above. Storage area in a separate off-premises location	In effect	No	N/A

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N/A = Not Applicable