The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2010-0045-7T

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

October 31, 2006 through February 26, 2010

OFFICIAL AUDIT REPORT

JUNE 30, 2010

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Commission Against Discrimination (MCAD) is organized under the authority of Chapter 6, Section 56, of the Massachusetts General Laws, as amended. The MCAD traces its origins to the mid-nineteenth century when the Commonwealth enacted laws prohibiting discrimination in education and public housing. The current 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.

MCAD is an independent agency of the Commonwealth of Massachusetts, administered by three Commissioners. The Governor appoints the three Commissioners and designates one Commissioner to serve as Chairman of the Commission. Commissioners serve overlapping terms of three years. The Governor also appoints an Advisory Board, presently consisting of 24 members to advise the Commission and the Governor regarding the implementation of MCAD programs and policies. The MCAD, which was staffed at the time of our audit by 69 employees, nine contractors, and 25 interns, operates a central office in Boston and maintains satellite offices in Springfield, Worcester, and New Bedford.

The duties of the MCAD, as defined in its latest annual report, are:

- To investigate complaints alleging that anyone in the Commonwealth is or has been deprived of his/her civil rights, or otherwise discriminated against in the areas of housing, employment, public accommodations, admission into an educational institution, on the basis of criminal record, maternity status of a female parent, and issues involving the Commonwealth's lead paint statute;
- To adjudicate complaints where after a finding of probable cause that anyone in the Commonwealth is or has been deprived of his/her civil rights, or otherwise has been a victim of discrimination;
- To assist parties in reaching resolution of any dispute where it is alleged that anyone in the Commonwealth is or has been deprived of his/her civil rights, or otherwise has been a victim of discrimination, if such resolution meets the public interest;
- To study and collect information relating to discrimination within the Commonwealth;
- To analyze laws and policies of the Commonwealth and its subdivisions with respect to discrimination;
- To serve as a conduit and clearinghouse for information regarding discrimination within the Commonwealth;
- To submit reports, findings, and recommendations to the Governor and the Legislature of the Commonwealth; and

- To train, educate and otherwise conduct outreach to individuals, business organizations, communities, governmental entities, and others regarding civil rights laws and matters of civil right law enforcement, and to discourage discrimination.

The Commission's business functions are performed through four major departments: Legal, Investigations, Administrative Operations, and the Hearings Division. The Administrative Department consists of the following units: Budget, Human Resources and Labor Relations, Alternative Dispute Resolution, Training and Outreach, Testing, Quality Control, and Management Information Systems. At the time of our audit, computer operations at MCAD included local area networks (LANs) in the Boston and Springfield offices. Of the ten file servers dedicated to MCAD computer operations, nine file servers are housed in Boston, and one file server is located in Springfield. The main office in Boston operates a LAN comprised of 130 workstations.

The file servers in Boston and in Springfield are connected through a wide area network (WAN) to the Commonwealth's Information Technology Division's (ITD) facilities in Chelsea, allowing access to the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system, and the Human Resources Compensation Management System (HR/CMS).

The Case Management System (CMS) is the Commission's primary application system According to the 2003 Annual Report, 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 functional components, document processing that enables a user to view documents on-line and retrieve and review files; and an automated process that tracks and monitors active cases. In May 2007, MCAD completed a modification of the CMS to accept scanned documents, convert them to Portable Document Format (PDF), and store them in a dedicated server. The Commission also uses business applications to process daily administrative functions.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed a follow-up audit of certain information technology controls at the Massachusetts Commission Against Discrimination (MCAD). Our audit, which was conducted from January 14, 2010 through April 6, 2010, covered the period of October 31, 2006 through February 26, 2010. The scope of the audit consisted of an evaluation of the status of prior audit results provided in IT audit report, No. 2007-0045-4T, issued June 30, 2008, regarding inventory control over computer equipment and business continuity planning.

Audit Objectives

Our primary audit objective was to determine whether the MCAD had taken corrective action to address audit results and recommendations in our prior IT audit report, No. 2007-0045-4T, with respect to inventory control over computer equipment and business continuity planning. A further objective was to determine whether the Commission's internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives were in place and in effect to support inventory control over computer equipment and business continuity planning.

Regarding inventory control, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded and accounted for. In addition, our audit examined the controls over the assignment and use of notebook computers, the reporting requirements of GAAP, and the accounting for software products.

Regarding business continuity planning, we determined whether controls were in place and in effect to provide reasonable assurance that backup copies of magnetic media would be available when needed and that IT operations could be recovered within an acceptable period of time to support business operations.

Audit Methodology

To determine the areas to be audited during our follow-up audit, we reviewed the prior IT audit issued June 30, 2008 and interviewed MCAD senior management and staff regarding the resolution of the prior audit results. To obtain an understanding of the internal control environment, we reviewed the MCAD organizational structure and primary business functions and relevant policies and procedures. We performed a risk analysis for the areas where follow-up audit work was required. In addition, we reviewed controls to help ensure that personally identifiable information was protected. As part of pre-

audit, we also sought to determine whether MCAD had received funds through the American Recovery and Reinvestment Act (ARRA). We evaluated the appropriateness of stated controls noting any preliminary strengths and weaknesses of the internal control procedures. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To document inventory control procedures for IT resources, we conducted an examination of the MCAD inventory to determine whether adequate controls were in place and in effect to properly account for and safeguard computer equipment and software. We requested policies and procedures regarding the fixed-asset inventory and conducted inventory tests on the MCAD inventory, dated January 20, 2010, to determine whether the MCAD was in compliance with the Office of the State Comptroller's (OSC) regulations regarding fixed-asset control. We judgmentally sampled 53 of the Commission's 236 items of computer equipment and compared information regarding the equipment to what was recorded on the inventory system of record. Additionally, we selected 20 items of computer equipment that were listed on the inventory system of record and determined whether the items were locatable and verified the descriptive information regarding each item of equipment. For the items selected from their locations and the inventory list, we examined the inventory record for product description/name, cost, manufacturers serial numbers, agency asset tag number, location, installation/assignment date, and purchase order number.

We reviewed Generally Accepted Accounting Principles (GAAP) Fixed Asset reporting requirements for state agencies and departments required by the 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 a historical cost of $49,999 or more and an economic life of one year or more. We examined procedures controlling the assignment and use of notebook computers, and the maintenance of software licenses and the inventory system of record. Our tests of inventory items did not include equipment at the satellite offices in Springfield, Worcester, and New Bedford, because the largest portion of the Commission's computer equipment is located in Boston.

To assess the adequacy of system availability, we sought to determine whether formal planning had been performed to develop and maintain a business continuity plan to resume computer operations should the network application systems be inoperable or inaccessible. We also sought to determine whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. We inquired as to whether recovery and business continuity plans were in place to provide reasonable assurance that IT operations could be regained within an acceptable period of time through a comprehensive business continuity strategy should IT systems be rendered inoperable

or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether procedures were in place to generate backup copies of magnetic media for on-site and off-site storage. We interviewed staff from MCAD and the Commonwealth's Information Technology Division (ITD) regarding the generation and storage of backup media and obtained documented statements regarding backup storage. We reviewed controls over the on-site storage location, but did not conduct a site visit to the off-site storage location.

Our audit was conducted in accordance with generally accepted government auditing standards issued by Comptroller General of the United States through the U.S. Government Accountability Office 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 version 4.1) as issued by the Information Systems Audit and Control Association.

AUDIT CONCLUSION

Based on our audit at the Massachusetts Commission Against Discrimination (MCAD), we found that, except for certain areas of documentation, appropriate controls were in place to provide reasonable assurance that the Commission's inventory system of record for computer equipment was reliable. In addition, while MCAD had implemented controls regarding business continuity planning, we found that control practices needed to be strengthened to ensure that IT capabilities and business operations can be recovered within an acceptable period of time. Although we found that MCAD had implemented IT-related inventory controls and that the inventory record of computer equipment was accurate, complete and valid, control practices regarding the documentation of annual inventories and reconciliation needed to be enhanced to help ensure that reconciliation procedures are followed and that the reliability of the inventory system of record is maintained and verified.

Our audit found that the Commission had strengthened inventory controls over computer equipment since our prior audit. At that time, MCAD could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon. Our current audit indicated that although an annual physical inventory and reconciliation according to MCAD had been performed, documentation of the annual inventory and reconciliation had not been retained as required by the Office of the State Comptroller. Our examination of the inventory system of record revealed that the inventory contained appropriate data fields and that recorded information was sufficient to locate and identify the Commission's computer equipment. Our tests of inventory data, based on two samples totaling 73 out of 236 items of computer equipment, confirmed that equipment had tag numbers attached and that the inventory record contained relevant and reliable data pertaining to equipment descriptions, tag numbers, serial number, unit cost, and location. Our audit also confirmed that prior audit results regarding software inventory, GAAP reporting, and controls over notebook computers had been adequately addressed to meet operational and control objectives.

Our review of disaster recovery and business continuity planning indicated that although specific controls were in place regarding backup copies of magnetic media and that an alternate processing site had been identified, recovery strategies for IT and business operations needed to be documented and tested in conjunction with ITD. We determined that although the Commission had developed a Continuity of Operation Plan (COOP), dated February 2006, a copy of the COOP was not readily available. With respect to disaster recovery planning for computer operations, we found that ITD is responsible for the operation and maintenance of IT equipment and applications at the Commission. We note that MCAD did not have a documented agreement that outlined disaster recovery services that would be provided by

ITD in the event that IT systems were rendered inoperable or access to One Ashburton Place was denied for an extended period.

To strengthen controls, an updated, detailed business risk and impact analysis needs to be performed to provide input for the development of a business continuity plan that would be used in conjunction with an updated COOP. The Commission also needs to obtain increased assurance from the Commonwealth's Information Technology Division that IT recovery and business continuity strategies will enable business operations to be restored within an acceptable period of time. By not having the strategies documented, tested and validated, the Commission is placed at risk to experiencing an adverse impact to business operations should IT recovery be required at an alternate site.

During the course of our audit we observed that MCAD management were aware of the importance of having security controls in place to protect sensitive and personal information against unauthorized access or disclosure.

AUDIT RESULTS

1. Prior Audit Results Unresolved - Disaster Recovery and Business Continuity Planning

Our prior 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.

Our current audit revealed that although certain management control practices for business continuity and contingency planning existed, our audit found that MCAD did not have a sufficiently comprehensive business continuity plan (BCP) in place to provide for the timely restoration of business and IT capabilities should application systems be rendered inoperable or inaccessible. We found that the Commission could not provide a current version of a Continuity of Operation Plan (COOP), which would provide high-level procedures to be performed to sustain key business functions during and after a disruption of computer operations. The prior version of the Commission's COOP that had been filed with the Massachusetts Emergency Management Agency (MEMA) in 2006 was no longer available through MEMA as it had been determined to be out-of-date.

Although we found that MCAD did have a designated alternate processing site and that backup copies of magnetic media were being generated and stored off site, we determined that a formal disaster recovery plan (DRP) was not in place to document specific steps to be taken to recover MCAD's IT operations at the alternate processing site. The disaster recovery plan would be used in concert with the Commission's COOP to address a catastrophic event that would deny access to the main MCAD facility for an extended period of time.

The Commission is dependent on ITD and two contracted vendors for maintenance of IT equipment and applications installed at the Commission. The MCAD's Financial Officer has the administrative responsibility for the Management Information Systems (MIS) Unit which is staffed by a part-time network administrator. ITD provides the MCAD with electronic data backup to their Chelsea facility twice daily.

A business continuity plan should document the recovery strategies with respect to various disaster scenarios. Without adequate business continuity and disaster recovery planning, including required user area plans, the Commission is at risk of not being able to fulfill its mission in a timely manner to "investigate complaints alleging that anyone in the Commonwealth is or has been deprived of his/her civil rights, or otherwise discriminated against in the areas of housing, employment, public accommodations,

admission into an educational institution, on the basis of criminal record, maternity status of a female parent, and issues involving the Commonwealth's lead paint statute." Furthermore, the absence of a comprehensive and tested business continuity and disaster recovery plan could result in unnecessary costs and significant processing delays. The lack of a detailed, tested plan to address the resumption of IT capabilities might also render data files and software vulnerable should a disaster occur. The absence of testing a disaster recovery plan at an alternate processing site places MCAD at risk of not having adequate assurance of the viability of recovery and business continuity strategies.

An appropriate risk analysis needs to be conducted to identify the possible scenarios that could render IT systems inoperable or inaccessible, the likelihood of the threat, and expected frequency of occurrence for each disaster scenario. The Commission should evaluate the impact of a loss of IT capabilities on their business operations. Although recovery of IT operations will require the assistance of ITD, the Commission should identify courses of action that it might be able to initiate to assist ITD in its recovery efforts. Ideally, disaster recovery and business continuity plans should be coordinated and the related roles and responsibilities of Commission and ITD staff should be clearly defined. Generally accepted business practices and industry standards for computer operations support the need for the Commission to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate business continuity and contingency plans.

Recommendation

MCAD should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs, and develop recovery plans based on the critical operational requirements supported by information systems. We recommend that the Commission enhance its COOP and ensure that the developed recovery and business continuity plans work in conjunction with the COOP. We suggest that the COOP include identification of current mission-critical operations and the supporting IT infrastructure.

We recommend that a sufficiently detailed business continuity plan be developed based on the criticality of business operations, business impact assessment, risk management, and recovery plan objectives. The BCP should address all key business processes including procedures for sustaining the business functions during and after a disruption of services. The Commission should confirm with ITD that an appropriate disaster recovery plan has been developed to meet the operational requirements of the Commission. We further recommend that the Commission obtain a copy of ITD's disaster recovery plan for MCAD's IT systems and that copies of the recovery and business continuity plans be stored in a secure off-site location. The business continuity plan should also address circumstances when access to the One

Ashburton Place facility is denied for an extended period of time. In conjunction with ITD's disaster recovery plan, the business continuity plan should be designed to restore business operations and IT functions at an alternate processing site.

Auditee's Response

> *The issue you address in your audit results (Disaster Recovery and Business Continuity Plan) continues to be a work in progress. Your report acknowledges that the MCAD does have an alternate processing site and that backup copies of magnetic media are being generated and stored off site. In July of 2006 we contracted with ITD to manage our file servers in our Boston office. They back up our servers twice daily and the data is stored in their Chelsea site. We also have separate back up tapes kept on site in a secured room, safe from environmental hazards. Your report further mentions that although MCAD has control practices for a business continuity and contingency plan, it needs to be fine tuned and put into an official COOP. As a result of the audit, your recommendation is for MCAD to formalize its COOP and recovery plan, and to confirm with ITD that an appropriate disaster recovery plan has been developed to minimize the disruption in service.*

Auditor's Reply

We acknowledge that MCAD has taken numerous steps to protect its assets by working with ITD and having its data stored in ITD's data center in Chelsea. However, until business continuity plans are enhanced beyond what is documented in the current version of the COOP, the Commission is vulnerable to a disruption in service.

2. Prior Audit Results Resolved - Inventory Control over Computer Equipment

Our prior audit disclosed that adequate controls were not in place to provide reasonable assurance that a reliable inventory system of record for computer equipment was being maintained. At that time, 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 had found significant weaknesses regarding the accounting for and reporting on MCAD's IT resources.

Our current audit found that the Commission had taken steps to address a significant portion of the prior audit results regarding inventory control over computer equipment. Our audit tests confirmed that computer equipment information was correctly and completely recorded on the Commission's inventory system of record. Based on a sample of 73 of MCAD's inventory of 236 items of computer equipment, we found that all of the items were locatable and that related information for each item was properly

recorded on the inventory record. Our analysis also indicated that the necessary data fields, such as model, description, tag identification number, unit cost, and serial number were contained in the system of record. However, the Commission lacked adequate documentation of procedural requirements and the results of annual inventories and reconciliation.

Although according to MCAD's management, an annual physical inventory and reconciliation had been performed, documentation had not been generated or retained to support the annual inventory and reconciliation as required by the Office of the State Comptroller (OSC). The requirements of the OSC's Fixed Assets-Acquisition Policy, dated November 1, 2006 states, in part: "there shall be a reconciliation of the fixed asset inventory against the books and records maintained by the Department and that the reconciliation is to be done, at a minimum on an annual basis This reconciliation shall be available for audit either by the department's internal auditors, the Office of the State Auditor or the Commonwealth's external auditors."

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

Recommendation

We recommend that MCAD document annual physical inventories and reconciliation of the inventory system of record as required by the Fixed Assets-Acquisition Policy of the OSC, dated November 1, 2006. The purpose of performing an annual reconciliation is to determine whether the inventory system of record is properly maintained and that data regarding each asset is recorded in an accurate, complete and valid manner. The documentation of an annual inventory and reconciliation provides management and auditors with an additional basis upon which the reliability of the inventory record can be assessed. The reconciliation should provide increased assurance that all IT-related equipment is properly recorded and accounted for and that any missing equipment is identified.

Auditee's Response

> *The audit result concerning (Inventory Control over Computer Equipment) details an issue that was a prior area of concern at the MCAD. As you mention in your audit findings, the MCAD has taken several steps to address the previous concerns regarding inventory control over computer equipment. Your report notes that we are currently in compliance with the requirements of the Office of the State Comptroller, and also mentions that all computer equipment information and model numbers were correctly and accurately recorded and inventory was properly reported. Although in compliance with inventory policies and procedures, your audit recommendation for the MCAD is to retain the documentation of the annual inventory and reconciliation to provide auditors*

with an additional basis upon which the reliability of the inventory record can be assessed. The MCAD will implement your recommendation beginning with the next inventory, and will also begin to keep a real time inventory list, adding and deleting equipment as the transactions occur.

Auditor's Reply

As noted in our report, we acknowledge that certain corrective steps have been taken to strengthen inventory control over computer equipment. We are pleased that the Commission will further strengthen internal controls by documenting its annual inventory and reconciliation. We will review the new inventory procedures during our next audit.