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. 2007-1300-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY RELATED CONTROLS AT THE MASSACHUSETTS LEGAL ASSISTANCE CORPORATION

July 1, 2005 through March 30, 2007

OFFICIAL AUDIT REPORT

JUNE 27, 2007

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Legal Assistance Corporation (MLAC) was established by the Legislature in 1983 to oversee and fund civil legal aid programs in Massachusetts. MLAC is administered by an Executive Director appointed by an 11-member Board of Directors. The Executive Director is responsible for the administration of MLAC's programs and services. MLAC, which operates with a staff of 13 employees, is located at 11Beacon Street in Boston, Massachusetts.

MLAC makes grants to civil legal aid programs and non-profit legal services organizations (LSOs) that in turn provide free legal advice and assistance to needy Massachusetts residents with civil (non-criminal) legal problems. To qualify for assistance, clients must be elderly or have incomes below 125 % of the federal poverty line ($481 per week for a family of four). According to MLAC, the 207 attorneys and 60 paralegals at MLAC-funded programs closed 28,224 cases in the areas of domestic violence, child custody, healthcare, and housing.

During fiscal year 2006, MLAC granted over $18.86 million to these civil legal aid programs and LSOs. More than half of MLAC's funding comes from the Massachusetts Interest on Lawyers' Trust Accounts (IOLTA) program. Under the IOLTA program, lawyers holding funds on behalf of a client must place the funds either in an account that pays interest to the client or in an IOLTA account. Although each IOLTA deposit earns a very small amount of interest, the pooled IOLTA accounts accumulate enough interest to make a substantial contribution to MLAC. MLAC also received an annual appropriation of state funds for fiscal year 2006 of $8.56 million. Of the $8.56 million, $4.32 million was for general support of legal aid programs while the remaining $4.24 million was designated for three special projects; the Battered Women's Legal Assistance Project, Disability Benefits Project, and Medicare Advocacy Project.

Currently there is one administrative staff member designated to maintain MLAC's information technology (IT) operations. At the time of our audit, four file servers, 13 desktop computer workstations, and four notebook computers supported the MLAC's IT operations. The file servers and desktop computers were configured in a local area network (LAN), which is located in MLAC's 8th floor office space. The MLAC had designated file servers that were connected through a wide area network (WAN) to the Commonwealth's Information Technology Division (ITD) mainframe providing connectivity for access to the Web-based Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS). Microsoft Office 2000 software was used for correspondence, spreadsheet and database analysis, and documentation.

During the course of our audit, the MLAC and LSOs throughout Massachusetts were in the process of implementing a single, organization-wide case management system entitled "Legal Files" that would standardize the software used for all offices. Senior management indicated that there was a state-wide need for a unified case management system and that the unified system would help support the agency's mission by enhancing MLAC's services to disadvantaged state residents by providing advocates with a new tool to share information regarding how best to serve clients.

The Office of the State Auditor's examination focused on an evaluation and review of certain IT-related general controls.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at the Massachusetts Legal Assistance Corporation (MLAC) for the period of July 1, 2005 through March 30, 2007. The audit was conducted from December 14, 2006 through March 30, 2007. Our audit scope included an examination of IT-related general controls pertaining to documented IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect to support MLAC's IT processing environment. In this regard, we sought to determine whether MLAC's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support business functions.

Our audit objective regarding IT-related policies and procedures was to determine whether IT-related policies and procedures adequately addressed the areas under review, and were sufficiently documented and in place. We also sought to determine whether MLAC had implemented IT-related strategic and tactical plans that help direct the use of technology to fulfill MLAC's mission and goals. We determined 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-related assets. We also determined whether sufficient environmental protection controls were in place to prevent and detect damage to, or loss of, computer equipment and data.

Our objective regarding system access security was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to MLAC's application system and data files. We evaluated whether procedures were in place to prevent unauthorized user access to automated systems and IT resources through the local area network (LAN) file servers and workstations. In addition, we determined whether LAN data was sufficiently protected against unauthorized disclosure, modification or deletion, and whether MLAC was actively monitoring password administration.

With regard to inventory control over computer equipment, including notebook computers, we reviewed and evaluated control policies and practices regarding the accounting for computer equipment. In addition, we determined whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647, the Internal Control Act, reporting requirements.

With respect to the availability of automated processing capabilities and access to IT resources and data, we determined whether business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup procedures were being performed and whether copies of backup magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding MLAC's overall mission and IT environment. Regarding our review of IT policies and procedures, we interviewed senior management and staff, completed questionnaires, and obtained, reviewed, and analyzed existing IT-related policies, standards, and procedures. To determine whether IT internal controls were adequately documented and whether MLAC's internal control plan included or referenced IT control policies and practices, we obtained and reviewed its internal control plan. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also interviewed MLAC staff regarding the extent to which IT policies and procedures were documented and identified, or cross-referenced, in its internal control plan.

To determine whether computer equipment and backup copies of magnetic media stored on-site and off-site were adequately safeguarded from damage or loss, we reviewed physical security over the IT resources through observations and interviews with senior management. We conducted walkthroughs, observed and identified security devices, and reviewed procedures to document and address security violations and/or incidents. We determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to the file server room and the central office. We reviewed control procedures for physical access, such as the authorization of staff to access the file server room, and key management regarding door locks to the central office and other areas housing IT equipment. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms.

With respect to environmental protection, our objective was to determine whether controls were adequate to prevent and detect damage to, or loss of, IT-related equipment and media for MLAC's file server and workstations at the central office. To determine the adequacy of environmental controls, we conducted walkthroughs of the file server rooms containing the file servers and office areas housing IT equipment at MLAC's main office. Our examination included a review of general housekeeping; fire prevention, detection and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of pertinent documentation.

We reviewed MLAC's system access security policies and procedures to prevent unauthorized access to MLAC software and data files residing on the LAN. We discussed the security policies and procedures with the system administrator, who was designated as being responsible for controlling access to MLAC's LAN and desktop computers. Our examination of system access security included a review of the staff's access privileges to applications residing on the LAN and the desktop computers. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition, length, and frequency of password changes. 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 procedures for authorizing access to MLAC's IT resources residing on the LAN and desktop computers. We then determined whether individuals granted access to the systems were currently employed by MLAC by comparing an automated list of individuals authorized to access the system with an official listing of current employees.

With regard to inventory control over IT equipment, we evaluated whether an annual physical inventory was conducted, whether IT equipment was accurately reflected in the fixed-asset inventory, and whether the IT system of record was properly maintained. We also evaluated whether the IT resources were properly accounted for in the IT system of record. To determine whether adequate controls were in place and in effect to properly account for MLAC's computer equipment, we reviewed inventory control policies and procedures and requested and obtained MLAC's inventory system of record for computer equipment. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related fixed assets. We also performed a data analysis on the inventory and made note of any distribution characteristics, duplicate records, unusual data elements, and missing values. To determine whether the system of record for computer equipment for fiscal year 2007 was current, accurate, and valid, we used a judgmental sample of 49 items (46%) out of a total population of 106 items. We traced the inventory tags and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand. In addition, we selected all four notebook computers and verified their actual location.

To determine whether MLAC complied with Commonwealth of Massachusetts regulations for accounting for assets, we reviewed evidence supporting MLAC's performance of an annual physical inventory of IT assets. Further, to determine whether MLAC complied with Commonwealth of

Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that MLAC plans to request Commonwealth approval to dispose of as surplus. Finally, to determine whether MLAC was in compliance with Chapter 647 of the Acts of 1989, regarding reporting requirements for missing or stolen assets, we reviewed incident reports for missing or stolen IT-related equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess the adequacy of business continuity planning, we evaluated the extent to which the MLAC had plans that could be activated to resume IT-supported operations should the network and servers be rendered inoperable or inaccessible. We interviewed senior management to determine whether the MLAC had formally documented procedures for the development and maintenance of appropriate business continuity plans. We also determined the extent to which the MLAC had performed a risk analysis with regard to the loss of IT-enabled business operations under different disaster scenarios. As part of our examination of business continuity planning, we assessed the adequacy of generation and storage of backup copies of magnetic media, and physical security and environmental protection controls for on-site and off-site storage. In that regard, we interviewed IT staff responsible for creating and storing backup copies of computer-related media and reviewed rotation logs and security procedures associated with backup tape storage. We further sought to determine whether IT personnel were aware of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the 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), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Massachusetts Legal Assistance Corporation (MLAC), we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to physical security, environmental protection, system access security, inventory control over computer equipment, and on-site and off-site storage of backup copies of magnetic media. However, we found that MLAC did not have adequate documented IT policies and procedures regarding IT operations and needed to strengthen its overall business continuity planning to ensure an adequate level of system availability to support the restoration of network and business operations within an acceptable period of time.

We found that documented IT strategic and tactical plans were in place. Although we determined that IT policies and procedures were in existence, the level of formal documentation needed to be strengthened for inventory control over computer equipment, business continuity and contingency planning, and system access security. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced. We recommend improving the degree of documentation for control procedures with respect to IT security and operations.

Our examination of physical security revealed that controls provided reasonable assurance that MLAC's IT resources were safeguarded from unauthorized access. We found that the data center used to implement the new case management system "Legal Files" was locked and that a list was maintained of individuals who had access. The MLAC data center had full-time security guards on duty 24 hours per day, seven days per week, and the facility was equipped with intrusion alarms. Our examination also disclosed that these areas have restricted keycard access to only approved individuals. In addition, visitors are escorted when accessing the data center to minimize the risk of damage and/or theft of computer equipment. Our review of selected areas housing microcomputer workstations disclosed that on-site security make periodic rounds nightly to verify that all office doors are locked and secure.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply, were in place in MLAC's file server room, as well as in the building housing MLAC's case management system data to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an uninterruptible power system (UPS) was in place to prevent sudden loss of data and that hand-held fire extinguishers were located within the data center. Moreover, evacuation and emergency procedures were documented and posted within the data center.

Our audit disclosed that MLAC did not have a formal, tested, disaster recovery plan to provide reasonable assurance that the Legal Files case management system and essential data processing operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable. At the time of our audit, MLAC had an informal disaster recovery plan and in conjunction with LSOs had begun to formulate a business continuity strategy. Our audit indicated that the level of disaster recovery and business continuity planning needed to be strengthened to provide detailed documented plans to address recovery strategies and continuity of business operations. Although a potential alternate processing site had been identified, no user area plans had been established to document the procedures to be followed by non-IT staff to support business continuity objectives in the event of a disaster. Although we determined that adequate procedures were in place regarding the storage of backup copies of magnetic media at secure on–site and off-site locations, the frequency of storing the backup copies off-site was only on a biannual basis.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to MLAC's data files and programs residing on the MLAC's filer servers and microcomputers. We found that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should MLAC employees terminate employment or incur a change in job requirements. Also, through observations and interviews, we determined that administrative password protection and changes to passwords were adequately controlled through MLAC's IT network. We also determined that access privileges granted to individuals were appropriate, given their job responsibilities and functions. Our tests revealed that all of the current system users were current MLAC employees. However, our audit also revealed that documentation of stated control practices with respect to policies and procedures needed to be formally documented.

With respect to inventory control over computer equipment, we found that MLAC was adhering to the policies and procedures promulgated by the State Comptroller's Office and had conducted an annual physical inventory and reconciliation. We found that MLAC maintained an up-to-date inventory record that included the computer equipments' location, tag number, serial number, and description. Our review of 49 items from MLAC's inventory listing of 106 IT-related items revealed that the items were locatable, properly accounted for, and tagged. However, although MLAC was aware of Operational Services Division's policy and procedures regarding surplus computer equipment, our audit revealed that MLAC had not complied with the requirements and had failed to properly surplus 11 items before their disposal.

At the time of the audit, MLAC was in the process of implementing additional documented policies and procedures, specifically with regard to surplus equipment.

AUDIT RESULTS

1. Documentation of IT-related Policies and Procedures

Our audit determined that, although MLAC had certain IT-related control procedures in effect, it lacked documented, formalized policies and procedures. At the time of our audit, MLAC did not have sufficiently-developed or documented IT policies and procedures for system access security and disaster recovery and business continuity planning.

Documentation is a fundamental requirement for a system of internal control. In that regard, documentation should include policies and standards to outline the “rules of the road,” procedures to describe how to perform tasks and activities, written descriptions of business processes and systems, and systems of record. Understandably, the latter would include records of business events captured to transaction files (or stores), updated to master files (or stores), suspense files, tickler files, and appropriate management audit trails.

While recognized as a management responsibility, MLAC had not taken on the task of developing, documenting, and promulgating policies and procedures relating to IT functions or across its grantee legal services organizations (LSOs). Documented IT policies and procedures are essential to ensure that an organization’s roles and responsibilities are defined, communicated, and aligned with management objectives. Documented IT policies and procedures also facilitate effective direction and adequate control.

The lack of formally documented policies and procedures limits management’s ability to provide guidance and oversight for IT-related activities at both MLAC and across the LSOs. In addition, a significant portion of the agency’s knowledge base of IT functions and practices could be lost should key personnel terminate employment. Documentation of key processes and activities within an IT function helps to provide clear guidelines regarding the exercise of control practices and monitoring and evaluation of expected results. Documented policies and procedures should address all IT functions, including IT planning, risk assessment, risk management, defining information architectures, data ownership, security, virus protection, authorized use of IT resources, training, monitoring, and reporting.

Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken, that corrective action is taken, and that undesired events are prevented or detected, and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff, serve as a good basis for evaluation, and enhance communication among personnel to improve operating effectiveness and efficiency. Formal documentation of policies and procedures also enables personnel to develop a broader understanding of their duties and to improve their knowledge and level of competence.

In the absence of formal IT policies, standards, and procedures, employees may rely on individual interpretations of what is required to be performed or how best to control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result, and important control practices may not be performed as needed and key control IT objectives may be inadequately addressed. In addition, management may not be adequately assured that desired actions have or will be taken. Further, the absence of documented IT policies and procedures undermines the ability to monitor and evaluate the performance of IT processes, computer and network operations, and application systems and to provide management with sufficient feedback and assurance. In addition to documentation being a generally accepted control practice, Chapter 647 of the Massachusetts General Laws requires that all state agencies have documented and approved internal control procedures.

Although MLAC had made a good effort to document internal controls related to fiscal management, at the time of our audit sufficient effort had not been made to document IT-related controls that are part of the overall internal control framework. In addition to the general absence of IT-related policy and procedure development, an adequate framework was not in place to define and assign IT-related responsibilities, establish points of accountability, and enforce compliance with IT policies and procedures within the user community. Barriers to policy and standard procedure development, issuance, and enforcement may be an impediment to the success of the case management system (CMS) project. While the success of the CMS project will depend upon many elements, critical success factors include having an appropriate framework of IT-related policies and procedures in place and understood, assigned responsibilities, points of accountability, and compliance monitoring and oversight.

To assess the adequacy and appropriateness of IT policies and procedures, the framework for policy and procedure development and implementation should include changing control processes to ensure that policies and procedures are reevaluated and updated periodically or upon significant changes to the IT or business environment. The framework should require the review and approval of policies, standards, directives, and procedures and should include appropriate communication mechanisms and channels to ensure that policies and procedures are understood and accepted by all users throughout MLAC and the LSOs.

Recommendation:

MLAC management should develop, document, and promulgate policies and procedures to control IT-related activities, including the areas of IT-related organization and management, system access security, physical security and environmental protection over IT resources, and disaster recovery and business continuity planning. In addition, MLAC should train all appropriate personnel in adherence to the comprehensive IT-related policies and procedures upon their formalization.

Auditee's Response:

> *Documentation of IT-Related Policies and Procedures*: *MLAC will develop, document and promulgate policies and procedures as recommended [in] . . . the draft audit report. Policies will be drafted by 1 September 2007 and the policies will be completed by 15 October 2007.*

Auditor's Reply:

We are pleased that MLAC management will develop, document, and promulgate policies and procedures as we have recommended. Documented controls, policies, and procedures provide a framework to guide and direct staff in the discharge of their responsibilities. The nature and extent of the documented IT control procedures need to address all IT functions; accommodate staff experience, competency, and knowledge; and take into account any changes to IT processes, IT infrastructure, and regulatory requirements. The development of documented policies and procedures for MLAC's IT environment is necessary to ensure that internal control practices are in effect to provide reasonable assurance that operational and control objectives will be met.

2. Disaster Recovery and Business Continuity Planning

Our audit indicated that MLAC did not have a documented business continuity plan and had not developed a formal business continuity strategy, including user area plans, that would provide reasonable assurance that essential business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. MLAC had not assessed the relative criticality of the automated systems supporting MLAC operations and identified the extent of potential risks and exposures to business operations.

At the time of our audit, management of MLAC had determined that there were no business applications that justify maintaining a permanent alternate processing site. MLAC uses Microsoft Office software for its training purposes and internal correspondence, which is currently maintained on the MLAC LAN. MLAC LAN data, documentation, software, and system configuration could potentially be lost if IT processing capabilities are unavailable. Also, as a result of loss of IT processing capability, MLAC may be impeded in tracking grant activity for indigent counseling services. MLAC's full and incremental backups potentially provide a means of recovery for lost information on the LAN.

According to MLAC management, a full disaster recovery capability was not affordable. However, a contract between a vendor and the Commonwealth has enabled MLAC to implement a network to support a centralized case management system (CMS) for MLAC and its grantee legal services organizations (LSOs). Although this new network design and capability is currently in the second year of implementation, it is not currently used for business continuity planning purposes.

The objective of business continuity planning is to help ensure the continuation of essential functions enabled by technology should a disaster cause significant disruption to computer operations. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required.

Contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

Recommendation

We recommend that MLAC, in conjunction with its grantee legal services organizations, assess their automated processing environment from a risk management and business continuity perspective and develop and test appropriate business continuity and contingency plans. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to MLAC’s operations or the overall IT environment.

The business continuity plan should document MLAC’s recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities needed to effectively and efficiently recover network or IT operations within the needed time frames. We recommend that business continuity be tested and periodically reviewed and updated, as needed, to ensure the viability of the plans. MLAC’s completed plans should be distributed to all appropriate staff, who in turn should be trained in the execution of the plans under emergency conditions. In addition, a complete copy of the plans should be stored in a secure off-site location.

Auditee's Response:

> *Business Continuity and Risk Management: MLAC will, in conjunction with the Legal Aid Organizations it supports, assess the automated processing environment from a risk management and business continuity perspective and develop and test appropriate business continuity and contingency as recommended in the draft audit report. The initial assessment and draft plan will be completed by 1 October 2007. Final business continuity plans will be completed by 15 November 2007. Plans will be reviewed and updated by 1 October each year.*

Auditor's Reply:

We are pleased that MLAC will perform the appropriate criticality assessments and develop a business continuity plan. The business continuity strategy should be sufficiently comprehensive to address various disaster and recovery scenarios and ensure system availability to mission-critical operations and IT processing for MLAC and the legal aid organizations it supports.