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. 2003-1419-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS DISTRICT ATTORNEYS ASSOCIATION

JULY 1, 2002 THROUGH MARCH 20, 2003

OFFICIAL AUDIT REPORT
JULY 23, 2003

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts District Attorneys Association (MDAA) was established under Chapter 12, Section 20D of the Massachusetts General Laws. The MDAA consists of an executive director appointed by the eleven elected Massachusetts District Attorneys. The executive director is responsible for the administration of agency programs and services. The MDAA operates with a staff of twelve employees and supports a comprehensive web presence at www.state.ma.us/mdaa/. The MDAA maintains its office in Boston, Massachusetts.

The MDAA's primary mission is to promote public safety, the fair and effective administration of justice, and the education of prosecutors throughout the Commonwealth. The MDAA also supports the eleven elected Massachusetts District Attorneys by providing technology infrastructure, professional training and conferences, and legislative and policy initiatives. While MDAA provides a variety of services, its primary responsibility is to maintain the District Attorneys' 11 individual locations that are connected via a frame relay wide area network (WAN). According to the MDAA, their goals are to coordinate and standardize services and programs, while providing information, technical assistance and educational services in an effort to help ensure the standardization of goals, operations, and procedures.

At the time of our audit, the Massachusetts District Attorneys Association's information technology operations were supported by eleven file servers, twenty desktop computers, and nine laptop computers. The eleven servers and desktop computers were configured in a local area network (LAN), which is located in the MDAA's second floor office space. All file and print servers run Windows 2000. MDAA's e-mail and Internet traffic were provided through the Information Technology Division (ITD).

At the time of our audit, Microsoft Office 2000 software was used for correspondence, spreadsheet and database analysis, and documentation. Also, NetIQ and Check Point software applications were used for system security management.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From January 6, 2003 to March 20, 2003, we performed an information technology (IT) audit at the Massachusetts District Attorneys Association (MDAA), covering the period of July 1, 2002 through March 20, 2003. Our audit scope included an examination of internal controls over selected information technology functions. We evaluated IT-related controls pertaining to organization and management, physical security, environmental protection, logical access security, hardware inventory, business continuity planning, and on-site and off-site storage of magnetic media.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect to provide a properly controlled IT environment. We determined whether adequate controls regarding organization and management, physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. With respect to logical access security, we sought to determine whether adequate controls were in place to prevent and detect unauthorized access to system and application software and related data files residing on the MDAA's LAN-based file servers and desktop computers. Our objective with respect to hardware inventory was to determine whether IT-related assets were properly identified, recorded, and accounted for in the MDAA's inventory system of record.

With respect to the availability of automated processing capabilities and access to electronic information resources, 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 MDAA's overall mission and its IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the MDAA's organization and

management activities and internal control environment, we reviewed MDAA's mission, organizational structure, segregation of duties, employee job descriptions, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the LAN file servers and desktop computers through observation, interviews with MDAA management and staff, documentation review, and completion of appropriate audit checklists.

We reviewed MDAA's logical access security policies and procedures to prevent and detect unauthorized access to the MDAA software and data files residing on the MDAA's LAN. We reviewed the security policies and procedures with the MDAA management. The Director of Information Technology is responsible for controlling MDAA's access to ITD's mainframe and the MDAA's LAN and desktop computers. We reviewed access privileges of MDAA's staff who had been authorized to access applications residing on the LAN and the desktop computers. Our examination of logical access security did not include a review of the MDAA staff's access privileges to the Commonwealth's Information Technology Division's (ITD) mainframe located at the ITD data center. 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 MDAA's IT resources on the LAN and desktop computers. Subsequently, we determined whether all system users authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of password changes. We then determined whether individuals granted access to the MDAA's systems were currently employed by the MDAA by comparing an automated list of eleven individuals authorized to access the automated systems to the MDAA's payroll records.

To determine whether IT resources were properly accounted for, we reviewed inventory policies and procedures, interviewed appropriate staff, and examined the MDAA's system of record for maintaining an inventory of computer equipment. To determine whether the MDAA's hardware inventory record was accurate, complete, current, and valid, we reviewed inventory data for 44 items (100%) of computer equipment located at the MDAA. Moreover, to determine whether all hardware that was physically located at MDAA was listed on the inventory record, we traced selected items to the inventory records. Further, to test whether purchased hardware was being listed on the system of record for inventory and physically located at the MDAA, we compared purchase orders and invoices for four selected items of hardware purchased by the

MDAA during fiscal year 2003 to the inventory records and located the individual hardware items at the MDAA offices. We also determined whether computer equipment was properly tagged and verified the tag numbers to the inventory record. We also compared the state identification or tag numbers listed on the inventory record to the actual piece of equipment on hand.

To assess the adequacy of business continuity planning, we reviewed the level of planning and established procedures to be followed to resume computer operations in the event that the file servers and desktop computers were rendered inoperable or inaccessible. We interviewed MDAA management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been identified and evaluated, whether a written business continuity plan was in place, and, if so, whether it was adequately tested. We sought to determine whether an evaluation of the adequacy of controls was in place to ensure that software and data files would be available for recovery efforts should the automated systems be rendered inoperable. We also conducted a review of the adequacy of provisions for on-site and off-site storage of critical backup tapes. In that regard, we interviewed MDAA staff responsible for creating and storing backup copies of computer-related media and reviewed rotation logs and security procedures associated with backup tape storage.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing 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. CobiT control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices that provides a reference framework for management, users, security practitioners, and auditors.

AUDIT CONCLUSION

Based on our audit, we found that information technology-related controls in place at the Massachusetts District Attorneys Association provided reasonable assurance that control objectives regarding IT organization and management, physical security, environmental protection, logical access security, and the accounting of IT inventory would be met. We found, however, that controls needed to be strengthened regarding business continuity and contingency planning, which have taken on added importance given the events of terrorist threats.

Our audit revealed that adequate physical security and environmental protection were being provided for the MDAA's IT-related assets. In this regard, we found that the computer room and business areas were appropriately secured and alarmed, fire detection and suppression controls were in place, processing areas were well maintained, a fire emergency plan was in place and posted, and appropriate air quality was afforded to the file server room.

We determined that adequate controls were in place to provide reasonable assurance that only authorized users would be able to access MDAA's automated systems. Our audit revealed that the MDAA did not have system users sign a computer usage form; however, at the end of the audit, the MDAA had fully implemented this control measure to reinforce user understanding of their responsibilities regarding acceptable use, data confidentiality, copyright protection, virus protection, access security, and e-mail usage.

We found that the MDAA had appropriate controls in place to provide reasonable assurance that IT resources would be properly accounted for on the MDAA's system of record for its equipment inventory. Our audit tests indicated that the inventory system of record was accurate, complete, current, and valid for IT resources. We also found that computer equipment was properly tagged and that equipment purchased within the past year was properly recorded on the inventory and could be readily located.

With respect to recovery strategies and contingency plans, we found that the MDAA did not have a formal, tested business continuity plan for the timely restoration of business functions provided by automated systems to be used in the event that IT resources are rendered inoperable. With regard to the continued availability of computer operations and access to electronic information, we found that the draft version of the business continuity plan needed to be formalized and strengthened. Although the MDAA generated and stored backup copies of magnetic media at their on-site location, the MDAA did not store backup copies at a secure off-site location. Without sufficient business continuity planning, as well as backup copies of magnetic media stored off-site, a possible long-term loss of the MDAA's computer operations

could hinder access to processing capabilities and electronic information needed to perform business functions.

AUDIT RESULTS

1. Business Continuity Planning

The Massachusetts District Attorneys Association did not have a formal, comprehensive business continuity plan to provide reasonable assurance that mission-critical IT operations could be regained effectively and in a timely manner, should computer systems be rendered inoperable or inaccessible. Although we found that MDAA was performing backup procedures for applications residing on its LAN, and on-site backup copies of mission-critical and essential software and data files were being generated, specific arrangements had not been made to provide for an off-site backup location of the computer media. We also found that the MDAA did assess the relative criticality of their automated systems, and management was aware of the relative importance of their application systems to the mission of the MDAA. We found that an informal detailed risk analysis had been performed to identify and determine the extent of potential risks and exposures to MDAA data processing operations. Information obtained from a detailed risk analysis not only assists an entity in addressing business continuity planning, but also helps ensure that appropriate internal control measures are implemented. Our audit revealed that the MDAA's business process areas had developed informal user-area contingency plans to address a potential loss of their automated processing.

Regarding the generation and storage of backup copies of mission-critical and essential software and data files, we found that backup copies were generated on a daily basis and that on-site storage of backup tapes was being handled effectively; however, there was no off-site tape storage of these backup media. MDAA had not designated or tested an alternate processing site to be used in the event a disaster occurs. MDAA relies considerably on information maintained in its management information system; therefore, it is essential that backup copies of data files be available for off-site support recovery procedures. If a formal plan were not in place, valuable information might be lost or be difficult to reconstruct and thus reduce work productivity.

Without adequate business continuity planning, including required off-site location plans, the MDAA is at risk of not regaining processing in an acceptable period of time should the automated system become inoperable. Furthermore, the absence of a comprehensive and tested business continuity plan could result in unnecessary costs, significant processing delays, and loss of good will.

Business continuity plans should be in place to direct recovery procedures; first, for the most important IT-based operations and, second, for less essential operations. A formal criticality

assessment assists management in establishing recovery and contingency plans in a triaged approach where resources and plans are allocated to mission-critical operations first and then to less important IT operations.

Business continuity plans should be formally tested to reduce time and the risk of errors and omissions when restoring computer operations. An effective business continuity plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the file servers and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate the need for comprehensive and effective backup and disaster recovery and business continuity planning to ensure that mission-critical and essential operations can be regained. Business continuity planning should be viewed as a process to be incorporated within the functions of the organization, rather than as a project that would be considered as completed upon the drafting of a written recovery plan. In as much as the criticality of systems, importance of business objectives, or the risks and threats associated with IT operations may change, a process should be in place to identify the change in criticality, business requirements, or risks and amend recovery and contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing contingency plans. Business continuity and contingency planning has taken on added importance given that potential processing disruptions could be caused by man-made events.

Recommendation:

We recommend that the MDAA immediately establish off-site storage for backup copies of magnetic media in a secure and environmentally sound location. The MDAA should consider the establishment of an alternate processing site as part of their business continuity plan. In addition, the MDAA should define and implement a formal continuity planning framework, including standards and policies for the development and maintenance of comprehensive business

continuity and information technology recovery plans. The MDAA should ensure this framework includes provisions to:

- assign the responsibility of coordinating disaster recovery and business resumption activities to an emergency management team and ensure that all personnel are aware of and trained in their duties and responsibilities as they apply to the comprehensive continuity plan,
- develop formal procedures to incorporate periodic business impact analysis to monitor the ongoing requirements of the business continuity plans and arrangements, and
- develop and document adequate emergency response procedures regarding information technology recovery activities, ensuring that staff members are appropriately trained to respond in the event of an emergency.

We recommend that the MDAA assess the relative criticality of its automated systems and conduct a formal risk analysis of its IT components, including outsourced services. Based on the results of the criticality assessment and risk analysis, the MDAA should confirm its understanding of business continuity requirements and, as necessary, amend recovery plans to address mission-critical and essential IT-supported business functions and services.

The MDAA should develop and maintain a formal business continuity plan that is comprehensive enough to adequately guide recovery and/or contingency efforts for various disaster scenarios. Once the plans are formulated, tested, and approved, they should be periodically reviewed, tested, and updated, if necessary. The MDAA should also develop and document procedures for secure off-site storage of backup media for applications and data files and any other IT resources required for recovery efforts needed to resume business operations. These procedures should include requirements to test the recovery of applications, tracking of backup copies of applications data files, maintaining a perpetual inventory of backup copies of magnetic media in on-site and off-site storage, and segregation of duties for personnel responsible for generating and storing backup copies of magnetic media.

Auditee's Responses:

For clarification purposes, the data in the report show that we have more workstations than we have members of our staff. This is the case because a part of our mission is to monitor and manage the statewide DA wide-area network, and many of our workstations are used to control and manage various tools and processes for controlling the network.

I agree with the two recommendations included in the audit. With regard to the storage of back-up data at an off-site location, we are in the process of contracting with a local bank to store the small physical quantity of disks and tapes in a secure bank vault. We expect to have this implemented within 30 days.

Regarding the recommendation for a formal, written business continuity plan, we agree with this concept and have (as you noted) a draft practice in place at this time. Much of our data is held at MITC in Chelsea, since we are participants in the MassMail service provided by ITD. We also have extensive work-at-home capability by use of our laptop computers.

We will finalize our business continuity/contingency plans and will evaluate - in conjunction with the 11 DA offices we support – the risks to be protected and the time period(s) of potential outages that can be tolerated by the offices we support.

Auditor's Reply:

We are pleased with the MDAA 's intention to address business continuity planning and the steps outlined above. We agree with the approach of finalizing the business continuity plan and evaluating the plan in conjunction with the eleven District Attorney Offices. Given that the requirements of the relationship might change over time, the documented responsibilities should be periodically reevaluated to permit timely changes to the agreed-to responsibilities.

Once the key elements of the business continuity plan are finalized, they should be tested, reviewed, and approved. Understandably, until the business continuity plan is fully developed and off-site storage for backup copies of magnetic media is maintained in a secure and environmentally sound location, the MDAA would remain vulnerable from a business continuity perspective.