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. 2003-0302-4T

OFFICE OF THE STATE AUDITOR'S REPORT OF THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS COMMISSION FOR THE DEAF AND HARD OF HEARING

JULY 1, 2001 THROUGH MARCH 21, 2003

OFFICIAL AUDIT REPORT

NOVEMBER 28, 2003

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Commission for the Deaf and Hard of Hearing (MCDHH) was established within the Executive Office of Health and Human Services in July of 1986 under Chapter 716, Acts of 1985 of the Massachusetts General Laws. The mission of the Massachusetts Commission for the Deaf and Hard of Hearing is to serve as the principal agency of the Commonwealth on behalf of people of all ages who are deaf and hard of hearing "in recognition of the need for a visible, fully communication accessible, central point of contact in state government."

The Commission, which has a website at www.state.ma.us/mcdhh/, maintains its central office at 150 Mount Vernon Street, Boston and has three regional offices located in Springfield, Worcester, and Plymouth. The Commission is comprised of a Commissioner and two Deputy Commissioners with sixty-two employees. The Commission also has an Advisory Council that meets eight times a year. The number of Advisory Council members, who are appointed by the Governor, range from no fewer than twelve to no more than twenty members.

Since 1996, the Commission has entered into ten deaf and hard of hearing independent living service contracts with third-party providers and one interpreter service agreement with the Department of Public Health. In addition, to make interpreter services available throughout the Commonwealth, the Commission has on-going third-party agreements with interpreters through a statewide contract. Since 2001, the MCDHH has had an Interdepartmental Service Agreement (ISA) with the Commonwealth's Department of Education to improve the provision of educational and special educational services for students in Massachusetts schools who are deaf and hard of hearing, and an ISA with the Executive Office of Elder Affairs to establish an elder caregiver program for deaf seniors.

The Commission is responsible for regulating the activities of the Massachusetts Assistive Technology Partnership (MATP), www.matp.org/sitemap.html, which is federally funded through the National Institute on Disability and Rehabilitation Research, U.S. Department of Education. The purpose of the MATP, which is affiliated with Children's Hospital located on

Boylston Street in Boston, is to increase access to technology that assists people of all ages and all disabilities through a variety of consumer focused activities.

At the time of our audit, the Commission's business activities were supported by microcomputer workstations configured in a Windows 2000 local area network (LAN). The LAN's file servers, which were dedicated to the Commission's IT operations, were housed in the central office in Boston. Of the two hundred and seventy-one IT related pieces of equipment at the Commission, there were ninety-five microcomputer workstations and servers agency wide, eighty-one of which were in the Boston office, eight in the Springfield office, four in the Worcester office, and two in the Plymouth office. The five computer servers located in the Boston office were dedicated in the following manner: one for the Administration and Finance's Information Technology Division's (ITD) IBM mainframe access to the Exchange and domain controller host protocols (DCHP); one for the Primary Domain Controller (PDC) with drive emulation to the statewide wide area network (referred to as MAGNet) and the Massachusetts Management and Accounting and Reporting System, the Commonwealth's centralized accounting information system; one host server for the Internet and intranet access; one as a print and file server, and one Sequel server used for support processing for the Interpreter Referral Information System (IRIS) and Case Management and Client Services (CMCS). Overall, the MCDHH's LAN is used for public service programs, budgetary information, and interdepartmental information sharing. With respect to regional office connections, the Springfield office's print and file server is directly routed to MAGNet, the Worcester office's server is routed through the Department of Social Services (DSS), and the Plymouth office's server is routed through the Department of Transitional Assistance (DTA) with direct access to MAGNet. At the time of the audit, there were no remote access server (RAS) connections to the MCDHH network.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From October 3, 2002 through March 21, 2003, we conducted an IT audit at the Massachusetts Commission for the Deaf and Hard of Hearing (MCDHH) for the period of July 1, 2001 through March 21, 2003. The scope of our audit included an examination of internal controls regarding IT-related physical security and environmental protection, system access security, hardware and software inventory, and business continuity planning, including on-site and off-site storage of backup media. The audit included a review of selected documentation supporting payroll expenditures for IT staff and policies and procedures regarding accounts receivable accounting. In addition, the audit also included a review of the status of audit results and recommendations brought forward in our prior audit report (No. 97-0302-4C), issued June 11, 1998. The prior audit results requiring corrective action were in the areas of business continuity planning, inventory control and annual contractor evaluations.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken regarding the audit results and recommendations identified in our prior IT audit report. We also determined whether adequate controls were in place and in effect for the selected IT and financial-related areas.

We sought to determine whether policies and procedures were in place to control accounts receivable, service provider contracts, travel and payroll expenditures. We sought to determine whether adequate business continuity plans were in place to ensure that IT functions could be regained within an acceptable period of time should a disaster render the Commission's IT systems inoperable or inaccessible. We also sought to determine whether adequate media backup procedures were being performed and whether copies of mission-critical and essential IT-related magnetic media were stored in secure on-site and off-site locations. In addition, we sought to determine whether access to the LAN file servers and microcomputer systems was adequately restricted to authorized users in order to prevent damage to, or loss of, computer equipment or IT-related media. We also sought to determine

whether sufficient inventory controls were in effect to properly account for hardware and software.

Our objectives with respect to the financial-related areas were to assess controls regarding the IT-related asset inventory and compliance with Generally Accepted Accounting Principles (GAAP) for reporting requirements and to assess the associated internal control environment. Specifically, our follow-up review of financial-related controls concerned the adequacy of fixed-asset inventory procedures and the relevance and reliability of inventory records for IT resources. We evaluated whether adequate inventory controls were in place to provide reasonable assurance that IT equipment and software were properly accounted for and safeguarded against unauthorized use, damage or theft.

Audit Methodology

To determine the scope of the audit, we performed preliminary survey work which included observation of IT-related areas in order to gain an understanding of the general internal control environment at the Commission concerning information technology and financial-related applications, as well as deaf interpreter scheduling database software residing on the LAN, in addition to interviewing senior management.

To determine the adequacy of internal controls for IT-related operations, we reviewed the documentation for IT organization and management controls. In this regard, we evaluated the degree to which MCDHH uses information technology to support various accounting and administrative functions through questionnaires and interviews with management. We examined physical security, environmental protection, business continuity planning, on-site and off-site storage of backup media, system access security, and hardware and software inventory. We determined the extent of corrective action taken by MCDHH to address the prior audit findings and recommendations.

To determine whether IT-related assets were safeguarded, we reviewed internal control policies and procedures and assessed potential risk factors regarding physical security and environmental protection at the Commission's main facility in the Dorchester section of Boston, along with its area offices located in Worcester and Springfield. We did not examine IT-related controls at the Plymouth office given the small amount of IT resources employed at

that location. We completed a risk analysis questionnaire and interviewed MCDHH`s management staff responsible for IT-related physical security and environmental protection. We determined whether the Commission's IT equipment was adequately protected against unauthorized use, theft, or damage. During the audit we inspected the server rooms and switching closets to verify the existence of air conditioning, air filtration, smoke and fire alarms, and a sprinkler system, and to determine whether all electronic media, servers, switches and routers were elevated two to three feet off the floor to provide protection from water damage.

To determine the adequacy of system access security for users having access to the local area network (LAN), we determined whether logon user IDs and passwords were being properly administered. To ensure that access privileges were granted only to authorized users, we reviewed procedures for granting system access and performed a test comparing the LAN access list to a current personnel list of employees. We reviewed user profiles for users authorized to access the LAN to ascertain whether their levels of access as individuals or as members of groups to which they were assigned was appropriate given their job descriptions and responsibilities. In addition, we tested a judgmental sample of ten of the twenty nine employee workstations (34%) located in the executive office area for violations of authorization access procedures. Our test consisted of attempts to gain access to restricted programs or folders on the network or employee workstations. We determined whether the password administration settings on the Windows 2000 operating system were appropriate for MCDHH. We also determined whether MCDHH`s access security administrator was notified immediately of changes in employee personnel status (e.g., terminations, job transfers, or leaves of absence) which may require that system access privileges need to be changed or deactivated.

With regard to business continuity and contingency planning, we assessed the relative criticality of the Commission's automated systems and IT resources, and determined whether the Commission had performed a risk assessment and developed and documented business continuity plans for mission-critical and essential IT systems. We interviewed MCDHH staff responsible for generating daily backup copies of computer media to assess whether appropriate controls were in place to generate, store, test and protect the backup media. In addition, we examined backup procedures and a list of backup tapes to ensure that backup tapes were in secure on-site and off-site locations. We visited the Springfield office and

EOHHS, the parent agency of MCDHH, that would be used temporarily to restore operations should a disaster occur. We also determined whether successful tests of the business continuity plan had been performed.

With respect to physical inventory, we performed a judgmental test sample of sixty-five of eighty-six microcomputer workstations (76%) and eight of nine servers (89%) out of a total population of ninety five. In addition, we verified fifty three (30%) of the remaining one hundred and seventy-six IT-related equipment items agency wide to determine whether the IT-related fixed assets in Boston, Springfield, and Worcester were properly accounted for. As an additional test, we traced twenty-eight (27%) IT-related fixed asset items from the fiscal year 2002 IT-related fixed asset inventory list to the fiscal year 2001 IT-related inventory list to determine whether identifying information regarding IT equipment had been properly recorded in the inventory system of record.

We reviewed the Commission's internal control policies and procedures pertaining to software license control, cross-checked the list of software licenses to the software programs residing on the LAN and servers, and obtained and reviewed a listing of the Commission's software licenses to determine whether there was an adequate amount of licenses to account for all the programs residing on the LAN, workstations and servers. We determined whether adequate documentation was available to support the purchase and installation of selected software products. In that regard, we reviewed purchase orders and copies of software licenses to determine whether installed software had been purchased.

With regard to the prior audit report, Audit No. 97-0302-4C, we reviewed and examined documentation to determine whether corrective action had been taken to address prior audit results regarding business continuity planning, inventory control, and annual contract evaluations. (See page 9 for details).

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry auditing practices. Audit criteria used in the audit included IT management control practices outlined in Control Objectives for Information and Related Technology (CobiT) as published by the Information Systems Audit and Control Association, July 2000. CobiT's 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 control framework for management, users, security practitioners, and auditors.

AUDIT CONCLUSION

Based on our audit, we found that adequate controls were in place at the Massachusetts Commission for the Deaf and Hard of Hearing (MCDHH) to provide reasonable assurance that physical security and environmental protection were in place, inventory control over computer equipment was appropriate, system access controls were operating in a proper manner, business continuity and contingency planning, along with an annual risk assessment, was documented, and that there was adequate storage of back up copies of magnetic media at both on-site and off-site locations for disaster recovery.

We found that adequate physical security was in place at the Commission's main office. The building was monitored twenty-four hours a day, seven days a week by both security guards and surveillance cameras. To access the Commission's main office, visitors are required to obtain prior approval, sign in with building security, and obtain a visitors badge. The visitor is then escorted to the elevator, where security staff use a magnetic card to access the elevator to the floor where the Commission is located, which has surveillance cameras that cover the entire floor. Access doors to the Commission are locked at all times, and can only be accessed by employees by way of a cyber-lock code system. The main door has a doorbell that visitors must press to notify the receptionist before the visitor is allowed entry. Physical security at the Worcester and Springfield locations was adequate in that IT equipment was kept locked in buildings with managed security.

Although the file server room does not have its own intruder alarm, the door to the room is locked at all times. The only entrance to the room is through the system manager's office, and the only people that have access to the room are the manager and the assistant manager of the Information Systems (MIS) section. We found that MCDHH's off-site storage area was also subject to appropriate controls to prevent unauthorized access.

Our audit revealed that adequate environmental protection was being provided for MCDHH`s IT-related fixed assets located in the main office's server room. We found the room to be well maintained in a neat and tidy fashion. A fire emergency plan was in place and posted, fire detection and fire alarm device controls were in place, and the overhead sprinkler system was subject to annual testing. All IT resources in the server room were elevated over two feet

above the floor in a rack mounted cabinet to provide protection against accidental water damage. The room had its own separate automatic climate control system in place with a daily log. At the time of our inspection, the thermometer indicated that the room temperature was within an accurate range. The room also had UPS backups with a software program that automatically shuts down the servers after ten minutes on auxiliary power.

We found that the Commission had appropriate inventory control of IT resources as a result of maintaining a master annual inventory list and a perpetual inventory list that provide reasonable assurance that IT resources would be properly accounted for on the Commission's inventory system of record. Our audit tests of 126 units of technology equipment indicated that the inventory system of record was accurate, complete, current, and valid for equipment located at the Commission's main building and the Worcester and Springfield locations. We also found that items of computer equipment recorded on the inventory record could be located and were properly tagged. In addition, there was adequate evidence that computer equipment purchased within fiscal year 2003 was properly recorded on the inventory record.

Regarding system access security, controls appeared to be in place to provide reasonable assurance that only authorized users had logical access to the Commission's LAN and connected computer systems. We found that the frequency of password changes was adequate, and that equipment controls were in place to ensure that access privileges would be deactivated in a timely fashion for users no longer authorized access, due to termination of employment or extended leaves of absence, as stated in the Commission's policy and procedures handbook. We also found that appropriate password administration settings had been established for MCDHH`s LAN Windows 2000 operating system regarding password length, frequency of password change, and denying system access after a set number of unauthorized access attempts.

With regard to the continued availability of systems, we found that the Commission had a documented comprehensive business continuity strategy to provide reasonable assurance that mission-critical processing could be regained within an acceptable time frame should processing be deemed inoperable. With respect to the storage of backup copies of critical computer media, we found that the Commission had a documented agreement with the Executive Office of Health and Human Services (EOHHS) for off-site storage of backup

media and access to an alternate location at EOHHS from which mission critical applications could be restored.

The prior audit results of business continuity planning, inventory control of fixed assets, and annual evaluations of Deaf and Hard of Hearing Independent Living Services contracts had been resolved. The Commission was able to provide sufficient documentation to demonstrate that business continuity planning, inventory control, and contractor evaluations are an ongoing process.

STATUS OF PRIOR AUDIT RESULTS

Status of Prior Audit Results from Report No. 97-0302-4C, issued June 11, 1998:

Prior Audit Results - Resolved

1. BUSINESS CONTINUITY PLANNING

Prior Audit Result

Our prior audit revealed that the Commission had not documented a comprehensive recovery strategy for business continuity to regain mission-critical processing within an acceptable period of time should significant disruptions or loss of automated processing capabilities occur. Although the Commission had adequate controls in place for on-site backup media and had implemented provisions for off-site storage of backup media, the absence of a comprehensive business continuity plan could have resulted in the Commission experiencing significant delays in re-establishing the processing of LAN-based functions should a disaster render the system inoperable and require recovery efforts from another location.

Current Audit Result

The Commission now has a business continuity plan in place to identify the steps to be taken to regain mission-critical and essential IT processing. We note that the Commission implemented version two of their business continuity plan on September 2002. The plan has the following sections within it: Purpose, Scope, Mission-Critical and Important Systems, Primary Services Provided, Hazard Analysis for Primary MCDHH Services, emergency server shutdown, IRIS manual entries, alternate IT operations, tape backup system, MMARS & HR/CMS operations at EOHHS or alternate site, call-out plan, troubleshooting by IT personnel, technical assistance by vendors, emergency server on stand-by for critical processes. This plan, when fully tested, should provide MCDHH with a safe means of continuing operations in the event of a disaster.

2. INVENTORY CONTROL OF FIXED ASSETS

Prior Audit Result

The audit determined that although controls related to the safeguarding of fixed assets were in place, controls to properly account for the Commission's fixed assets should be strengthened to ensure that all assets are tagged, and that information regarding value, location, tag number, and status is completely included in the inventory records. Our audit disclosed that although the Commission had documented policies and procedures related to inventory and had developed an inventory record of office furniture, office equipment, hardware and software, the Commission could not provide reasonable assurance that the policies and procedures were followed and that a perpetual inventory record was maintained. Although we found that appropriate information, such as date of purchase, date of installation, description, and cost figures were listed on the fixed-asset inventory records, we determined that adequate controls were not in effect to ensure that a current, accurate and complete perpetual inventory would be maintained. Our tests indicated that not all items from our review sample could be located and that a significant number were not tagged. Further, there was insufficient evidence that an annual physical inventory had been performed or that items listed on the inventory record were being periodically confirmed to the physical inventory.

Current Audit Result

Our current audit confirmed that the Commission maintained an inventory system of record on a perpetual basis. Our tests indicated that all items from our audit sample could be located and that all were properly tagged. We traced 79 microcomputer workstations out of a total population of 126 (63%) commission-wide to verify that IT-related fixed assets were accounted for in the Boston, Springfield, and Worcester locations. We were able to verify the location based upon information supplied in the system of record in Boston for 68 out of 112 pieces of equipment, in Springfield for 7 out of 7 pieces of equipment, and in Worcester for 4 out of 4 pieces of equipment. We were able to obtain an annual physical inventory for 2001 and 2002 and items listed on the inventory record were being periodically confirmed to the physical inventory.

3. ANNUAL DEAF AND HARD OF HEARING INDEPENDENT LIVING SERVICES (DHILS) CONTRACTOR EVALUATIONS

Prior Audit Result

Our review of annual Deaf and Hard of Hearing Independent Living Services (DHILS) contracts revealed that although MCDHH followed the majority of required service contracting procedures and completed the necessary forms for vendor servicing contracts, the Commission had not performed adequate monitoring and evaluations of these contracts as required by the Commonwealth's Purchase of Service System User Handbook Chapter 8.

These contracts are typically for terms of one, three, or five years in length, and are designed as service contracts to employ, train, and certify Massachusetts caregivers who assist and train disabled people in adapting to everyday life. Our prior examination of eleven ongoing DHILS service provider contracts with seven individual contractors disclosed that, although required to do so under its purchase of service agreements, MCDHH had not performed evaluations on an annual basis. We found that MCDHH had not performed any evaluations for the two fiscal years ended June 30,1997, and had performed only one thorough evaluation from fiscal year 1992 through 1995.

Follow-up Audit Result

Our examination of ongoing DHILS service provider contracts with ten individual contractors disclosed that MCDHH is now performing evaluations on an annual basis, and that the most recent evaluations were performed for May 2002.