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. 2009-1324-7T

OFFICE OF THE STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY-RELATED CONTROLS
AT THE DIVISION OF APPRENTICE TRAINING

July 1, 2007 through December 21, 2008

OFFICIAL AUDIT REPORT

APRIL 16, 2009

TABLE OF CONTENTS

INTRODUCTION

The Division of Apprentice Training (DAT) is organized under Chapter 23, Section 11E through 11W of the Massachusetts General Laws, as amended, and operates under the purview of the Department of Workforce Development (DWD), which is an agency that operates through the Executive Office of Labor and Workforce Development. DAT's primary mission is to educate the public and agencies to better understand and utilize apprenticeship as a workforce development tool. DAT works closely with other agencies, such as the Department of Education, and public and private sector entities to develop and maintain both school-to-work programs (pre-apprenticeship programs) and formal apprenticeship programs.

The Division is managed by a Director, who is appointed by the Director of the Department of Workforce Development and approved by the Governor. At the time of our audit, DAT had eight employees and had a budget of $445,181 for fiscal year 2009. In addition, DAT had receipts in fiscal year 2008 in the amount of $319,758, of which $225,892 was revenue deposited in the State's General Fund account and $93,866 was deposited in DAT's Trust Fund account. These funds are received by the State Treasurer on behalf of the Commonwealth and are deposited in a special trust account for the Division and may be expended, without further appropriation, under the direction of the Director.

Information technology processing at DAT is supported by the Department of Workforce Development's IT Department, which manages network operations and associated technology to support DAT's systems. The IT Department also provides IT services for DWD's other two agencies, the Division of Career Services and Division of Unemployment Assistance. DAT's local area network (LAN) is comprised of eight workstations. The LAN server allows users to share software applications and data files, such as electronic mail, word processing, spreadsheets, and apprenticeship data within DAT. DAT's primary application is the Apprenticeship Case Tracking System, which is a Microsoft Access database application. The Apprenticeship Case Tracking System is used for the tracking and retention of apprentices, assisting with curriculum development, and accessing apprenticeship programs. Access to the Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS) is limited to a single administrative staff person at DAT, with read-only access.

As a division of the Department of Workforce Development, DAT is dependent upon DWD for its IT processing capabilities, internal control planning, business continuity planning, environmental protection, system access security, hardware acquisitions, and payroll support.

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 Division of Apprentice Training (DAT) for the period of July 1, 2007 through December 21, 2008. The scope of the audit consisted of an evaluation of the status of prior audit results from our IT audit report, No. 2003-1324-4T, issued May 6, 2003, regarding documented IT-related policies and procedures, business continuity planning, and inventory control of computer equipment. In addition, we examined internal controls over selected IT functions pertaining to physical security and environmental protection for areas housing DAT computer equipment, provisions for on-site and off-site backup media, and system access security. The audit was conducted from September 29, 2008 through December 21, 2008.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results and to review selected IT-related controls. We sought to determine whether the Division of Apprentice Training's IT-related internal control environment, including policies and procedures, provided reasonable assurance that the DAT's IT-related objectives would be achieved. We sought to determine whether the Department of Workforce Development (DWD), in conjunction with DAT, had adequate disaster recovery and business continuity plans in place to provide reasonable assurance that computer operations would be regained within an acceptable period should a disaster render DAT's computerized functions inoperable. We also determined whether adequate provisions for on-site and off-site storage was being maintained for backup copies of DAT's computer-related media. In addition, we determined whether adequate controls were in place and in effect to provide reasonable assurance that IT resources were properly accounted for in an inventory system of record and safeguarded against unauthorized use, theft, or damage.

We sought to determine whether adequate physical security and environmental protection were in place over IT resources at DAT's office and DWD's data center to prevent unauthorized access to, or loss of, IT-related assets. We sought to determine whether adequate controls were in place to prevent unauthorized system access to DAT's file server, which hosts the Apprenticeship Case Tracking System. Our objective regarding system access security for user account management was to determine whether adequate controls were in place and in effect for the activation, maintenance, and deactivation of access privileges to ensure that only authorized personnel had access to the DAT's automated systems.

Furthermore, we sought to determine whether DAT management was actively monitoring the management of user accounts.

Audit Methodology

To evaluate whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2003-1324-4T, we performed pre-audit work that included gaining an understanding of DAT's mission and business objectives, current IT environment, and the degree of oversight provided by DWD regarding the Division's IT activities. We reviewed our prior recommendations and examined the extent to which DAT had implemented corrective action regarding documented IT-related policies and procedures, business continuity planning, off-site storage, and inventory control of computer equipment. To accomplish a preliminary review of the appropriateness and adequacy of general controls over Division's IT-related functions and assets, we observed and identified computer systems in use at DAT. We also conducted a site visit to DWD's computer room where the servers that contain DAT application and data files that would be used to support recovery efforts for DAT. Since the audit did not include DWD, we did not conduct tests of controls for IT functions at DWD. A survey form was initially used as an audit tool to assess and record the existence of IT general controls pertaining to DAT. We also interviewed DAT and DWD senior management and IT staff and observed IT operations.

Regarding our review of the adequacy of IT-related policies and procedures, we interviewed DAT and DWD senior management and staff to identify IT functions and responsibilities. We then evaluated the degree to which documented policies and procedures addressed selected IT functions and provided guidance to DAT staff.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed by DAT in conjunction with DWD to resume IT operations should the network application systems be inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Furthermore, to evaluate the adequacy of controls to ensure that backup copies of application systems and data files would be available for recovering automated systems and network services, we interviewed DWD staff regarding the generation and storage of backup copies of magnetic media. We determined whether backup copies of magnetic media were being stored on-site and off-site for DAT's Apprenticeship Case Tracking System. We did not review the off-site storage location of backup media.

To determine whether adequate controls were in place and in effect to properly account for computer equipment, we reviewed and evaluated the appropriateness of inventory control practices and procedures.

Because the Department of Workforce Development has managed inventory control for DAT since fiscal year 2005, we interviewed the Operations Director to determine the role of DWD regarding the accounting for IT resources.

We obtained and reviewed the inventory record for computer equipment as of October 31, 2008. We reviewed the current inventory system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of computer equipment. We reviewed the content of selected data fields, such as state identification number, serial number, cost, and equipment location, in order to assess the level of completeness of the system of record and to determine whether sufficient information was available to perform audit tests, including a reconciliation of items listed on the record to the actual equipment. We reviewed control procedures regarding the tagging of computer equipment purchased by DWD for DAT. We compared purchase orders for IT equipment purchased during our audit period to inventory records and to the computer equipment on-hand. By observation, we determined whether the computer equipment was properly tagged with state identification numbers and that the tag numbers were accurately recorded on the inventory system of record. In addition, we determined whether computer equipment serial numbers were accurately recorded on the hardware inventory record.

To determine whether the inventory system of record for computer equipment for DAT was current, accurate, and complete, we reconciled the inventory list provided by the auditee to the actual computer equipment on hand. We selected 100% of DAT's computer equipment, consisting of 55 items, for review. We judgmentally sampled 36 equipment items from DWD's DAT inventory list and traced them to their physical locations. We then selected and traced another 19 hardware items from their physical locations back to the inventory list to verify the accuracy of the recorded information. We also reviewed the sign out receipt logs for five of the 19 items listed as notebook computers. Furthermore, we reviewed DWD property disposal practices to determine whether procedures required by state laws and regulations were being followed when DWD disposed of DAT surplus assets.

To determine whether adequate controls were in place and in effect to prevent and detect unauthorized access to the DAT administrative office and DWD's computer room, we inspected physical access controls, such as appropriately locked entrance and exit doors, the presence of a receptionist in the administration building, intrusion detection, and whether visitor badges were required.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we reviewed general housekeeping procedures for the DWD computer room and the area housing DAT's file server. To evaluate provisions for temperature and humidity control for the DWD computer room, we determined whether adequate air conditioning units

were available. We determined whether an uninterruptible power supply (UPS) had been installed to prevent loss of data through a controlled shutdown of equipment following the loss of electrical power. Furthermore, we checked for the presence of an automated fire suppression system and water detection devices within the computer room and the area housing DAT's file server, and whether the server and other computer equipment were on racks and raised above floor levels to prevent water damage.

Our examination of system access security controls included a review of access privileges of those employees authorized to access automated systems, such as the Apprenticeship Case Tracking System. To determine whether existing system-based access privileges were authorized and reflected current responsibilities, we reviewed procedures for granting and updating system access. To determine whether security controls were in place at DAT, we conducted interviews and assessed the level of access security being provided. We determined whether procedures were in place to ensure that DWD was promptly and properly notified when a change in personnel status (e.g., employment termination, job transfer, or leave of absence) occurred so that user account access could be promptly deactivated or access privileges appropriately modified in a timely manner.

Our audit was conducted in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States and generally accepted auditing practices. Audit criteria used in the audit included IT management control guidelines outlined in Control Objectives for Information and Related Technology (CobiT) as issued by the Information Systems Audit and Control Association, July 2007

AUDIT CONCLUSION

Our examination of the status of audit results from our prior audit report (No. 2003-1324-4T), issued May 6, 2003, indicated that corrective action had been taken to address control objectives regarding documented IT-related policies and procedures, business continuity planning, off-site storage, and inventory controls of computer equipment. Our current audit indicated that the Department of Workforce Development (DWD), in conjunction with the Division of Apprentice Training (DAT), is now supporting the control functions that required corrective action as identified in our prior audit. We found that IT resources, including the file server and workstations installed at the DAT administrative office and the DWD computer room, were properly safeguarded, environmentally protected, and properly accounted for. In addition, we determined that appropriate control practices regarding logon ID and password administration were in place to help provide reasonable assurance that only authorized parties could access the Division's IT resources.

We determined that corrective action had been taken to provide reasonable assurance that IT-related organization and management control objectives had been addressed with respect to documented IT policies, procedures, and functions. We found that IT policies and procedures, which had been promulgated by DWD, were available and in effect at DAT regarding physical security, environmental protection, access security, and inventory control of computer equipment. We also found that DWD had disaster recovery and business continuity plans for the divisions under its jurisdiction.

We found that the Department of Workforce Development had a formal business continuity plan to help ensure the resumption of mission-critical and essential processing should IT systems be rendered inoperable or inaccessible. However, at the time of our audit, the plan did not specifically identify and include DAT's IT systems. We determined that the risk of loss of DAT's IT operations was relatively low should its system be rendered inoperable. In addition, based on a review of policies, procedures, and back up logs from the DWD backup server, we determined that DWD, in conjunction with DAT, had adequate on-site and off-site provisions for generating backup copies of media and adequate storage for on-site backup media to support recovery efforts. Management informed us that backup copies were maintained in a vendor-provided off-site storage location. We recommend that DAT and DWD enhance their business continuity plans to more adequately document business continuity provisions specific to DAT.

Regarding inventory control, we found corrective action had been taken to provide reasonable assurance that computer equipment at DAT would be properly safeguarded, accounted for in DAT's inventory record, and reported, when appropriate, to DWD. Specifically, DWD maintained DAT's official

inventory system of record that included the location, tag number, serial number, and description of computer equipment. We verified that DAT had complied with DWD's policies and procedures by submitting a listing of computer equipment to aide reconciliation of DAT's records to the master inventory record maintained by DWD. Regarding compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets, our review revealed that DWD and DAT staff responsible for inventory were aware of the reporting requirements and that DAT had not had any reported occurrences of missing or stolen computer equipment during the audit period. However, we recommend that DWD, in conjunction with DAT, document the process for performing an annual physical inventory and reconciliation of the inventory system of record by comparing the specific information on computer equipment provided by DAT through its physical inventory to the specific items noted in DWD's formal system of record. We also recommend that DWD, in conjunction with DAT, enhance the inventory system of record to include complete information with respect to cost and condition of equipment.

Our audit found that adequate physical security controls were in place over and within DAT's administrative office in Boston and DWD's computer room to provide reasonable assurance that access to IT resources would be restricted to authorized persons only and that IT resources would be safeguarded from damage or loss. We determined that security officers were on duty 24/7 for the building, visitors were required to sign in prior to entering the building's business offices, and thatcameras and intrusion detection devices were installed in appropriate locations. We found that appropriate key management controls were in place for DAT's administrative office. We determined that DWD's computer room was locked by means of a punch keypad lock and a separate physical key and access was restricted to selected DWD staff.

We determined that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place in DWD's computer room, DAT's file server room, and areas housing DAT's workstations to help prevent damage to, or loss of, IT resources. Emergency procedures were posted in the administrative office and, according to DWD management, staff had been trained during the prior two years regarding emergency shutdown procedures. Our audit disclosed that DWD's computer room was well organized, temperature and humidity levels within the room were appropriate, and an uninterruptible power supply (UPS) device was in place to permit a controlled shutdown and to prevent a sudden loss of data. We verified that the file servers were placed on a rack above floor level to prevent water damage, a fire suppression system was installed in the room, and a hand-held fire extinguisher was also located within the server room.

Regarding systems access security, we found that appropriate control practices regarding the authorization of personnel to be granted access to network resources, activation of access privileges through the granting of a logon ID and password, and deactivation of access privileges were in place. We found controls in place so that access privileges would be deactivated or appropriately modified should DAT employees terminate employment or incur a change in job requirements. A security officer was designated; policies and procedures were documented; and DAT staff were required to participate in formal security training, sign a formal security statement regarding password protection and confidentiality, and pass a security-related test. Our tests confirmed that users granted access to the Apprenticeship Case Tracking System were DAT employees. We determined that adequate policies and procedures were in place for password formation, use, and frequency of change.

AUDIT RESULTS

STATUS OF PRIOR AUDIT RESULTS

a. Business Continuity Planning and Off-Site Storage of Backup Media

Our prior audit indicated that the Division of Apprentice Training (DAT) had not developed a formal comprehensive disaster recovery and business continuity plan for restoring processing functions in the event that automated systems were rendered inaccessible or inoperable. We had recommended that the Division define and implement a continuity planning framework, including standards and policies for the development and maintenance of comprehensive business continuity and information technology (IT) and recovery plans, and implement appropriate procedures for off-site storage for back-up copies of magnetic media.

Although DAT had not developed a formal comprehensive disaster recovery and business continuity plan as of December 21, 2008, the Department of Workforce Development (DWD) stated that if DAT's system failed, DWD could provide a replacement file server, reconstruct the lost data, and recover all of DAT's systems and information. We acknowledge that DWD does have a strategy for disaster recovery and business continuity planning for IT operations of the divisions under its jurisdiction. We determined that DWD had prepared a business continuity plan and had detailed back-up procedures in place for restoring processing functions in the event that automated systems were rendered inoperable. However, we noted that the business continuity plan covered only those systems that were most critical to DWD's services at the 19 Staniford Street address where DAT is also located. We found that DAT was performing backup procedures for applications residing on its local area network (LAN) and that DWD had detailed backup procedures for all systems and applications supported by DWD for both generation and storage of magnetic media at on-site and off-site locations. Our audit determined that minimal risks exist with regard to a loss of IT processing capability at DAT.

Recommendation

We recommend that DWD specifically include DAT in its disaster recovery and business continuity plans and related documents.

b. Information Technology-Related Organization and Management

Our prior audit found that DAT had not developed IT-related policies and procedures to provide sufficient formal guidance for IT operations and activities. We had recommended that an analysis of IT-related functions at DAT be conducted to identify the responsible parties within the Division who perform IT-related functions. We had recommended that once the IT-related policies and procedures had been developed, they should be formally approved and communicated to staff.

Our current audit found that oversight with respect to IT functions and activities was being provided by DWD. Our review of documentation, including the DWD Internal Control Plan dated October 2008, of IT internal controls provided by DWD indicated that the documented policies and procedures addressed relevant activities related to DAT's IT operations.

Recommendation

DWD should include specific references regarding DAT in its Internal Control Plan and IT-related policies and procedures.

c. Hardware Inventory Control

Our prior audit indicated that DAT's inventory system of record for computer equipment was not accurate and complete. DAT had not conducted an annual physical inventory and had not performed reconciliation for computer equipment. Our prior audit had recommended that DAT develop and implement formal written policies, standards, and procedural guidelines regarding inventory control for computer equipment. We had recommended that a physical inventory and reconciliation be performed on a periodic basis.

Our current audit disclosed that the asset inventory function was the responsibility of DWD's Inventory Control Manager and not that of DAT. We found that DAT, in conjunction with DWD, had improved inventory controls to ensure safeguarding and accounting for DAT's computer equipment. DWD was able to provide a current and accurate inventory system of record for DAT's 55 items of computer equipment. We found that DAT had forwarded information to DWD supporting the performance of a physical inventory and reconciliation. Our inventory tests of all 55 items indicated that they were accurately recorded on the DWD inventory system of record and we were able to locate all DAT computer equipment items. DAT IT purchase data for the period under review was obtained, reviewed, and traced to the inventory record. Although we found that the inventory system of record contained appropriate fields to record information, such as description, cost, serial number, and location, the inventory records did not record condition or status of equipment, and cost figures were often listed as "0" or "$1.00."

Recommendation

DWD, in conjunction with DAT, should enhance the inventory system of record to include complete information with respect to cost and condition of equipment.

Auditee's Response:

This serves as the Division of Apprentice Training's response to the audit report 2009-1324-7T you provided on March 27, 2009. We have reviewed the report and have found that it is accurate and valid. Additionally, we are pleased that you have determined that corrective action has been taken to address items noted in the report you issued in May 2003.

With respect to the items you've noted as a result of your most recent review, we fully concur with the recommendations included in the report and will implement the following by June 30, 2009:

- *DAT will be specifically noted in DWD's Internal Control Plan, documents regarding disaster recovery and business continuity and appropriate IT policies and procedures (those which make reference to DWD Divisions);*
- *DWD, in conjunction with DAT, will enhance the DWD inventory control system to include complete information regarding the cost and condition of DAT computer equipment.*
- *DWD will ensure, through a documented process, that the DWD inventory system is reconciled, on an annual basis, with the physical inventory of DAT's computer equipment.*

Auditor's Reply:

We are pleased that DAT will be included in DWD's Internal Control Plan and business continuity plan. Understandably, it is important that DAT's specific businesses processes and IT environment are addressed in the Internal Control Plan and business continuity plan. With regard to inventory control for computer equipment, the additional data elements of cost and condition will assist in meeting control objectives related to the accounting for computer equipment and for configuration management. In addition, documenting the process for conducting an annual physical inventory and reconciliation will help ensure an adequate level of data integrity for the inventory system of record for computer equipment.