A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2008-0105-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE
DIVISION OF PROFESSIONAL LICENSURE

July 1, 2005 through May 30, 2008

OFFICIAL AUDIT REPORT
OCTOBER 16, 2008

TABLE OF CONTENTS

INTRODUCTION

The Division of Professional Licensure (DPL) was established under Chapter 13 of the Massachusetts General Laws. The Division, which is headed by a director appointed by the Governor, is located at 239 Causeway Street Boston, Massachusetts, with a branch office located at 436 Dwight Street, Springfield Massachusetts. The DPL employs approximately 108 people, including 3 to 5 staff assigned to the Springfield Office. The DPL's mission is to protect the public welfare by issuing licenses to qualified individuals who provide services to consumers, and to ensure the fair and consistent enforcement of statutes and regulations of the Boards of Registration. The Division is responsible for ensuring the integrity of the licensure process for more than 43 trades and professions regulated by 30 Boards of Registration, the continual updating of licenses for over 330,000 licensees, and the maintenance of multiple databases related to licensing, enforcement, and revenue collection. This work is accomplished through the combined efforts of: the members of the Boards and the staff of the Board offices and the various DPL divisions, including the Computer Services Department, the Accounting Unit, the Office of Legal Counsel, the Office of Prosecutions, the Office of Investigations, and the Administrative Office. The Office of Consumer Affairs and Business Regulation, which is a Department under the Executive Office of Housing and Economic Development, has oversight for the Division.

The Division of Professional Licensure collected revenues in the amount of $18,971,152 in fiscal year 2006 and $16,557,082 in fiscal year 2007, while expenditures totaled $10,134,573 in fiscal year 2006 and $9,200,884 in fiscal year 2007.

The Computer Services Department, which handles the Division's computer operations, has eight staff and is comprised of three units: the Network Services Unit; the Electronic Data Processing Services Unit; and the Web Services Unit. The DPL's Computer Services Department, as noted in DPL's annual report, "acts as a liaison between the Commonwealth's Information Technology Division (ITD), the lockbox vendor, testing companies, boards, licensees, and other vendors or agencies." The Computer Services Department is also responsible for DPL's network infrastructure, telephone system, and its web site. The Division has a Web and Database Development Unit that is responsible for maintaining the agency Intranet and Internet web sites; developing and maintaining mission-critical MS Office based applications; the SQL Server databases; and the Online Application Self-Service Information System (OASSIS).

Licensee data is stored in four mainframe databases that are on servers at the Massachusetts Information Technology Center in Chelsea, Massachusetts. The databases are License, Complaint, Applicant Tracking, and Inspections. The License database is the official electronic record for the Division's

licensees. Access to the mainframe databases is obtained through two custom applications: REG, which is a legacy system that can view one database at a time, and OASSIS, which is a web-based application that can view multiple databases at a time.

The Division's business operations are supported by an IT configuration consisting of a local area network (LAN) containing approximately 10 file servers and 170 workstations. The Division has connections to MAGNet, the Commonwealth's wide area network (WAN), for access to statewide application systems. There are no DPL servers at the Springfield DPL office. Users at the Springfield office connect to DPL's network through the Division of Bank's WAN connection.

In addition to the Division's 30 boards of registration, the DPL also provides revenue accounting and computer licensing functions for the seven boards of registration that are under the Department of Public Health's Division of Health Professions Licensure.

The Office of the State Auditor's (OSA) examination focused on an evaluation of selected IT-related controls over DPL's IT operations and IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope:

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) controls at the Division of Professional Licensure (DPL) covering the period of July 1, 2005 through May 30, 2008. The audit was conducted from November 16, 2007 through May 30, 2008. The scope of our audit included an evaluation of IT-related controls pertaining to organization and management of IT activities and operations, business continuity and contingency planning, on-site and off-site storage of magnetic media, physical security, system access security, environmental protection, and hardware and software inventory. We also performed a review of selected mission-critical application systems at DPL and reviewed DPL's actions for improving security over personally identifiable information in its licensing database application.

Audit Objectives:

The primary objective of our audit was to determine whether adequate controls were in place and in effect to provide reasonable assurance that control objectives would be met for selected areas within the IT environment, and that application systems were in place to assist the DPL in meeting its mission. We sought to determine whether IT organizational and management controls were in effect over information technology activities to ensure that such activities are managed effectively and efficiently and that IT policies and procedures are adequately documented.

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 determined whether sufficient environmental protection controls were in place to prevent and detect damage to, or loss of, computer equipment and data residing on the systems. We also reviewed physical security and environmental protection for the Division's on-site and off-site storage locations for backup media.

Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to the Division's automated systems and data files. We also determined whether the data was sufficiently protected against unauthorized disclosure, change, or deletion. We sought to determine whether password administration was being properly controlled and monitored.

Regarding system availability, we determined whether controls were in place to provide reasonable assurance that required IT processing and access to data files could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible. In conjunction with reviewing

business continuity and contingency planning, we determined whether a business continuity and contingency plan adequately documented recovery strategies and whether adequate on-site and off-site storage of backup copies of magnetic media was in effect to assist recovery efforts.

Our objective with respect to the DPL's hardware and software inventory was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-resources were properly accounted for and safeguarded against unauthorized use, theft, or damage.

Our objective with respect to the DPL's mission-critical application systems was to review whether recent security related exposures and confidential information breaches had been addressed.

Audit Methodology:

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of relevant operations, including the IT infrastructure and in-house software applications, reviewing documentation and interviewing staff regarding DPL's mission, operations, and IT organization and management. We interviewed the DPL's Director of IT and the Director of Administration and Finance to obtain an understanding of the DPL's operations, the IT systems infrastructure, the IT control environment, and the organization of the Computer Services Department. To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we evaluated the degree to which the DPL had documented, authorized, and approved IT-related control policies and procedures.

Regarding our examination of organization and management, we interviewed IT senior management; requested and reviewed documented IT-related policies, standards, procedures and strategic plans to determine their adequacy; and assessed IT-related management practices. We interviewed IT management to determine whether the IT-related job descriptions and specifications were up-to-date and reflected current responsibilities and technological knowledge requirements. We obtained a current list of the personnel employed by the IT Department and compared the list to the IT Department organizational chart and the employee's IT-related responsibilities at the time of the examination. We reviewed the adequacy of IT-related operational and management controls through interviews, documentation review, and observation regarding the mission of the IT Department, segregation of duties, and extent of management supervision over IT operations.

To assess the adequacy of controls to provide continued operations, we assessed the degree to which business continuity and contingency plans were in place for the DPL and whether steps had been taken to formally document recovery and contingency plans to regain important operations should IT systems be rendered inoperable or inaccessible. In addition, we interviewed the DPL's Director of IT to determine

whether a written, tested business continuity and contingency plan was in place, the criticality of application systems had been assessed, and risks and exposures to computer operations had been evaluated. We also determined whether an alternate processing site had been designated to permit timely restoration of IT capabilities and, if necessary, whether an agreement had been established with the entity providing the alternate site. The alternate processing site would allow DPL to regain processing should its processing site be damaged or become inaccessible. Further, through interviews with DPL's IT Director and an inspection of the on-site facilities, we reviewed DPL's backup procedures and assessed the degree to which copies of backup media were stored in secure on-site and off-site locations.

To determine whether IT-related assets were adequately safeguarded from damage or loss, we reviewed physical security over IT resources through observation and interviews with DPL's IT staff. We determined whether procedures were in place and effect to help prevent unauthorized persons from gaining access to the file server room, areas housing IT equipment, and whether personnel authorized to access the file server room were specifically instructed in physical security operational standards and procedures. We reviewed potential risk factors regarding physical security through inspection of the file server room and the areas housing IT equipment, and through interviews with the management and staff responsible for the file server room and the areas housing IT equipment. Through observation, we determined whether the door to the file server room was locked at all times and whether there was a list maintained of persons authorized to enter the file server room.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems, an uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in the file server room that houses computer equipment. Furthermore, we reviewed control procedures to prevent water damage to automated systems, agency records, and magnetic backup media stored on site.

To determine whether system access security controls were in place to provide reasonable assurance that only those personnel authorized to use the Division's network and microcomputer workstations were able to gain access to programs and data files, we evaluated procedures for logon user ID and password administration. Regarding password administration, we reviewed controls to activate and deactivate user IDs and passwords, require appropriate length and composition of passwords, and to ensure that

passwords are periodically changed. We determined the frequency with which all staff authorized to access the automated systems were required to change their passwords.

To determine whether user ID and password security was being properly maintained, we interviewed the Director of IT. To determine whether access privileges were provided to only authorized users, we reviewed procedures for granting system access and compared a system-generated list of DPL's current users with an HR/CMS employee list for DPL. We determined whether procedures were in place to provide reasonable assurance that the DPL's Director of IT was notified in a timely manner of changes in personnel status (e.g., employment terminations, job transfers, or leaves of absence) that would impact access privileges and possibly require deactivation from the system.

To determine whether adequate controls were in place and in effect to account for IT resources, we initially reviewed the Division's inventory control policies and procedures. We obtained and reviewed the IT-related asset inventory record to determine whether the DPL's hardware inventory records were current, accurate, and valid. We compared recorded data related to a selected sample of computer hardware items from the computer hardware inventory listing to the actual computer hardware on hand, and vice versa. We determined whether computer equipment purchased in fiscal years 2006, 2007, and 2008 were properly recorded on the inventory and that the equipment was available for use. We evaluated the adequacy of inventory controls through tests and observations by assessing the integrity of the inventory record, determining whether computer hardware was properly tagged, and that the equipment serial numbers attached to the items were properly recorded on the inventory list. Furthermore, we reviewed the DPL's IT inventory record to determine whether it contained the appropriate data fields to identify equipment and to indicate the value and location of the item and whether the DPL had conducted an annual physical inventory of IT-related assets. We tested seventy equipment items from the IT inventory record based on an ACL sample

We determined whether controls were in place at DPL to account for the Division's software inventory. We reviewed the policies and procedures for software use and an inventory record of software. We determined that according to the policies and procedures for software usage that only approved applications were to be used by staff.

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 industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Based on our audit, we found that information technology-related controls at the Division of Professional Licensure (DPL) were in place to provide reasonable assurance that control objectives would be met for IT organization and management, physical security, system access security, and environmental protection. The selected mission-critical applications examined for the audit appeared to be secure, easy to use and able to generate reports that satisfied user needs. While evaluating IT-related inventory, we found that controls were in place to safeguard the hardware and software, however, the inventory records needed to be strengthened. Although controls in place provided reasonable assurance that IT resources were recorded on the inventory system of record, inventory control could be strengthened by retaining documentation of the performance and reconciliation an annual physical inventory for audit review.

Regarding business continuity and contingency planning, we determined that although DPL has documented their disaster recovery plans and their continuity of operations plans, control practices needed to be enhanced to provide reasonable assurance that normal business operations could be resumed in a timely manner should office sites become unavailable for an extended period. Although DPL had developed a Continuity of Operations Plan (COOP) and an IT-related disaster recovery plan for restoring services on a temporary basis, further effort is needed to develop a comprehensive business continuity plan to help ensure a long term recovery solution. We acknowledge that an effort to develop a business continuity plan by DPL had been started in conjunction with the assistance of the Massachusetts Information Technology Division. In addition, we determined that control practices and procedures for the generation of on-site and off-site storage of backup copies of magnetic media were adequate.

We found that the DPL has a well-defined organizational and management structure within the IT Department. Our review of organization and management confirmed that DPL's organizational controls included an established chain of command, clearly delineated reporting responsibilities and points of accountability, and documented job descriptions for information technology staff.

We found that physical security controls provided reasonable assurance that IT resources located in the Division's offices, off-site storage area, and file server room were adequately protected against unauthorized physical access. We found that the combination of preventive and detective controls, including management control practices, provided reasonable assurance that IT equipment would be adequately safeguarded. We also found that environmental protection controls over the file server room and office areas provided reasonable assurance that IT resources were operating in a controlled environment. We confirmed that the DPL had procedures and appropriate control mechanisms in place to address environmental protection objectives. Specifically, we found that control objectives would be

met regarding air conditioning; fire prevention, detection, and suppression; floor and emergency fire plans; emergency power and lighting; general housekeeping; and power shut-off.

Regarding system access security, our audit disclosed that the DPL had established adequate system access security controls to provide reasonable assurance that unauthorized access to automated systems would be prevented. We found that appropriate logon procedures were in place to gain access to system resources. In addition, appropriate control practices were in place for password composition, length, and frequency of required change, and that passwords would expire upon reaching a pre-set number of days requiring users to enter a new password to continue having system access.

With respect to business continuity and contingency plans, DPL did not provide a copy of plans that were in development, but only offered the explanation that a business continuity plan was being prepared in conjunction with assistance from the Massachusetts Information Technology Division. Without sufficient business continuity planning, a possible long-term loss of DPL's business sites or computer operations could hinder processing capabilities needed to perform business activities such as licensing functions. However, DPL did have a prepared Continuity of Operations Plan (COOP) which provides management with a high-level framework, establishes operational procedures to sustain functions, and guides the restoration of full functions if normal operations in one or more of DPL's locations were not feasible. The COOP Plan, which is designed to provide guidance to sustain operations only for periods up to 30 days, had not as yet been tested.

Our audit revealed that DPL's inventory record contained adequate fields of information to identify, describe and locate the Division's computer equipment. Our tests revealed that all 70 computer-related items selected from the Division's inventory record were locatable, properly accounted for, and tagged. However, our review of inventory control of computer equipment revealed that the DPL did not record the actual date of acquisition of assets, but only the year of acquisition. Moreover, DPL was unable to provide evidence of that a reconciliation had been performed of an annual physical inventory with the inventory system of record. However, the Division stated that an inventory reconciliation had been performed, but that the records were not retained. DPL should properly record the date of acquisition and maintain evidence of physical inventories and reconciliations performed. With respect to software inventory, we found DPL had appropriate policies and procedures to track software inventory and licenses.

In September 2007, the Division of Professional Licensure was first made aware of a security lapse that included the inadvertent release of certain personally identifiable information (PII) on CDs containing the

names, addresses and social security numbers. Upon learning of the security lapse, the Division took immediate action to temporarily suspend further disclosure of the public information request, to, recover all of the personal information that was inadvertently released, and to notify all licensees of the security information breach. Reportedly all of the personally identifiable information that was inadvertently released was recovered in a short time, and there were no indications or reports of misuse of the information. A private security consultant firm was subsequently engaged to review and provide a report on operation of the DPL concerning the protection of PII. Based on the recommendations of the consultant's report, the DPL began instituting improvements and changes to its procedures to improve the security of its operations with respect to licensing data and PII information.

AUDIT RESULTS

1. Business Continuity and Contingency Planning

We found that DPL has made a good faith effort to develop a disaster recovery plan that documents IT-related recovery strategies to resume business processes in the event that IT systems and network capabilities are rendered inoperable. From a business continuity planning perspective, we also found that although key elements of a high-level continuity plan had been documented, further efforts were needed to address business impact analysis, training, recovery testing, and user area plans. We found that senior management recognized the need for having comprehensive recovery plans in place to help ensure cost-effective resumption of business operations that are dependent upon technology. To DPL's credit, the Division has documented a Continuity of Operations Plan (COOP) and disaster recovery plan and efforts have been initiated to develop a business continuity plan.

We found that the structural content of the COOP and disaster recovery plans contained many of the important elements of a business continuity strategy. However, the formal composition, long term planning considerations, the identification of and a possible written agreement for a relocation site, as well as the required testing of an acceptable business continuity plan, have yet to be accomplished.

Because one of DPL's application systems resides on a mainframe computer operated by the Information Technology Division (ITD) at the Massachusetts Information Technology Center (MITC), the Division is dependent upon ITD to have effective recovery plans in place to support those services. DPL acknowledged that the Division has been included in ITD's biennial recovery tests. However, except for some incident-driven recovery efforts, DPL has not performed disaster recovery tests of their automated systems.

Although, according to the Division, a business continuity plan was in the process of being developed in conjunction with the assistance of the Commonwealth's Information Technology Division (ITD), a draft of the plan was unavailable for review. Without a comprehensive, formal, and tested recovery strategy for the DPL's various application systems, the DPL might experience delays in re-establishing the processing of mission-critical system functions, such as licensing, should a long-term disaster occur.

We found that the DPL has addressed aspects of business continuity planning in their continuity of operations and disaster recovery plans. Since neither of these plans had been tested, the viability of stated recovery strategies could not be verified. In addition, long term strategies needed to be documented, since the COOP is intended to address short-term considerations up to a period of thirty days. We also found that documentation regarding operational procedures and logistics issues specific to the alternate processing sites needed to be developed.

We acknowledge that DPL, together with OCABR, has taken steps to ensure that backup copies of magnetic media were stored in on-site and off-site storage locations and were available for recovery efforts. We note, however, that if a disaster were to occur, the restoration of automated systems is not completely assured, as it has not been supported by documented tests, and although the COOP Plan provides for a short term relocation site in either the OCABR office in Boston (or in the DPL Boston office if the disruption affects only the DPL Springfield office), the disaster recovery plan does not similarly identify a relocation site available for an extended period of time. The disaster recovery plan provides "If an event occurs that restricts access to the Boston office for an extended period of time, or permanently, DPL will work with the Division of Capital Asset Management to quickly find office space to relocate."

Our audit confirmed that procedures regarding on-site storage of backup copies of magnetic media were adequate. We determined that DPL's IT Department has a designated location at OCABR for off-site storage of backup media as well as a secondary location in Springfield, MA. While the backup copies will aid in a recovery strategy, a viable alternate processing site is essential for recovery strategies when the original site is unavailable. DPL has stated that other office locations within the Office of Consumer Affairs could be used as alternate processing sites.

The objective of business continuity planning is to provide reasonable assurance that mission-critical and essential functions will continue or be made available should a disaster cause significant disruption to computer or network operations. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems in relation to business goals and that appropriate recovery and contingency plans are developed as required. Without a formal, tested recovery strategy, DPL might experience delays in re-establishing mission critical functions related to licensure for various consumer services.

An effective business continuity and contingency 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 entity's automated systems 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 and essential data processing functions either at the original site or at an alternate processing site. In addition, the plan should describe the responsibilities and tasks 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. Understandably, if off-site storage of backup media were at the same

location as the alternate processing site, the plan should include procedures for activating another off-site storage location should use of the alternate processing site be required.

The success of the business continuity planning process requires management commitment and close involvement by system users in the development and testing of the recovery plans. Importantly, efforts must be made to ensure that there is a continued clear understanding and documentation of DPL's information system environment and appropriate assessments are made of system criticality and associated risks to support IT and user area plans and business impact. Business continuity test plans and scripts should be developed by IT in conjunction with business process owners and that appropriate change management should be in place to maintain business continuity and contingency policies, procedures and related plans.

A comprehensive business continuity and contingency plan should document the DPL's recovery strategies with respect to numerous disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames.

Recommendation

We recommend that DPL complete its business continuity plan to provide more detailed information regarding the business relocation and alternate operational sites. We recommend that the Division enhance its documentation of business impact, complete the development of a test strategy in conjunction with the Commonwealth's Information Technology Division, and conduct sufficient review and test steps to confirm the viability of the recovery strategies. The DPL should implement procedures to provide reasonable assurance that the criticality of systems is evaluated and business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the IT environment.

DPL should develop contingency plans that would address resumption of critical and essential business functions should MITC be unable to recover wide area network and DPL's mainframe system.

As a necessary requirement to successful recovery, the DPL should ensure through appropriate testing the viability of the alternate processing site(s). Considerations should be made as to the extent of readiness required by the alternate processing site(s). We further recommend that the business continuity and contingency plan once developed and approved be subject to regular testing to ensure its continued viability and the plan should be periodically reviewed and updated as necessary to ensure that it is current, accurate, and complete. The DPL staff should be trained regarding their responsibilities to be carried out in the event of an emergency or disaster. To the extent possible, personnel should be made aware of

manual procedures to be used when automated processing is delayed for an extended period of time. A copy of the business continuity plan should be stored off-site in a secure and accessible location.

The business continuity plan should contain emergency test procedures and test criteria relative to the business restoration portions of the plan, rather than disaster recovery planning, which should already be incorporated in the existing DRP. We further recommend that DPL ensure that the business continuity framework include procedures for reassessing the adequacy of the recovery plan and updating the plan accordingly.

Auditee's Response:

> *The Division of Professional Licensure ("DPL") recognizes the need for a Business Continuity Plan. Please be assured that DPL will continue to work on such a plan. As you know, some pieces of the plan are already in place but DPL will work diligently with ITD to prepare a final, formal plan.*

Auditor's Reply:

We are pleased that the Division of Professional Licensure recognizes the need for a business continuity plan and is working on such a plan with ITD. The business continuity strategy should be sufficiently comprehensive to incorporate various documented disaster recovery scenarios to ensure system availability for DPL's mission-critical operations and business processing. Once the business continuity plan is developed and approved, DPL should ensure that the viability of the plan is maintained as changes to business requirements, technology and the IT environment occur.