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. 2005-0101-7T

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

July 30, 2001 through December 4, 2006

OFFICIAL AUDIT REPORT

JANUARY 30, 2007

TABLE OF CONTENTS

INTRODUCTION

The Division of Insurance (DOI) was established in accordance with Massachusetts General Laws, Chapter 26, and is one of seven agencies operating under the Office of Consumer Affairs and Business Regulation (OCABR). The Division is managed by a commissioner whose term in office is coterminous with that of the governor. The mission of DOI is to regulate the Commonwealth's insurance industry and to license Massachusetts insurance companies, producers, and brokers. The Division, which regulates all aspects of the insurance industry in the Commonwealth, annually, licenses more than 6,200 companies, business entities and HMOs and more than 70,000 insurance producers and brokers, whose licenses are renewed triennially. The Division conducts financial examinations of domestic and foreign insurance companies, audits licensees, reviews rates and policy forms, and participates in rate settings.

The DOI uses information technology (IT) extensively to carry out its mission and support its business operations. At the time of our audit, the DOI's information technology infrastructure consisted of a local area network environment comprised of approximately 160 desktop computers configured to run Windows 2000 and Windows XP along with Microsoft Internet Explorer. While the Office 2003 suite is standard on all desktop computers, some computers have special application software, such as Ultimus, Document Direct, and Attachmate, which are available to specific authorized personnel. All computer workstations at DOI are connected by a 1gigabit Ethernet local area network (LAN) serviced by twelve file servers.

The Commonwealth's Information Technology Division in Chelsea, Massachusetts hosts two Web Applications for the DOI: Producer Renewal Processing (ARE) and Online Producer Appointments (OPRA), which are both run on a Windows 2000 secure server with an MS SQL Server database running under Windows 2000. Information is exchanged between the DOI and the ITD hosted systems via SQL DTS (Data Transformation Services) packages that are hosted within the DOI environment.

The Division's information technology unit manages the servers, workstations, and access to the various DOI applications. Over the past three years the Division, in conjunction with the Office of Consumer Affairs, has participated in the statewide MassMail project with the Windows Professional version installed on all desktop workstations and servers.

The Division's mission-critical application is the Consolidated Licensing and Regulation Information System (CLARIS). The CLARIS application is a transaction-based system that records information on the insurance companies, producers, and brokers licensed to sell insurance in Massachusetts. In addition, through OCABR, the Division tracks and records revenue generated from new insurance licensing, as well as renewals, processed through the Commonwealth's primary accounting and reporting system known as the Massachusetts Management Accounting and Reporting System (MMARS). The DOI has a

dedicated microcomputer to receive information from the Bank of America with respect to the revenue collected through the bank's lockbox system.

The Division also has access to the Commonwealth's wide area network, the Massachusetts Access to Government Network (MAGNet) and to the National Association of Insurance Commissioners (NAIC). The Commonwealth's Information Technology Division manages the Internet firewall for the MAGNet and NAIC connections.

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) examination of controls at the Division of Insurance covering the period of July 30, 2001 through December 4, 2006. The scope of the IT audit, which was conducted from May 12, 2005 to August 30, 2005 and from December 1, 2006 to December 15, 2006, included a follow-up examination of the status of prior audit results regarding internal control documentation and business continuity planning brought forward in our prior IT-related audit report, No. 2001-0101-4C, issued December 19, 2001. The audit also included a general control examination of IT-related internal controls pertaining to organization and management, physical security and environmental protection for computer equipment, logical access security, and hardware and software inventory.

Audit Objectives

The primary objective was to conduct a follow-up audit at the Division of Insurance to determine whether the status of IT issues identified in the prior audit No. 2001-0101-4C regarding internal control documentation and business continuity planning had been corrected.

With respect to IT-related controls, we sought to determine whether adequate IT organization and management controls were in effect to properly support the Division's IT processing environment. We determined whether adequate controls regarding physical security and environmental protection were in place and in effect to safeguard computer operations and IT-related assets. A further objective was to determine whether adequate controls were in place to prevent and detect unauthorized access to DOI's primary application and its data files and to software available through the Division's local area network (LAN) file servers and workstations. Our objective with respect to hardware and software inventory was to determine whether IT-related assets were properly identified, recorded, and accounted for in the Division's inventory records.

We sought to determine whether DOI's business continuity plan would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether proper backup procedures were being performed and whether copies of backup magnetic media were being stored in secure on-site and off-site locations.

With respect to the documentation of internal controls, we sought to determine whether DOI had an agency-specific internal control plan and whether documented internal controls were sufficiently

comprehensive and detailed to support agency business functions, including IT-related operations. In addition, we sought to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of the agency's system of internal controls.

Audit Methodology

To determine the scope of the audit, we performed a pre-audit survey regarding DOI's 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 Division's activities and internal control environment, our pre-audit work included a review of DOI's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT-related activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To obtain an understanding and to evaluate the organization and management of IT operations, we reviewed the Division's organizational structure with respect to IT operations and evaluated reporting lines, oversight mechanisms, and separation of duties. We reviewed IT policies and procedures to determine the level of documentation regarding the IT general control areas related to our audit.

To determine whether IT-related assets were adequately safeguarded, we reviewed physical security and environmental protection over the microcomputer systems and online workstations through observation, conducting interviews with DOI management and staff, and by completing appropriate audit checklists.

We reviewed DOI's logical access security policies and procedures that should be designed to prevent and detect unauthorized access to the DOI data files and systems on ITD's mainframe and DOI's file servers and microcomputer workstations. We reviewed the security procedures with the IT Director and the LAN Manager who were responsible for controlling DOI's access to ITD's mainframe, and DOI's microcomputer systems. We reviewed the access privileges of those staff who were authorized to access applications residing on ITD's mainframe, and DOI's IT systems. Subsequently, we determined whether all system users who were authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. Further, we determined whether users were restricted to only the application programs and data files to which they had been authorized. 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 DOI's data and system resources on ITD's mainframe, and on the MA DOI microcomputer systems. We then compared the list of individuals authorized to access DOI's IT systems to the list of current DOI employees to determine whether all current users were employed by DOI.

To determine whether the DOI's hardware inventory record was current, accurate, complete, and valid, we reviewed information on recently purchased and leased items and compared it to the information recorded on the inventory record, and we conducted verification tests of IT equipment from the inventory record to the items and vice versa. We traced a sample of judgmentally selected hardware items to the inventory record to determine whether the hardware items selected were physically locatable, properly tagged, properly recorded, and accounted for with their historical cost valuation We compared the state identification numbers listed on the hardware inventory record to the actual equipment on hand. DOI records leased IT hardware equipment on its inventory records but does not attach inventory tags to the leased equipment items, serial numbers were compared for the leased equipment items.

To determine whether the DOI had implemented adequate controls to account for licensed copies of application software residing on its file servers and microcomputer workstations, we first sought to obtain an inventory list of software installed or available for use. In addition, to determine whether the DOI could ensure that only authorized copies of software were installed on the automated systems, we interviewed the MIS Director regarding procedures used to install and monitor microcomputer-based software, and requested a list of authorized software.

To assess the adequacy of business continuity planning, we reviewed the nature and extent of formal planning that would be exercised to resume computer operations in the event that the information technology systems were inoperable or were unavailable. We interviewed DOI management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We reviewed policies and procedures regarding backup media to determine whether appropriate controls were in place to ensure that backup copies of data files and software would be available should the automated systems be rendered inoperable. Our review of backup procedures included an evaluation of provisions for on-site and off-site storage of critical backup tapes. We also interviewed DOI management responsible for creating backup copies of computer-related media.

To determine the existence and appropriateness of DOI's internal control plan, we evaluated the internal control documentation received. We reviewed documentation submitted and evaluated it against compliance requirements as set forth in Chapter 647 of the Acts of 1989 i.e., the Commonwealth's Internal Control Act. We then requested documentary evidence of internal control monitoring activities to determine whether appropriate mechanisms were in place to monitor and evaluate the effectiveness of DOI's system of internal controls. In this regard, we also reviewed internal control requirements as established by Chapter 647 and the Office of the State Comptroller's Internal Control Guidelines.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government

Accountability Office and generally accepted auditing practices. With respect to IT-related control objectives and controls, we used the Information Systems Audit and Control Foundation's and the IT Governance Institute's Control Objectives for Information and Related Technology (CobiT), published in July 2000, to identify IT management control practices as criteria for review.

AUDIT SUMMARY

Based on our audit at the Division of Insurance, we found that there was reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, logical access security for the local area network, and environmental protection. We believe that controls should continue to be strengthened in the area of business continuity planning and internal control monitoring to comply with generally accepted control practices and the Division's established policies and procedures. Our review also indicated that improvements should be made regarding information technology hardware and software inventory procedures.

Our review of DOI's IT-related organization and management indicated that adequate organizational controls were in place and that IT-related policies and procedures were reasonably well documented. We determined that physical security controls in place at the DOI office provided reasonable assurance that IT-related resources would be safeguarded from unauthorized access in as much as the building had security guards, and office entrances and areas housing IT resources were controlled by appropriate security devices.

With respect to environmental protection, we found certain controls to be adequate, such as the computer room having fire and smoke detectors, a fire alarm, handheld dry chemical fire extinguishers, an automatic fire suppression system, and a self-contained air filter/dehumidifier and air conditioning unit. Moreover, DOI maintains a bank of UPS units in the computer room and additional units in certain wiring closets to help ensure that there is sufficient continuation of electrical continued power to bring the systems down in a controlled manner under normal circumstances.

Regarding system access security, we found that documented policies of logical access controls provided reasonable assurance that only authorized users had access to the DOI's primary computer system on which the Division's application systems reside. We found that controls over the administration of user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should DOI employees terminate employment or incur a change in job requirements. During our audit, nothing came to our attention to indicate that access privileges granted to individuals were inappropriate given their job responsibilities.

Our tests regarding controls over hardware and software inventory indicated that the Division was not documenting the performance and reconciliation of periodic physical inventories. Our tests indicated that although selected hardware items were locatable, DOI also has adopted the practice of not placing identifying inventory control tags on its newly leased 144 PC workstations or on the newly leased 32 laptop computers and 4 docking stations.

With respect to the Internal Control Plan we found that DOI had prepared a detailed agency- specific Internal Control Plan, as recommended in the prior audit report. However, based on the internal control documentation reviewed, IT-related controls examined, and interviews, sufficient evidence was not provided to demonstrate an adequate level of internal control monitoring and evaluation.

With respect to system availability, we found that DOI had well documented off-site storage and disaster recovery plans. The business continuity plan being developed appeared to reflect an appropriate strategy on paper, however, all procedures were not yet documented, in place, and tested to ensure that the business continuity plan would be viable and function as anticipated.

AUDIT RESULTS

1. Information Technology Inventory

Our review of the IT inventory records and procedures at DOI found that the IT asset inventory control practices and records in place were not fully in compliance with either DOI's Internal Control Plan or the fixed asset inventory instructions promulgated by the Office of the State Comptroller.

There was no documentation of an annual physical inventory procedure having taken place and no indication of reconciliation between the actual physical items at DOI and the inventory records. Also, required data such as cost, date of acquisition, and to a lesser extent description did not always appear on the inventory record to fully identify the individual items.

Based on policies and instructions issued by the Office of the State Comptroller, the DOI Internal Control Plan incorporates the following: …"The MIS Department is responsible for conducting at least an annual inventory of information technology related property and equipment. Each piece of equipment is recorded and valued at historical cost. MIS is currently conducting several audits of IT Equipment annually due to frequent purchases and reorganizations." The Fixed Asset Accounting and Management Policy statement issued by the Office of the State Comptroller provides for the conduct of an annual inventory to verify the existence and location of fixed assets, and the reconciliation of the fixed asset inventory against the books and records maintained by the department, with all changes needed to assets to be entered no later than seven business days after June 30th of each year.

The MMARS Fixed Assets Subsystem Policy Manual and User Guide-Part 1 issued August 2001 defines GAAP Fixed Assets as those costing $50,000 or more and in Chapter 4-1 directs that: "The asset will be recorded onto the system within seven (7) days of acquisition…" The Office of Consumer Affairs and Business Regulation (OCABR) receives a GAAP Fixed Asset Inventory Report of items over $50,000 from DOI and records that information with the Comptroller.

Each agency is responsible not only to maintain an inventory but to inform the Comptroller of assets over $50,000 in the MMARS GAAP Fixed Asset Inventory Report. During the course of the audit, it was brought to DOI's attention of discrepancies in its Non-GAAP Fixed Asset Inventory Report of items under $50,000 and the MMARS GAAP Fixed Asset Inventory Report maintained by Office of Consumer Affairs and Business Regulation. These discrepancies include items disposed in 1995 which continued to appear on DOI's records totaling $76,498 and items purchased in 2003 not appearing on the MMARS GAAP Fixed Asset Inventory Report totaling $58,500. Upon notification DOI and OCABR were able to reconcile the discrepancies between their respective inventories.

Additional discrepancies in the DOI inventory records were noted including: 1) cost data, dates of purchase and serial numbers was reported on the Non-GAAP Report which was not recorded on the DOI

inventory records; 2) variances in numbers and descriptions of computers, servers, and peripheral hardware items existed between the Non-GAAP Report and the Inventory record; and 3) a disparity was noted between the software inventory data appearing on the Non-GAAP Report and the software data appearing on the Inventory record. Sufficient detail did not appear on either the Non-GAAP Report or on the Inventory record to permit a detailed identification of the total variances between the two sets of records.

Recommendation:

We recommend that the DOI establish and maintain a complete and accurate IT inventory record, perform and document a physical inventory verification at least annually, and record any adjustments necessary to bring the inventory records into agreement with the physical inventory in accordance with the Office of the State Comptroller's instructions as outlined in Policy Memo 313A and in the MMARS Fixed Asset Subsystem Policy Manual and User Guide-Part 1, as well as with DOI's Internal Control Plan.

Auditee's Response:

The Division recognizes that its current inventory tracking systems are inadequately capturing all data elements necessary for a complete inventory record as described by the State Auditor's Office. It has been our intention for some time to purchase, install and customize a more sophisticated inventory software package which could broaden and streamline the collection of data for all assets, including those in the information technology area; however these attempts have been hampered by external factors.

It is our intention to bring our current inventory into compliance with the Auditor's recommendations and add additional data to the current inventory record. At the same time, the Division will proceed with our efforts to modernize the inventory system with the purchase of an inventory recording and reporting system that streamlines the collection of such data.

The Division will also proceed with conducting an annual physical inventory by June 30th of each year, which shall consist of reconciling actual physical items and the inventory record.

Auditor's Reply:

We agree with the Division's plan to conduct an annual physical inventory by June 30th of each year. Until a more sophisticated inventory system can be acquired, we suggest that the additional fields required be implemented in the current system. We also suggest the process of acquiring a more sophisticated inventory software package be coordinated with the Office of Consumer Affairs and Business Regulations.

STATUS OF PRIOR AUDIT RESULTS

2. Internal Control Documentation, Monitoring, and Evaluation

Our prior Audit Report No. 2001-0101-4C described that the Division of Insurance (DOI) did not have an agency specific internal control plan to address the agency's operations. During our current audit, DOI produced a Fiscal Year 2005 Internal Control Plan which includes an Agency and Administrative Overview as well as individual Departmental Internal Control Plans concerning the 12 departments within the Division of Insurance. The plan is 49 pages in length and lists Seven Key Internal Control Concepts: 1) Risk Assessments Should be Conducted; 2) Internal Control Plans Must Be Documented; 3) Duties Should Be Segregated; 4) Internal Control Systems Should Be Supervised; 5) Transactions Should Be Documented; 6) Transactions Should Be Authorized; and 7) Access to Resources Should Be Controlled. The Office of the State Comptroller, on its website, lists internal control components which are all addressed in the agency's Fiscal Year 2005 Internal Control Plan.

However, indications are that the procedures described in the internal control plan in Concept No. 4 (above), concerning the supervision (monitoring) function, have not, as yet, been completely put in practice. Although requested by us, during the course of our review, DOI did not provide adequate evidence of formal reviews and assessments of the operation and effectiveness of the Internal Control Plan.

The monitoring component, one of The Five Components of Effective Internal Controls identified by the Office of the State Comptroller, and which is addressed in DOI's Internal Control Plan Concept No. 4, is described in the Office of the State Comptroller's statement as follows: *" Monitoring- After internal controls are put in place, their effectiveness needs to be periodically monitored to ensure that controls continue to be adequate and continue to function properly. Management must also monitor previously identified problems to ensure that they are corrected"*.

Chapter 647 of the Acts of 1989, an act relative to improving internal controls within state agencies requires internal control systems of the agency to be clearly documented and readily available for examination. Objectives for each of these standards are to be identified or developed for each agency activity and are to be logical, applicable, and complete.

As previously stated, DOI has now adopted an agency specific and detailed internal control plan, however, DOI has yet to demonstrate and document that the controls contained in the plan are being monitored to ensure that they are implemented, adequate and are functioning properly.

Recommendation:

We recommend that DOI increase its efforts to monitor and evaluate the effectiveness of its internal controls. It is essential to actually monitor and evaluate the internal controls to ensure that internal

control policies and practices are in effect to provide reasonable assurance that operational and control objectives will be met.

Auditee's Response:

The Division shall implement a process to monitor and document the adequacy of its Internal Control Plan on an annual basis.

Auditor's Reply:

We agree that it is a good practice to evaluate and document the adequacy of the Internal Control Plan on at least an annual basis. It is also important that controls, such as policies, procedures, organizational assignments, and control mechanisms, be monitored and evaluated on an as needed basis to provide sufficient feedback as to whether the controls are in place and in effect. In addition, control evaluations should be adequately documented.

3. Business Continuity Planning

Our prior Audit Report No. 2001-0101-4C described several weaknesses in the Business Continuity Plan in effect at DOI. The described deficiencies concerning data backup and its on-site and off-site storage weaknesses have been satisfactorily addressed and corrected in the draft of the current business continuity plan. However, the previously described weakness concerning the lack of a detailed plan for the restoration of computer functions in the event of a substantial loss of IT operations has not as yet been fully addressed in the plan and not tested.

Items yet to be accomplished in connection with the Business Continuity Planning effort, as described in an OCABR report prepared in October 2004, follow:

> *" What we are planning on doing in the future Develop recovery plan and perform live test, Develop implementation plan, Partner with ITD disaster recovery planning staff, Perform a live test of the recovery plan, and Integrate OCA IT Disaster Recovery planning into overall Business Continuity plan."*

A business continuity plan should document the DOI recovery strategies with respect to various disaster scenarios. Without a formal and tested recovery strategy for the file servers and stand-alone microcomputers, DOI might experience delays in reestablishing the processing of mission-critical information. The lack of a detailed tested plan to address the resumption of processing by the LAN and microcomputer systems might render DOI's data files and software vulnerable should a disaster occur. If the LAN or microcomputers' hard drives were damaged or destroyed, DOI could lose critical, important, and confidential data, including insurance licensing and rating information not yet included on backup media.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans.

During the course of the audit, on August 28, 2006 the Division of Insurance gathered with members of the Massachusetts Emergency Management Agency (MEMA), and others to participate in an interactive Continuity of Operations (COOP) tabletop exercise simulating two significant potential emergencies. An After Action Report was created which addressed the following areas: the identification and prioritization of essential functions, maintaining orders of succession to key positions, preparing their personnel for the possibility of unannounced relocation of essential functions, executing its essential functions at its alternate operating facilities, and addressing the needs of essential and non-essential personnel during an incident.

The DOI is to be commended for participating in this tabletop exercise. However, the tabletop exercise, although an important part in understanding the complexities of a Continuity of Operations or a disaster recovery plan, should be fully tested at an alternative processing site as described in the plan, and not merely simulated in a tabletop exercise.

Recommendation:

We recommend that management, in conjunction with OCABR and key users, thoroughly review their business continuity strategy for comprehensiveness and viability for all mission-critical and essential systems. The DOI should ensure that adequate user area plans are in place to ensure that business processing capabilities can be restored, should IT operations be rendered inoperable or inaccessible. We recommend that the business continuity plan be updated as needed to reflect the current IT infrastructure and be thoroughly tested to the degree possible. We recommend that test scripts be defined and that test results be adequately documented and reviewed by management and business process owners.

Once the business continuity plan has been formally accepted and tested, the plan should then be periodically reviewed and updated to address changes in technology, staff, business conditions or risks to the IT environment. The DOI should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans. The DOI should specify who should be trained in the implementation and execution of the plans under each of the noted disaster scenarios and who will perform each required task to fully implement the plans. Further, copies of the

completed business continuity and user area plans should be distributed to all appropriate staff members. A copy of the plans should also be kept in a secure, off-site location.

Auditee's Response:

> *During the past eighteen months, the Division has devoted considerable internal resources to the examination and development of a continuity of operations plan and a draft disaster response plan. The development of these plans has involved dozens of Division employees working on various aspects of a disaster response strategy, including those related to our regulatory responsibilities as well as those related to restoring our internal essential functions within the Division. The Division recognizes the vital nature of this task and we are committed to ensuring a complete plan is in place that assures the continued operations of the agency in the wake of a disaster or other emergency event.*
>
> *During the next eighteen months, the Division will be finalizing the details of the disaster response plan and working to deploy many of its most critical recommendations. This stage of the project will include a closer examination of our business continuity strategy and plan. The project would rely on the Office of Consumer Affairs' participation in our preparations and a commitment to provide adequate backup facilities and equipment. Our goal is to develop a comprehensive plan that will ensure that business processing capabilities can be restored should our IT operations be rendered inoperable or inaccessible. As recommended, we shall also adopt a plan to test the business continuity strategy on a regular basis and to ensure it is reviewed and updated regularly.*

Auditor's Reply:

The Division of Insurance has shown the most improvement in the area of business continuity planning by addressing data backup and on-site and off-site storage of backup media. Given the magnitude of the potential exposure of not being able to regain IT processing within an acceptable period of time, we strongly suggest that the Division work toward shortening the eighteen-month time frame for completing and testing a disaster recovery and business continuity plan.