The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2007-0158-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON THE EXAMINATION OF INFORMATION TECHNOLOGY RELATED CONTROLS
AT THE STATE OFFICE OF MINORITY AND WOMEN BUSINESS ASSISTANCE

July 1, 2005 through September 18, 2007

OFFICIAL AUDIT REPORT

DECEMBER 4, 2007

TABLE OF CONTENTS

INTRODUCTION

The State Office of Minority and Women Business Assistance (SOMWBA) is an agency within the Department of Business and Technology (DBT) as defined in Section 1(b) of Chapter 23A of the Massachusetts General Laws. The Office was originally created as the State Office of Minority Business Assistance through Chapter 23A, Section 40. Chapter 7, Section 40N of the Massachusetts General Laws is the legislation modifying the Office's title to the State Office of Minority and Women Business Assistance (SOMWBA).

SOMWBA is a federally-subsidized, state-supported agency dedicated to helping women and minorities meet the challenges of participating in affirmative business opportunities throughout the Commonwealth. In addition, SOMWBA helps Disadvantaged Business Enterprises (DBE) compete for contracts funded by the United States Department of Transportation. The DBE certification requirements state the business must be owned and controlled by one or more socially and economically disadvantaged persons as defined by DBE Regulation 49 CFR Parts 23 and 26. The SOMWBA office, which is located at 10 Park Plaza in Boston, Massachusetts, is managed by an executive director and has 18 employees.

SOMWBA provides a certification tool used to enhance a firm's ability to do business in public markets. While SOMWBA-certification does not guarantee that a business will be awarded a contract each time a bid is submitted, certification may add a competitive edge to the bidding process. According to SOMWBA, the Commonwealth of Massachusetts expends in excess of $4 billion annually on business contracts. More than $240 million of this amount is targeted to SOMWBA-certified minority and women-owned businesses.

SOMWBA helps government agencies within the Commonwealth meet their affirmative purchasing and contracting goals by providing information on procurement opportunities and business resources to SOMWBA-certified companies. Finally, SOMWBA publishes and provides an online directory of certified minority and women-owned business enterprises and certified minority and women-controlled non-profit organizations.

Information technology processing at the State Office of Minority and Women Business Assistance is supported by the Department of Business and Technology and is performed by the Department's Chief Information Officer who manages network operations and associated technology to support SOMWBA systems as well as IT services for the other four sub-agencies of DBT. SOMWBA's local area network (LAN) is comprised of 20 workstations. The LAN servers allow users to share software applications and data files, such as electronic mail, word processing, spreadsheets, and fiscal data within the agency. SOMWBA's primary application system is CERTRAK, which is a database containing businesses certified by the agency. The CERTRAK system resides on a file server housed in DBT's file server room and is available through SOMWBA's local area network.

As a sub-agency of the Department of Business and Technology, SOMWBA is dependent upon DBT for much of its IT processing capabilities, internal control planning, business continuity planning, environmental protection, system access security, hardware acquisitions, and payroll support. DBT also provides internal control planning, program support and overall funding. The other sub-agencies are the Massachusetts Office of Travel and Tourism, Massachusetts Office of Business Development, Massachusetts Office of International Trade and Investment, and the Office of Small Business and Entrepreneurship.

The Office of the State Auditor's internal control examination was limited to a review of selected IT general controls over and within SOMWBA's IT environment and an assessment of the adequacy of supporting documentation related to certification and re-certification.

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 State Office of Minority and Women Business Assistance (SOMWBA) for the period July 1, 2005 through September 18, 2007. The audit was conducted from May 2, 2007 to September 18, 2007. Our audit scope included a general control examination of internal controls relating to documented IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. We also performed an assessment of controls in place to ensure that documentation adequately supported determinations of certifications and re-certifications.

Audit Objectives

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

With respect to the availability of automated processing capabilities and access to electronic information resources, we determined whether disaster recovery and business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup procedures were being performed and whether copies of backup magnetic media were stored in secure on-site and off-site locations.

Regarding controls in place to ensure the integrity of the CERTRAK data for certifying applicants seeking to participate in affirmative business opportunities in the Commonwealth, we determined whether SOMWBA conducted adequate reviews and investigations of these applicants. We sought to determine whether supporting documentation would ensure compliance with the requirements of SOMWBA

management's policies related to certification and re-certification and renewal policies for approved minority and women-owned businesses.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding SOMWBA's overall mission and its IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the SOMWBA's activities and internal control environment, we reviewed SOMWBA's mission, organizational structure, and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

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

We reviewed the SOMWBA's system access security policies and procedures to prevent and detect unauthorized access to the SOMWBA software and data files residing on the workstations and DBT's LAN. We reviewed the security policies and procedures with DBT's Chief Information Officer who was responsible for controlling SOMWBA's access to DBT's LAN and desktop workstations. Our examination of system access security also included a review of SOMWBA staff's access privileges to applications residing on the LAN and desktop workstations. Subsequently, we determined whether all system users authorized to access the automated systems were required to periodically change their passwords and, if so, the frequency of password changes. 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 SOMWBA's IT resources on the LAN and desktop workstations. We then determined whether individuals granted access to the system were currently employed by comparing an automated list of IT users to the then most recent payroll listing.

To determine whether IT resources were properly accounted for, we reviewed inventory policies and procedures, interviewed appropriate staff, and examined SOMWBA's system of record for maintaining an inventory of computer equipment. To determine whether SOMWBA's computer equipment inventory record was accurate, complete, current, and valid, we reviewed the inventory data recorded for 39 items (100%) of computer and related equipment and compared this information with that obtained by examining actual equipment located at SOMWBA. Moreover, to determine whether computer equipment that was physically located at SOMWBA was correctly recorded on the inventory, we traced

information regarding selected items to the information listed on the inventory system of record. Further, to test whether purchased hardware was listed on the system of record for inventory and was physically located at SOMWBA, we compared purchase orders and invoices for eight hardware items purchased by the SOMWBA during fiscal year 2006 to the inventory records and located the individual hardware items at the SOMWBA office. We also determined whether all computer equipment tested was properly tagged and then verified the tag numbers to the inventory record.

To assess the adequacy of business continuity planning and disaster recovery, we reviewed the level of planning and established procedures to be followed to resume computer operations in the event that the file servers and/or desktop workstations were rendered inoperable or inaccessible. We interviewed SOMWBA management to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been identified and evaluated, whether a written business continuity plan was in place, and, if so, whether the was plan adequately tested. Our interview also addressed an evaluation of the adequacy of controls to ensure that software and data files would be available for recovery efforts should the automated systems be rendered inoperable. The latter included a review of the adequacy of provisions for on-site and off-site storage back-up copies of magnetic media. In that regard, we interviewed the MIS Director of DBT and staff responsible for creating and storing backup copies of magnetic media.

Our audit methodology included reviewing SOMWBA's fiscal year 2006 and 2007 applicant files; certification program policies, processes, and procedures; certification reports and program statements; monthly staff reports to the Executive Director; and quarterly reports to the independent certification specialists that SOMWBA uses to assess the various eligibility classifications of organizations to participate in Massachusetts business and economic development opportunities.

To evaluate program oversight activities, we reviewed data contained within 75 judgmentally-selected files of SOMWBA's 2,440 applications filed for fiscal years 2006 and 2007, and compared them to the provisions of SOMWBA's governing legislation. In addition, we interviewed the Executive Director and appropriate staff members.

Our audit was conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted auditing practices. Audit criteria used in the audit included management policies and procedures, and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000. CobiT control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices that provides a reference framework for management, users, security practitioners, and auditors.

AUDIT CONCLUSION

Based on our audit, we found that the information technology-related controls in place at the State Office of Minority and Women Business Assistance (SOMWBA) provided reasonable assurance that IT-related control objectives would be met with respect to physical security, environmental protection, system access security, inventory control over computer equipment, and on-site and off-site storage of backup copies of magnetic media. However, IT-related controls needed to be strengthened to provide reasonable assurance that control objectives regarding business continuity planning would be addressed.

We found that adequate physical security was implemented and in place for SOMWBA within the State Transportation Building since the building was subject to parameter security, areas in both the SOMWBA office and Transportation building were locked during off hours, and the building was alarmed to guard against unauthorized access, damage, or theft. We found that SOMWBA's office area housing desktop workstations was also subject to appropriate controls to prevent unauthorized physical access. We found that DBT's file server room was appropriately locked and that only authorized staff had been given keys to the room. We also found adequate physical security controls over the off-site backup storage area.

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

We found that adequate environmental protection, such as smoke detectors and alarms, a water sprinkler system, and an uninterrupted power supply (UPS), were in place in DBT's file server room, as well as throughout DBT's office area, and in the building housing SOMWBA offices and the CERTRAK data system, to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the file server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an UPS was in place to prevent sudden loss of data, and that hand-held fire extinguishers and emergency lighting were located within the file server room. In addition, evacuation and emergency procedures were documented and posted within the file server room. An automatic fire suppression system exists throughout the Transportation building, including the DBT's file server room, DBT's office area and SOMWBA offices.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to SOMWBA's data files and programs residing on the DBT's filer servers and workstations. We found that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should SOMWBA employees terminate employment or incur a change in job requirements. We also determined through observations and interviews that administrative password protection and changes to passwords were adequately controlled through DBT's IT network. We determined that access privileges granted to individuals were appropriate given their job responsibilities and functions. Our tests revealed that all of the current system users were SOMWBA employees.

Regarding on-site and off-site storage of back-up copies of magnetic media, our audit indicated that adequate control procedures were in place. We determined that SOMWBA had implemented procedures and schedules for generating backup copies of magnetic media and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which back-up tapes were stored off-site, and logs were maintained demonstrating the authorized schedule for the transport and return of back-up copies.

Our audit disclosed that SOMWBA did not have a formal, tested, disaster recovery plan to provide reasonable assurance that the CERTRAK case management system and essential data processing operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable. At the time of our audit, SOMWBA had an informal disaster recovery plan and had begun, in conjunction with DBT, to formulate a business continuity strategy. Our audit indicated that the level of disaster recovery and business continuity planning needed to be strengthened to provide detailed documented plans to address recovery strategies and continuity of business operations. Although a potential alternate processing site had been identified, no user area plans had been established to document the procedures to be followed by non-IT staff to support business continuity objectives in the event of a disaster.

Based on our review, we believe SOMWBA should enhance their internal controls to ensure that its certification and re-certification requirements are clearly delineated within the documented procedural instructions followed by the certification specialists. The form that identifies the required documentation should be strengthened to more clearly identify mandatory documents. Also, senior management should ensure that all required supporting documentation is present within an applicant's folder, and can be reconciled within CERTRAK. We found seven instances, within our sample of 35 applications, in which the certification specialist accepted or omitted specific documentation for certification due to their individual interpretation, as well as the lack of specific guidelines within SOMWBA's policies and

procedures. For example, we found that SOMWBA's process for certification does not always require specific documentation from applicants needed to validate permanent residency in the United States.

AUDIT RESULTS

1. Business Continuity Planning

We found that the State Office of Minority and Women Business Assistance (SOMWBA) had appropriate policies and procedures regarding the generation and on-site and off-site storage of back-up copies of magnetic media. However, we determined that SOMWBA did not have a documented and tested disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems that are processed through Department of Business Technology's (DBT) local area network (LAN) be rendered inoperable. SOMWBA had not assessed the relative criticality of the automated systems supporting its operations and identified the extent of potential risks and exposures to business operations. Given that business continuity is a shared responsibility with DBT, it is important that SOMWBA have adequate mechanisms to provide assurance that adequate business continuity plans are in place and that staff are sufficiently trained in performing recovery efforts.

Since SOMWBA is a sub-agency receiving IT support from DBT, SOMWBA needs to coordinate its disaster recovery and business continuity plans with that of DBT. One means of performing this is to have SOMWBA and the other sub-agencies that report to DBT develop and maintain appropriate user area plans for each sub-agency. The user area plans would allow the sub-agencies to meet their respective business continuity planning responsibilities that affect only their agency, while the department-wide disaster recovery and business continuity plan developed by DBT would coordinate the planning of the various sub-agencies into one cohesive set of recovery and contingency strategies.

Although a potential alternate processing site had been identified, no user area plans had been established to document or test the procedures to be followed by non-IT staff to support business continuity objectives in the event that SOMWBA's IT processing were lost should a disaster occur. The absence of a tested business continuity plan, which designates an alternate processing site, places at risk the SOMWBA's ability to regain mission-critical and essential data processing operations that support administrative functions within an acceptable time period. A coordinated business continuity planning effort between SOMWBA and DBT is needed to ensure that the primary application system, CERTRAK, which is accessed through DBT, would be available for processing.

Recommendation:

The SOMWBA should develop, in conjunction with DBT, business continuity plans (user area plans) appropriate to business and operational objectives, potential risks and exposures, and the relative importance of SOMWBA systems and data. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to SOMWBA's operations or the overall IT environment. We recommend that SOMWBA obtain assurance from DBT that network-based functionality would be available within an acceptable period of time at an alternate processing site.

Auditee's Response

> *The strengthening of IT controls is a continuous process supported in full by our Secretariat, the Office of Housing and Economic Development. Oversight of our IT controls will be supported through the complete rewrite of our disaster recovery plan, the implementation of our new SOMWBA policies, and the IT backup plan that has recently been implemented through our Secretariat as discussed below.*
>
> *The Executive Office of Housing and Economic Development will in the next two months rewrite its disaster recovery plan to incorporate all sub-agencies. The Secretariat has also just implemented a new remote back-up system whereby all data at One Ashburton Place and 10 Park Plaza (Transportation Building) are backed up to the SAN at OCABR at South Station. This will ensure a seamless and automatic backup plan that will complement our backup strategies that we already have in place. We anticipate a dry run through the disaster plan to identify any issues that will be problematic by the end of this year. If there is any slippage in this implementation due to circumstances that are beyond our control, we will be happy to notify you of any change in schedule.*

Auditor's Reply

We are pleased that the Executive Office of Housing and Economic Development will be redrafting their disaster recovery plan that will incorporate all sub-agencies, including SOMWBA. We acknowledge that recovery efforts will be supported by enhanced backup capabilities. We agree with the approach to first conduct a dry run review of the recovery strategies. We believe, however, that a comprehensive risk assessment would benefit the development of recovery and contingency plans, including user area plans that are more focused on non-IT processes.

2. Certification Data

Our audit revealed that although SOWMBA has evaluation criteria and required source documentation to support how a business is to be classified, the criteria requirements need to be more clearly delineated and specific information in the database should be monitored more closely to ensure that SOMWBA certification specialists are adhering to the Office's policies and procedures.

Our tests of the information contained in the CERTRAK database consisted of a judgmental sample of 35 out of 2,275 SOMWBA hardcopy files for individuals seeking SOMWBA certification for the fiscal years 2006 and 2007. The 35 individual files were reviewed for eight data elements requiring various forms of supporting documentation. The eight documents required for certification were applications, notarized statements of validity, documentation showing ethnicity, proof of permanent residency or citizenship, documentation showing gender, bank signature cards or corporate resolutions, tax returns, and proof of minority certification from out of state when applicable. There were seven discrepancies found within five of the 35 hardcopy files reviewed. Our test results revealed that all 35 SOMWBA certified businesses filled out an application, had either a bank signature card or a corporate resolution, had copies of their tax returns, and were certified as minority businesses in their own states, where applicable.

Out of a total of 35 SOMWBA certified businesses required to show proof of permanent residency or citizenship of the owners, two businesses did not have proof of either. Out of a total of 35 notarized statements of validity, for one application the name for the embossed stamp of the notary public did not match the actual signature of the notary public. Out of a total of 26 SOMWBA certified business filers required to show ethnicity, one business did not have a document showing ethnicity, and an additional business was designated as a Minority Women Business Enterprise (MWBE) even though the ethnicity of this business owner could not be determined because there was no documentation to indicate that the owner was either a minority or a woman. Two out of the 11 SOMWBA certified businesses required to provide a document showing gender did not have documents showing gender.

SOMWBA's policies and procedures for determining that an applicant is a woman require "Document showing gender, i.e., copy of birth certificate or similar proof." In one instance SOMWBA accepted a Marriage Certificate that did not indicate the birth date of the woman being married. Also, the policies and procedures leave it up to the individual applicant whether they should provide proof of permanent resident status or whether it is non-applicable. This policy is inconsistent with 425 CMR 2.00, which states, "The burden of proof shall be on the applicant show that it meets the certification criteria." 425 CMR 2.00 also states, "Eligible Person means: An adult permanent resident of the United States who is a minority or woman" therefore, the applicant must show proof of permanent residency, not take it upon themselves to make the decision whether or not it is applicable. SOMWBA policies and procedures require a minority applicant to provide "Document showing ethnicity, i.e., copy of birth certificate or similar proof." One applicant reviewed provided a birth certificate and driver's license with a photograph, however, neither of the documents provided evidence of minority status.

Generally accepted control practices for supporting documentation require that documented evidence should support decisions made in regard to eligibility or classification criteria set forth in established policy, standard procedures, or regulation. Standard practices also require that sufficiently detailed

procedures be available to staff to ensure consistent decision making and collection of supporting documentation.

We determined that SOMWBA could not provide reasonable assurance that control and business objectives would be achieved pertaining to SOMWBA certification for eligible business enterprises. The absence of thorough, detailed policies and procedures leads employees to rely on their individual interpretations of what is required as documentation for SOMWBA certification. In such circumstances, management may not be adequately assured that desired actions will be taken and that sufficient documentation is obtained.

Recommendation:

Based on our review, we believe SOMWBA management should enhance their internal controls to ensure that its certification and re-certification requirements are clearly delineated within the documented procedural instructions followed by the certification specialists. The form that identifies the required documentation should be strengthened to more clearly identify mandatory documents. Also, senior management should ensure that all required supporting documentation is present within an applicants folder and can be reconciled within CERTRAK. SOMWBA's policies and procedures for applicants applying for certification should be strengthened to more clearly specify required supporting documentation.

Auditee's Response

Filing System Upgrade for Certification Cases and Reconciliation of Supporting Documentation in File and Certrak

SOMWBA recognizes the lack of uniformity in the certification process and has moved immediately to implement a new application including a unified document list detailing the documents required. The new application and document list in conjunction with the newly formulated policies on the regulatory requirements for certification will dramatically improve the quality and uniformity of certification. We anticipate completion of this system upon implementation of our policy as highlighted below.

Implementation of SOMWBA Certification Policy and Procedures

SOMWBA has recently developed a major revision of the criteria for certification that will incorporate an expansion of the traditional SOMWBA criteria along with the addition of new criteria for business viability and development. In this new policy we have addressed specifically all of the concerns raised in the IT Audit including uniform procedures and documentation for the determination of citizenship, minority and gender status.

To implement the program we have developed a timeline for training and communication to our SOMWBA businesses, the federal, state and local agencies that support SOMWBA, and the general public. The Certification Policy Training for our certification specialists and case managers will be conducted over a 6 week time frame with classes scheduled two days a week for a total of 3 hours per week. The Program will be based on case studies and

analysis of specific problems based on actual practice and implementation of the new Certification Policy. The modules will focus on the new criteria and process for certification, the construction reform law, and a business writing module. The training will begin the week of December 4, 2007 and will be completed the week of January 10, 2008. In addition to the internal training, the external communication will be implemented in accordance with the process and schedule highlighted below.

Auditor's Reply

We commend SOMWBA for initiating corrective action regarding supporting documentation to validate certification status under the various SOMWBA classifications. SOMWBA should continue to perform quality standard reviews of the certification classifications being determined by their case management staff.