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. 2007-0664-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY RELATED CONTROLS AT THE GEORGETOWN HOUSING AUTHORITY

May 31, 2007 through July 20, 2007

OFFICIAL AUDIT
REPORT
OCTOBER 3, 2007

TABLE OF CONTENTS

INTRODUCTION

The Georgetown Housing Authority (GHA), which was established through Section 3 of Chapter 121B of the Massachusetts General Laws, provides affordable housing programs for the elderly, disabled individuals or couples, and low-income families. Residents of the town of Georgetown receive a preference in the selection process for housing services.

The Authority owns and manages 136 units of affordable housing that are subsidized through various State housing programs. GHA's State housing inventory consists of 126 units of elderly/disabled housing and 10 units of multi-bedroom family housing. GHA is governed by housing regulations issued by the Massachusetts Department of Housing and Community Development (DHCD). A five-person Board of Directors also provides oversight to GHA; four who are elected and one member who is appointed by the Governor. GHA's Executive Director is responsible for the administration of the Authority's programs and services The Authority, whose central office is located at 23 Trestle Way in Georgetown, was staffed by six employees at the time of our audit.

The Authority's computer operations were supported by desktop and laptop computer workstations located at the central office. GHA's primary application system is a vendor-supplied, integrated application system known as the Management Computer Services (MCS) system. The MCS application provides data processing functions using a module-based system to provide processing support for multiple housing authority functions. In addition, GHA utilizes Microsoft Office 2000-based applications to maintain its fixed-asset inventory, rental information, tenant applications, and other correspondence.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within GHA's IT environment.

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 Georgetown Housing Authority (GHA) for the period of May 31, 2007 through July 20, 2007. The audit was conducted from June 27, 2007 through July 20, 2007. Our audit scope included an examination of selected IT-related general controls pertaining to 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.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect to support GHA's IT processing environment. In this regard, we sought to determine whether GHA's IT-related internal control environment, including policies, procedures, and practices provided reasonable assurance that control objectives would be achieved to support business functions.

Our audit objective regarding physical security was to determine 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 also determined whether adequate environmental protection controls were in place to prevent and detect damage to, or loss of, computer equipment and data.

Our objective regarding system access security was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to GHA's application system and data files. We evaluated whether procedures were in place to prevent unauthorized user access to automated systems and IT resources through GHA's workstations. In addition, we determined whether GHA monitored password administration.

With regard to inventory control over computer equipment, including the notebook computer, we reviewed control policies and practices regarding the accounting for computer equipment. In addition, we determined whether an annual physical inventory and reconciliation was conducted.

With respect to the availability of automated processing capabilities and access to IT resources and data, we determined whether 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.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding GHA's overall mission and IT environment. Regarding our review of IT policies and procedures, we interviewed senior management and staff, completed questionnaires and obtained and reviewed existing IT-related policies, standards, and procedures. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also interviewed GHA staff regarding the extent to which IT policies and procedures were documented and identified.

To determine whether computer equipment and backup copies of magnetic media stored on-site and off-site were adequately safeguarded from damage or loss, we reviewed physical security over the IT resources through observations and interviews with senior management. We conducted walk-throughs, observed, and identified security devices. We determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to GHA's computer workstations. We reviewed control procedures for physical access, such as key management regarding door locks to the central office. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms.

With respect to environmental protection, our objective was to determine whether controls were adequate to prevent and detect damage to, or loss of, IT-related equipment and media for GHA's workstations at the central office. To determine the adequacy of environmental controls, we conducted walkthroughs of office areas housing IT equipment at GHA's main office. Our examination included a review of general housekeeping; fire prevention, detection and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews and observation.

We reviewed GHA's system access security policies and procedures to prevent unauthorized access to GHA software and data files residing on its workstations. We discussed the security policies and procedures with the Executive Director, who was designated as being responsible for controlling access to GHA's desktop computers. Our examination of system access security included a review of the staff's access privileges to applications residing on GHA's computers. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition, length, and frequency of password changes. To determine whether adequate controls were in place to ensure that access privileges to automated systems were only granted to authorized users, we reviewed procedures for authorizing access to IT resources residing on GHA's computers. We then determined

whether individuals granted access to the systems were currently employed by GHA by comparing a list of individuals authorized to access the system with an official listing of current employees.

With regard to inventory control over IT equipment, we determined whether an annual physical inventory was conducted and whether IT equipment was properly recorded in the fixed-asset inventory. To determine whether adequate controls were in place and in effect to properly account for GHA's computer equipment, we reviewed inventory control policies and procedures and requested and obtained GHA's inventory system of record for computer equipment. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related fixed assets.

To assess the adequacy of business continuity planning, we evaluated the extent to which GHA had plans that could be activated to resume IT-supported operations should the MCS system be rendered inoperable or inaccessible. We interviewed senior management to determine whether GHA had formally documented procedures for the development and maintenance of appropriate business continuity plans. We also determined the extent to which GHA had performed a risk analysis with regard to the loss of IT-enabled business operations. As part of our examination of business continuity planning, we determined whether GHA was generating and storing backup copies of magnetic media, and we reviewed physical security and environmental protection controls for GHA's on-site storage. In that regard, we interviewed IT staff responsible for creating and storing backup copies of computer-related media and security procedures associated with backup tape storage. We further sought to determine whether IT personnel were aware of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances.

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 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), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Georgetown Housing Authority (GHA), we found that internal controls in place 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 storage of backup copies of magnetic media. We determined, however, that GHA's internal controls in place did not provide reasonable assurance that IT-related control objectives would be met with respect to disaster recovery and business continuity planning. At the time of our audit we found that GHA was not storing backup copies of magnetic media at a secure off-site location. In addition, we found that GHA needed to develop a comprehensive disaster recovery and business continuity plan to ensure an adequate level of system availability to support the restoration of network and business operations within an acceptable period of time.

Regarding documented IT-related internal control policies and procedures, we found that although GHA had informal policies and procedures in existence, the Authority needed to develop and promulgate formal policies and procedures for physical security, environmental protection, systems access security, inventory control over computer equipment, on-site and off-site storage of backup copies of magnetic media, and business continuity and contingency planning. The absence of formal documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced. We recommend that GHA document and formalize its control procedures with respect to IT security and operations.

Our examination of physical security revealed that controls in place and in effect provided reasonable assurance that GHA's IT resources were safeguarded from unauthorized access. Our review of office areas housing computer workstations disclosed that the office was kept locked. We also found that the GHA administrative office was equipped with burglar alarms. However, we found that GHA did not maintain a list of individuals who were authorized to access the office areas.

Regarding environmental protection, we found that GHA had adequate controls in place and in effect. We found that GHA had environmental protection controls, including smoke detectors and alarms and an emergency power supply to help prevent damage to, or loss of, IT-related resources. However, we found that GHA did not have a sprinkler system. Our audit disclosed that the central office housing IT resources was neat and clean. General housekeeping procedures were adequate, and temperature and humidity levels within the office were appropriate. We found that an uninterruptible power system (UPS) was in place to prevent sudden loss of data and that hand-held fire extinguishers were located

within the office area housing IT resources. We found, however, that evacuation and emergency procedures were not documented and posted within the office area.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to GHA's data files and programs residing on GHA's computers. We found that administrative controls over user ID's and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should GHA employees terminate employment or incur a change in job requirements. However, through observations and interviews, we determined that administrative password protection and changes to passwords could be improved. We also determined that access privileges granted to individuals were appropriate, given their job responsibilities and functions. Our testing revealed that all of the current system users were GHA employees. Our audit also revealed, however, that GHA's system access policies and procedures needed to be formally documented.

Our audit disclosed that GHA had not developed a formal, tested, disaster recovery plan to provide reasonable assurance that its 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, the Authority had not developed a formal disaster recovery plan nor formulated a business continuity strategy. GHA management needs to provide detailed documented plans to address recovery strategies and continuity of business operations. Although we found that informal procedures were in place regarding the storage of backup copies of magnetic media in a secure on-site location, at the time of our audit, GHA was not storing backup copies of magnetic media in an off-site storage location.

With respect to inventory control over computer equipment, we found that GHA was adhering to the policies and procedures promulgated by the Office of the State Comptroller and had conducted an annual physical inventory and performed a reconciliation of fixed assets. We found that GHA's inventory system of record for computer equipment contained adequate columns of information, including location, tag number, serial number, and description. In addition, we found that the computer equipment items on GHA's May 31, 2007 inventory listing were locatable and properly recorded. However, we found that GHA had not recorded the costs of individual computer equipment items on its May 31, 2007 inventory listing.

AUDIT RESULTS

Disaster Recovery and Business Continuity Planning

Our audit determined that although Georgetown Housing Authority had in place provisions for performing on-site back up of magnetic media, GHA did not have a documented disaster recovery strategy and had not developed a formal business continuity plan that would provide reasonable assurance that essential business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. At the time of our audit, management of GHA had not made arrangements for a permanent alternate processing site. In addition, GHA had not formally assessed the relative criticality of the IT environment supporting GHA operations and identified the extent of potential risks and exposures to business operations.

GHA's mission-critical application system is a vendor-supplied, integrated application known as the Management Computerized Services (MCS) system. The MCS application provides GHA with essential data processing functions. GHA maintains sensitive tenant file information on the Authority's computer system. Our review indicated that GHA's data, documentation, software, and system configuration could potentially be lost if IT processing capabilities are unavailable.

The objective of business continuity planning is to help ensure the continuation of essential functions enabled by technology should a disaster cause significant disruption to computer operations. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required.

Contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

Recommendation

We recommend that Georgetown Housing Authority assess its automated processing environment from a risk management and business continuity perspective and develop and test appropriate business continuity plans. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to GHA's operations or the overall IT environment.

The business continuity plan should document GHA's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities, needed to effectively and efficiently recover network or IT operations within the needed time frames. We recommend that the business continuity plan be tested and periodically reviewed and updated, as needed, to ensure its viability. GHA's completed plans should be distributed to all appropriate staff, who in turn should be trained in the execution of the plans under emergency conditions. In addition, a complete copy of the plan should be stored in a secure off-site location.

Auditee's Response

In response to the IT Audit performed on June 27, 2007 to July 20, 2007. I am currently working on a Comprehensive disaster recovery and business continuity plan to add to the GHA management Plan. On July 22, 2007 we began off site storage for our magnetic media.

Auditor's Reply

We acknowledge Georgetown Housing Authority's goal to write a comprehensive disaster recovery and business continuity plan that will be added to the GHA management plan. The storage of magnetic media in an off site location is an important element in disaster recovery planning. We note that until the a disaster recovery and business continuity plan is developed and tested, the Authority remains potentially vulnerable to being unable to regain mission-critical IT processing within an acceptable period of time.