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. 2007-0596-4T

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

April 30, 2007 through June 15, 2007

OFFICIAL AUDIT

REPORT

OCTOBER 3, 2007

TABLE OF CONTENTS

INTRODUCTION

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

The Authority owns and manages 263 units of affordable housing that are subsidized through various state housing programs. AHA's state housing inventory consists of 205 units of elderly/disabled housing, 50 units of multi-bedroom family housing, and 8 units of housing for the chronically mentally ill. The Authority also administers the following two federal housing programs: voucher program (62 housing choice vouchers) and a 24-unit federally-subsidized program for men in recovery with a history of drug and alcohol abuse.

The Authority is governed by housing regulations issued by the United States Department of Housing and Urban Development (HUD) and the Massachusetts Department of Housing and Community Development (DHCD). A five-person board of directors also provides oversight to AHA; four who are elected members and one who is appointed by the Governor. AHA's Executive Director is responsible for the administration of the Authority's programs and services. The Authority, whose central office is located at 180 Main Street in Amesbury, was staffed by eight employees at the time of our audit.

During our audit, the Authority's computer operations were supported by one file server, five desktop microcomputer workstations, and notebook computers located at the central office. The file server provides network support for AHA's local area network (LAN). The Authority's primary application system is a vendor-supplied, integrated application known as the Computerized Housing Authority System (CHAS). The CHAS application provides data processing functions using a module-based system for the following**:**

(a) public housing, portability, Section 8 housing, and general work orders;

(b) mail merges for tenant, vendor, landlord and tenant application activities;

(c) cash receipts and disbursements, payroll, accounts payable, and general ledger; and

(d) fixed asset –hardware items, furniture and equipment assets.

The Authority also uses 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 AHA'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 Amesbury Housing Authority (AHA) for the period of April 30, 2007 through June 15, 2007. The audit was conducted from May 24, 2007 through June 15, 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 the Authority's IT processing environment. In this regard, we sought to determine whether AHA'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 AHA'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 the local area network file servers and workstations. In addition, we determined whether AHA was actively monitoring password administration.

With regard to inventory control over computer equipment, including notebook computers, 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 AHA'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 AHA 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 the file server and the central office. We reviewed control procedures for physical access, such as the authorization of staff to access the file server closet, and key management regarding door locks to the central office and other areas housing IT equipment. 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 AHA's file server and workstations at the central office. To determine the adequacy of environmental controls, we conducted walkthroughs of the room containing the file server and office areas housing IT equipment at AHA's central 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 the Authority's system access security policies and procedures to prevent unauthorized access to AHA software and data files residing on the LAN. We discussed the security policies and procedures with the Executive Director, who was designated as being responsible for controlling access to AHA's LAN and desktop computers. Our examination of system access security included a review of the staff's access privileges to applications residing on the LAN and the desktop 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 the automated systems were granted only to authorized users, we reviewed procedures for authorizing access to AHA's IT resources residing on the LAN and desktop computers. We then determined whether individuals granted access to the systems were currently employed by AHA 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 evaluated whether an annual physical inventory was conducted and whether IT equipment was accurately reflected in the fixed-asset inventory. We also evaluated whether the IT resources were properly accounted for in the IT system of record. To determine whether adequate controls were in place and in effect to properly account for AHA's computer equipment, we reviewed inventory control policies and procedures and requested and obtained AHA'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 AHA had plans that could be activated to resume IT-supported operations should the network and server be rendered inoperable or inaccessible. We interviewed senior management to determine whether AHA had formally documented procedures for the development and maintenance of appropriate business continuity plans. We also determined the extent to which AHA 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 AHA was generating and storing backup copies of magnetic media, and we reviewed physical security and environmental protection controls for AHA'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 Amesbury Housing Authority (AHA), 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 AHA'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. We found that AHA was not storing backup copies of magnetic media at a secure off-site location. In addition, we found that AHA 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 AHA had informal policies and procedures in existence, AHA 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 AHA 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 AHA's IT resources were safeguarded from unauthorized access. Our review of the file server closet and office areas housing desktop workstations disclosed that the office was kept locked and that a list was maintained of individuals who were authorized to access the office areas. We also found that the AHA administrative office was equipped with burglar alarms.

Regarding environmental protection, we found that AHA had adequate controls in place. We found that AHA had environmental protection controls, including smoke detectors and alarms, sprinkler systems, and an emergency power supply to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the administrative office housing the file server closet was neat and clean, general housekeeping procedures were adequate, and temperature 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 the file server closet. We found, however, that evacuation and emergency procedures were not documented and posted within the office area housing the file server closet.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to the Authority's data files and programs residing on AHA's server and workstations. We found that administrative controls over user ID's and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should AHA employees terminate employment or incur a change in job requirements. Also, through observations and interviews, we determined that administrative password protection and changes to passwords were adequately controlled through AHA's IT network. 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 current AHA employees. Our audit also revealed, however, that AHA's system access policies and procedures needed to be formally documented.

Our audit disclosed that AHA 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, AHA had not developed an informal disaster recovery plan nor formulated a business continuity strategy. AHA management needs to develop detailed documented plans to address recovery strategies and continuity of business operations. Although informal procedures were in place regarding the storage of backup copies of magnetic media in a secure on-site location, we found that AHA had not made provisions for the off-site storage of backup magnetic media.

With respect to inventory control over computer equipment, we found that AHA 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 AHA's inventory system of record for computer equipment contained adequate fields of information, including location, tag number, serial number, and description. In addition, we found that the computer equipment items on AHA's April 30, 2007 inventory listing were locatable and properly recorded.

AUDIT RESULTS

Disaster Recovery and Business Continuity Planning

Our audit determined that although Amesbury Housing Authority had procedures in place for performing on-site back up of magnetic media, AHA did not have a documented disaster recovery strategy. In addition, the Authority 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 AHA had not made arrangements for the storage of backup copies of magnetic media in a secure off-site location. In addition, the Authority had not formally assessed the relative criticality of the IT environment supporting AHA operations nor identified the extent of potential risks and exposures to business operations.

The Authority's mission-critical application system is a vendor-supplied, integrated application known as the Computerized Housing Authority System (CHAS). The CHAS application provides AHA with essential data processing functions. The Authority maintains sensitive tenant file information on CHAS and on the local area network. Our review indicated that IT processing capabilities could be unavailable and software and important data files could be placed at risk if IT resources were rendered inoperable or were damaged.

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 Amesbury 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 AHA's operations or the overall IT environment.

The business continuity plan should document AHA'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. The Authority's completed recovery plans should be distributed to appropriate staff, who in turn should be trained in the execution of the plans under simulated emergency conditions. In addition, the Authority should initiate the storage of backup copies magnetic media in a secure off-site location. A hardcopy and electronic copy of the business continuity plan should also be stored in the off-site storage location.

Auditee's Response

> *In response to . . . the draft audit report provided by your agency . . . the suggestions contained with the report are being addressed. This agency is in the process of creating:*
>
> - *Comprehensive Disaster Recovery Plan*
> - *Business Continuity Plan*
> - *Emergency Evacuation Procedures*
> - *Alternate storage and back-up of confidential data through an off-site web-based software vendor (MCS Computer Systems of LaCrosse, Wi).*
> - *Documented operational policies and procedures including IT-related operations.*
> - *Information technology-related planning documents such as computer or information systems strategic plans.*
> - *A list of staff involved in IT operations including their job descriptions and responsibilities.*
> - *Documents or reports that would provide a description of your automated processing environment (identification of hardware, operating system software, application systems interfaces with external systems).*
> - *A descriptive information regarding the Authority's mission critical IT application system.*
> - *Copies of any vendor contracts related to support of automated mission-critical applications.*
> - *Documentation of the IT-related internal control systems of the Authority.*
> - *Current inventory listing of IT equipment.*
>
> *This series of documents will soon be completed and will be forwarded to the Auditor's Office for review.*

Auditor's Reply

We acknowledge Amesbury Housing Authority's goal to write a comprehensive disaster recovery and business continuity plan as well as documenting other procedures. The back-up storage of media with an off-site web-based software vendor 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. Furthermore, in addition to backing up the application systems, the Authority needs to ensure that network software and files are also backed up.