Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued January 26, 2012

Lynn Housing Authority and Neighborhood Development

For the period January 1, 2007 through December 31, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Lynn Housing Authority and Neighborhood Development (LHAND), which was established by Chapter 121B, Section 3, of the Massachusetts General Laws, provides for the construction, acquisition, rehabilitation, and management of rental housing for low-income persons residing in Lynn. LHAND's primary mission is to assist low- and moderate-income families and individuals with safe, decent, adequate, and affordable housing with an emphasis on fostering economic independence and homeownership opportunities without discrimination, and addressing housing impediments for the special-needs population. In addition to providing public housing, LHAND makes affordable housing available through several rental assistance programs, such as the federal Section 8 voucher program and the state-funded Massachusetts Rental Voucher Program.

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of selected IT-related controls at LHAND for the period January 1, 2007 through December 31, 2010. Our audit objective was to determine whether LHAND's information technology-(IT) related internal control environment and documented policies and procedures provided reasonable assurance that IT control objectives would be achieved to support LHAND's business functions and whether LHAND had appropriate management control practices in place regarding the protection of personal information. Our audit scope also included a follow-up examination of corrective actions taken by LHAND to address the audit results and recommendations contained in our prior audit report No. 2005-0699-4T, dated September 8, 2006.

Our audit noted certain deficiencies in LHAND's IT-related internal control environment, documented policies and procedures, and management control practices for the protection of personal information. Specifically, our audit determined that although LHAND had taken steps to address the prior audit issues of disaster recovery and business continuity planning, system access security, and inventory controls over fixed assets, further improvements were necessary.

Our prior audit of LHAND revealed deficiencies in the areas of (a) disaster recovery and business continuity planning, (b) system access security, and (c) inventory controls over fixed assets. Our follow-up review revealed that although LHAND had taken steps to address these issues, improvements were still necessary, as discussed below.

Our prior audit report disclosed that LHAND had not developed an approved, comprehensive, and tested disaster recovery and business continuity and contingency plan for restoring processing functions in the event that automated systems were rendered inoperable or inaccessible.

Our follow-up review noted that although LHAND had taken steps to address this issue, it still had not developed a written disaster recovery and business continuity plan containing detailed emergency/evacuation plans, a list of mission-critical and essential automated systems, information related to the restoration of IT services, emergency declaration, a contact list, and sufficient recovery strategies and identification of resources to restore IT systems and business operations in a timely manner should IT systems be rendered unavailable for an extended period. In addition, LHAND had not designated an alternate processing site for backup recovery of IT capabilities. Depending on the nature and extent of a loss of IT systems or processing, LHAND could experience difficulties in regaining mission-critical and essential business processes within an acceptable period of time given the absence of a sufficiently comprehensive recovery and business continuity plan specific to LHAND.

b. System Access Security **8**

Our prior audit report disclosed that system access security controls over LHAND's network needed to be strengthened to ensure that only authorized users would have access to the system. Specifically, our audit found that although limited system access security policies were in place, LHAND lacked adequate policies and procedures for password controls, user authorization and activation, and changes in employee status.

Our follow-up review disclosed that LHAND had made improvements in this area by implementing appropriate control practices for personnel authorization and access to network resources and changes in employee status. However, documented policies and procedures still needed to be improved regarding password formation, use, and frequency of change. In addition, LHAND did not monitor employee compliance with its password administration and system user lockout policies. As a result of these issues, LHAND cannot ensure that mission-critical systems and confidential data are adequately safeguarded from access by unauthorized persons.

c. Inventory Controls over Fixed Assets **10**

Our prior audit report revealed that LHAND needed to improve its inventory controls over IT resources. Specifically, the prior audit determined that LHAND's IT and Procurement sections were maintaining separate inventory records, each of which listed different information regarding computer equipment items and neither of which was complete or reconcilable to the other. In addition, the prior audit report noted that written and approved policies and procedures for inventory control were not in place for LHAND's IT resources, the IT inventory listing did not include all relevant data fields (e.g., acquisition date, cost), and three of 56 hardware inventory items recorded on the perpetual inventory could not be located.

Our follow-up review indicated that LHAND had taken steps to address this issue by implementing certain recommendations in the prior audit report. Specifically, LHAND had updated and consolidated its computer equipment inventory records and recorded all required asset information, documented its policies and procedures regarding the ordering and purchasing of fixed assets, properly tagged its computer equipment, and maintained a current and complete list of licensed software at LHAND office locations. Moreover, our inventory testing revealed that all computer items could be located.

However, we found that LHAND's internal controls over inventory could be further strengthened. Specifically, although LHAND management claimed that it had taken an annual physical inventory of computer equipment, it did not maintain evidence that such a physical inventory was conducted or reconciled to LHAND's asset records. In addition, LHAND was not requiring employees to sign control sheets for assigned notebook computers to acknowledge user responsibilities for security and acceptable usage.

INTRODUCTION

Background

The Lynn Housing Authority and Neighborhood Development (LHAND), which was established by Chapter 121B, Section 3, of the Massachusetts General Laws, provides for the construction, acquisition, rehabilitation, and management of rental housing for low-income persons residing in Lynn. LHAND is governed by a five-member Board of Directors, one of whom is appointed by the Governor and four whom, including a tenant representative, are appointed by the Mayor of the City of Lynn. LHAND's primary mission is to assist low- and moderate-income families and individuals with safe, decent, adequate, and affordable housing. Additionally, LHAND provides neighborhood services and funds a range of loan and grant activities to address the needs of renters, owners, homebuyers, and nonprofit housing providers.

In addition to providing public housing, LHAND makes affordable housing available through several rental assistance programs, such as the federal Section 8 voucher program and the state-funded Massachusetts Rental Voucher Program. At the time of our audit, LHAND administered 2,590 rental assistance vouchers through its rental assistance program. LHAND is composed of 855 public housing units, of which 402 are state-owned housing and 453 are federal housing. LHAND's state-funded units consist of family and elderly/disabled housing and housing for special needs. LHAND also administers a program of certificates and vouchers to assist low-income persons and families in leasing apartments in privately owned housing. Of the 2,590 rental assistance vouchers, 2,210 represent the voucher allocation to LHAND, and the remaining 380 are administered by LHAND for other housing authorities. LHAND also administers 1,616 Section 8 vouchers and 311 Massachusetts rental vouchers. LHAND 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).

LHAND is composed of seven departments: administration, fiscal, maintenance, leased housing/rental assistance, planning and neighborhood development, resident support services, and information technology (IT). LHAND's central office, which is located at 10 Church Street in Lynn, manages three other LHAND sites throughout the city. At the time of our audit, LHAND was staffed by 76 full-time and part-time employees, including a full-time Management Information System Coordinator who provides IT support.

LHAND's computer operations are supported by two file servers and 76 computer workstations located at LHAND's central office and development sites. LHAND uses the two file servers to provide both a local area network (LAN) and a wide area network. LHAND's primary application system is a vendor-supplied, integrated application known as the Visual HOMES/AccountMate system. The Visual HOMES/AccountMate application provides data-processing functions using a module-based system for the following:

- Public housing, portability, Section 8 housing, and general work orders
- Mail merges for tenant, vendor, landlord, and tenant application activities
- Cash receipts and disbursements, payroll, accounts payable, and general ledger
- Fixed asset – hardware items, furniture and equipment assets

The Visual HOMES portion of the software package provides processing support for all housing operations, whereas AccountMate supports the financial applications.

LHAND's secondary application system was supplied by Tracker Systems, Inc., of Marlborough, Massachusetts. The integrated application system, known as Tracker, provides data processing functions for the DHCD Housing Voucher Program. The Tracker application also contains a general ledger function that LHAND does not use, since the general ledger function is performed within AccountMate. In addition, LHAND utilizes Microsoft Office applications for its fixed-asset inventory, rental information, and tenant applications on a supplemental basis. LHAND uses Symantec anti-virus software for scanning the LAN and all individual workstations.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of selected IT-related controls at LHAND for the period January 1, 2007 through December 31, 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with generally accepted industry practices. Audit criteria used included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007, and the Office of the State Comptroller's "Internal Control Guide for Departments" promulgated under Chapter 647 of the Acts of 1989. Further audit criteria included the Office of the State Comptroller's regulations on fixed-asset accounting and Operational Services Division guidelines regarding the disposition of fixed assets.

The scope of our audit included an examination of documented IT policies and procedures, physical security and environmental protection of IT resources at LHAND's offices in Lynn, system access security for LHAND's automated systems, inventory control for computer equipment and software, disaster recovery and business continuity planning, on-site and off-site storage of backup copies of magnetic media, and control practices regarding the protection of personal information. Our audit scope also included a follow-up examination of corrective actions taken by LHAND to address the audit results and recommendations contained in our prior audit report (No. 2005-0699-4T), dated September 8, 2006.

Our primary audit objective was to determine whether LHAND's IT-related internal control environment and documented IT policies and procedures provided reasonable assurance that control objectives would be achieved to support LHAND's business functions; adequate controls were in place to provide reasonable assurance that IT resources are safeguarded, properly accounted for, and available when required; adequate physical security controls were in place to restrict access to IT resources to only authorized; sufficient environmental protection controls were in place; adequate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources, including the Visual HOMES/AccountMate application system and other business-related applications; and procedures were in place to prevent and detect unauthorized access to automated systems.

Regarding system availability, we determined whether adequate disaster recovery and business continuity planning controls were in place to restore IT systems in a timely manner for mission-critical and essential business operations should LHAND's automated systems be unavailable for an extended period. In addition, we determined whether adequate controls were in place regarding on-

site and off-site storage of backup copies of magnetic media for application systems and data files. A further objective was to review LHAND's policies and procedures associated with the protection of personal information. With respect to our follow-up examination of the prior audit results and recommendations, we determined the extent and nature of corrective actions taken by LHAND to address these issues.

Our audit noted certain deficiencies in LHAND's IT-related internal control environment, documented policies and procedures, and management control practices for the protection of personal information. Specifically, our audit determined that although LHAND had taken steps to address the prior audit issues of disaster recovery and business continuity planning, system access security, and inventory controls over fixed assets, further improvements were necessary.

AUDIT RESULTS

STATUS OF PRIOR AUDIT RESULTS

Our prior audit (No. 2005-0699-4T) of the Lynn Housing Authority and Neighborhood Development (LHAND) revealed deficiencies in the areas of (a) disaster recovery and business continuity planning, (b) system access security, and (c) inventory controls over fixed assets. Our follow-up review revealed that although LHAND had taken steps to address these issues, improvements were still necessary, as discussed below.

a. Disaster Recovery and Business Continuity Planning

Our prior audit report disclosed that LHAND had not developed an approved, comprehensive, and tested disaster recovery and business continuity and contingency plan for restoring processing functions in the event that automated systems were rendered inoperable or inaccessible. Our follow-up review noted that LHAND had taken steps to address this issue. Specifically, LHAND had implemented on-site and off-site storage of backup copies of magnetic media for data files residing on LHAND's file servers and workstations and had established informal procedures for on-site and off-site storage of backup copies of magnetic media for systems under its charge. Moreover, the main application (Visual HOMES/AccountMate) and the secondary application (Tracker) are backed up daily to network-attached storage (NAS) external hard drives located on-site in LHAND's file server rooms. Further, all Visual HOMES/AccountMate data is encrypted and electronically transmitted to servers located at the LHAND vendor's location in Silver Springs, Maryland. In addition, LHAND had adequate physical security and environmental controls over the backup media at the on-site and off-site storage locations in the file server rooms in Lynn.

However, our follow-up review disclosed that improvements were still needed. Specifically, LHAND still had not developed a written disaster recovery and business continuity plan containing detailed emergency/evacuation plans, a list of mission-critical and essential automated systems, information related to restoration of IT services, emergency declaration, and a contact list to provide sufficient recovery strategies and resources to restore IT systems and business operations in a timely manner should IT systems be rendered unavailable for an extended period. Also, LHAND had not designated an alternate processing site for backup recovery of IT capabilities. Depending on the nature and extent of a loss of IT systems or processing, LHAND could experience difficulties in

regaining mission-critical and essential business processes within an acceptable period of time given the absence of a sufficiently comprehensive recovery and business continuity plan specific to LHAND.

Our audit found that LHAND had not:

- Performed a criticality assessment and risk analysis of the infrastructure of IT and business operations;
- Designated an alternate processing site where computer systems can be restored;
- Documented all potential disaster scenarios and instructions to follow for each specific event;
- Developed detailed procedures for relocating to an alternate operational site to ensure availability of required personnel and other resources;
- Developed a contact list, including IT personnel, to be notified in the event of an emergency and include all communication information, such as landline telephone and cell phone numbers and e-mail addresses;
- Developed departmental unit or user area plans that document the procedures to follow for each business unit to restore or continue business activities should automated systems be inoperable or unavailable for an extended time;
- Documented detailed procedures regarding restoration of network services; and
- Developed procedures for testing the disaster recovery and business continuity plan, and documenting tests performed and any corrective actions taken.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption or loss of computer or network 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 recovery and contingency plans, if required.

Disaster recovery and business continuity 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 recovery and 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.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different disaster scenarios. Appropriate user area plans should outline recovery or contingency steps with detailed procedures to be followed to efficiently restore business operations. The area plans should be coordinated with overall enterprise-based disaster recovery and business continuity plans.

Recommendation

LHAND should take steps to ensure that adequate disaster recovery and business continuity plans are in place and tested to provide adequate assurance of their viability. LHAND should:

- Review the list of disaster scenarios regarding the loss of IT systems that would impact LHAND operations and business functions, and develop and update recovery and business continuity strategies for each of the disaster scenarios identified.

- Designate an alternate processing site to support the recovery of automated systems and develop and verify through testing a documented disaster recovery plan.

- Perform on an annual basis or upon major changes to the operational or IT environment an enterprise-based risk analysis and criticality assessment of IT systems and related capabilities. The risk analysis and criticality assessment should include external partners upon which technical dependencies exist.

- Implement procedures to attain from all parties for which there are significant dependencies an adequate level of assurance of the viability of disaster recovery and business continuity plans to support mission-critical and essential business functions.

- Establish a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, LHAND should establish targets for acceptable time periods by which mission-critical IT operations need to be recovered.

- Develop and perform appropriate levels of testing to provide LHAND with sufficient assurance as to the viability of recovery and business continuity plans. Tests should be performed on control practices that can be reviewed and evaluated independently of the test of recovery strategies in conjunction with the implementation of the alternate processing site. Once tests are completed, test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.

- Review business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. Subsequent to testing the business continuity plan, LHAND should update the plan when needed to provide reasonable assurance that it is current and viable. The completed plan should be distributed to management and staff responsible to direct and perform recovery procedures.

- Ensure that management and staff are adequately trained to effectively execute disaster recovery and business continuity tasks and activities.

Auditee's Response

LHAND has now developed a written plan for disaster recovery and business continuity. This plan includes a list of mission-critical and essential automated systems, information related to restoration of IT services and a contact list to provide sufficient recovery strategies and resources to restore IT systems and business operations in a timely manner in the case of IT systems being rendered unavailable for an extended period.

The plan also includes designation of alternative sites where computer systems can be restored, a hierarchy of IT personnel to be notified in the event of an emergency and procedures regarding restoration of network services. A separate plan containing detailed emergency evacuation plans for each site has also been developed.

LHAND staff will continue work to refine these plans to provide more detailed steps that staff will take in the case of such an emergency. LHAND staff will also develop an annual risk analysis and criticality assessment, which will incorporate the expertise of external partners who LHAND depends on for technical support. LHAND will review business continuity requirements periodically, make changes as required and insure that management and staff are adequately trained to effectively execute disaster recovery and business continuity tasks and activities.

b. System Access Security

Our prior audit report disclosed that system access security controls over LHAND's network needed to be strengthened to ensure that only authorized users would have access to the system. For example, we found that although LHAND management had limited system access security policies in place, there were no written policies or procedures requiring users to change their passwords on a regular basis or control procedures requiring a specific number or type of characters in their passwords. In addition, the prior report noted that LHAND had limited written policies and procedures in place to address authorization and activation of system users. We also found that LHAND's authorized system user listings were not kept up-to-date. Specifically, there were no written IT policies and procedures in place to notify LHAND's IT staff when an individual terminated employment at LHAND, and no written notification was given from LHAND's Administrative Department to the IT Section concerning changes in employee status (e.g., terminations, leaves of absences, transfers). The prior audit determined that for both the primary

software application then in use (CHAS) and e-mail access, 18 former LHAND employees still had system access privileges.

Our follow-up review disclosed that, although LHAND's authorized system user listings contained only current employees, LHAND still lacked appropriate formal system access security policies and procedures for password administration, including formation, use, and frequency of change. In addition, LHAND did not monitor employee compliance with its limited informal password administration and system user lockout policies. Specifically, LHAND employees were not locked out after five unsuccessful system login attempts, contrary to LHAND's draft IT policies and procedures document. Overall, we found that LHAND's informal password policies and procedures in place were inadequate and that LHAND did not monitor employee compliance with them. Password weaknesses found included the following:

- LHAND did not require passwords to consist of at least eight alphanumeric characters;
- LHAND did not require passwords to contain at least three of these items: symbols, numbers, upper-case letters, and lower-case letters; and
- LHAND employees were using formal names or dictionary words in passwords, which can be more easily guessed.

In addition, our audit found that, although LHAND's written policy required that passwords be changed every 12 months, LHAND did not monitor employee compliance with this weak policy. Our audit testing revealed that four of six employees with access to the Visual HOMES/AccountMate and Tracker application systems had not changed their passwords in over 12 months. As a result of its inadequate password administration policies, procedures, and control practices, LHAND cannot ensure that mission-critical systems and confidential data are safeguarded from access by unauthorized persons.

Control Objectives for Business Information and Related Technology (CobiT) guidelines, as well as prudent business practices, require that entities develop adequate formal policies and procedures regarding password administration, train staff in their use, and monitor them to ensure compliance with these policies and procedures. During the audit, LHAND senior management acknowledged that they needed to develop stronger formal password administration policies, procedures, and practices and monitor compliance with them.

Recommendation

LHAND should develop appropriate formal policies and procedures for password administration, including formation, use, and frequency of change. Password policies should include the following requirements:

- All passwords should consist of at least eight alphanumeric characters;
- All passwords should contain at least three of the following four items: symbols, numbers, upper case letters, and lower case letters;
- No formal names or dictionary words should be allowed; and
- Passwords should be changed at least every 90 days.

In addition, LHAND should train all employees regarding the new formal password administration policies and procedures and monitor employee compliance with them.

Auditee's Response

LHAND has now developed formal written procedures for password administration. These password policies include the following requirements:

- *Passwords must be at least eight characters in length.*
- *Passwords cannot contain three or more consecutive letters from the employee's logon account name.*
- *Passwords must contain at least two uppercase, two lowercase, and two numeric values.*
- *Passwords will be changed every 90 days.*
- *Passwords will be locked out after three failed attempts. An employee will be able to try to login again after five minutes from the third failed attempt.*

All LHAND employees will be trained regarding these policies and monitored for their compliance with them.

c. Inventory Controls over Fixed Assets

Our prior audit report noted that LHAND needed to improve its inventory controls over IT resources. Specifically, the prior audit determined that LHAND's IT and Procurement sections were maintaining separate inventory records, each of which listed different information regarding computer equipment items and neither of which was complete or reconcilable to the other. In

addition, the prior audit report noted that written and approved policies and procedures for inventory control were not in place for LHAND's IT resources, the IT inventory listing did not include all relevant data fields (e.g., acquisition date, cost), and three of 56 hardware inventory items recorded on the perpetual inventory could not be located.

Our follow-up review indicated that LHAND had taken steps to address this issue by implementing certain recommendations in the prior audit report, including updating and consolidating its computer equipment inventory records and recording all required asset information. In addition, the consolidated inventory system of record for all computer equipment items on hand was complete and accurate as of September 28, 2010, and the listing contained all information required by the Office of the State Comptroller OSC guidelines for inventory control, including asset historical costs and dates of acquisition. Further, the sample audit testing of 112, or 49%, of the 227 items listed on the hardware system of record revealed that all 112 computer equipment items were locatable. Also, LHAND maintained a current and complete list of licensed software, and software licenses were kept on file at LHAND office locations.

However, our follow-up review also found that LHAND's documented control procedures and practices could be strengthened to provide reasonable assurance that LHAND properly monitors its computer equipment. Specifically, although LHAND management claimed that it had taken an annual physical inventory of computer equipment, it did not maintain evidence of conducting such a physical inventory or reconciling it to LHAND's asset records. Also, LHAND was not requiring employees to sign control sheets for assigned notebook computers to acknowledge user responsibilities for security and acceptable usage.

Recommendation

LHAND should enhance its documented control procedures and practices by ensuring that it maintains evidence of an annual physical inventory and reconciliation of asset records. With respect to notebook computers, LHAND should develop a formal policy requiring that users who are assigned notebook computers sign a responsibility and acceptable usage form. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment.

Auditee's Response

LHAND has now developed enhanced documented control procedures for inventory, which include evidence of an annual physical inventory and a reconciliation of asset records. LHAND also has begun using a responsibility and acceptable usage form for the use of notebook computers, which are signed by the users.