A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

Boston, MASSACHUSETTS 02108

TEL. (617) 727-6200

No. 2005-0699-4T

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

April 1, 2004 through May 18, 2006

OFFICIAL AUDIT REPORT

SEPTEMBER 8, 2006

TABLE OF CONTENTS

INTRODUCTION

The Lynn Housing Authority (LHA), which was established through Section 3 of Chapter 121B of the Massachusetts General Laws, provides for the construction, acquisition, rehabilitation and management of rental housing for low-income persons residing in Lynn, Massachusetts. The LHA is governed by a five-member Board of Directors, one of whom is appointed by the Governor and four who are appointed by the Mayor of the City of Lynn. One of the board members, who is appointed by the mayor, is a tenant representative.

The LHA is comprised of seven departments: administration, fiscal, maintenance, leased housing/rental assistance, planning and neighborhood development, resident support services, and information technology. The LHA's central office, which is located at 10 Church Street in Lynn, manages three other LHA sites throughout the city. At the time of our audit, the Authority was staffed by 74 employees, one of whom provided the role of information technology (IT) support.

The LHA 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). In addition to providing public housing, the LHA makes affordable housing available through several rental assistance programs, such as the Federal Section 8 voucher program and the Massachusetts rental voucher program. Furthermore, through its assistance program, the LHA administers 1,525 rental assistance voucher units. The LHA is comprised of 3,393 public housing units, of which 714 are state-owned housing and 2,679 are federal housing. The LHA state-funded units consist of family and elderly/disabled housing, housing for special needs, and the Massachusetts rental voucher program. Included in these totals are the LHA administration of programs for certificates and vouchers to assist low-income persons and families in leasing apartments in privately owned housing. The LHA administers 1,216 Section 8 vouchers and 309 Massachusetts rental vouchers.

According to the Authority's financial report for the period ending March 31, 2004, the LHA received revenue of $20,807,809 for federal programs and $8,196,193 for state programs. Expenditures for this period for federal programs totaled $22,065,483 and $8,159,293 for state programs.

At the time of our audit, the LHA's computer operations were supported by two file servers and 61 microcomputer workstations located at the LHA central office as well as the development sites. Of the 61 workstations, 56 were desktop computers and five were notebook computers. The two file servers provide network support for a local area network (LAN) and a wide area network (WAN).

The LHA'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;

(d) Fixed Asset –Hardware Items, Furniture and Equipment assets.

In addition, the LHA utilizes Windows-based applications for its fixed-asset inventory, rental information, and tenant applications.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From April 21, 2005 through July 28, 2005, and from May 15, 2006 through May 22, 2006, we performed an audit of selected information technology (IT) related controls at the Lynn Housing Authority (LHA) for the period covering April 1, 2004 through May 18, 2006. The scope of our audit included an evaluation of IT-related controls pertaining to physical security, environmental protection, user account and password administration, inventory control over IT resources, 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 adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the LHA's IT-related internal control framework, including policies, procedures, and practices, provided reasonable assurance that IT-related control objectives would be achieved to support business functions.

We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access into the LHA's automated systems. Furthermore, we sought to determine whether LHA management was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related assets were properly recorded and accounted for. We also determined whether the LHA had an effective disaster recovery and business continuity planning that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. In addition, we sought to determine whether the LHA had adequate procedures for on-site and off-site storage of backup media to support system and data recovery objectives.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior personnel. To obtain an understanding of the internal control environment, we reviewed the LHA's organizational structure and primary business functions. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities.

As part of pre-audit work, we reviewed the prior audit report for Lynn Housing Authority (2003-0699-3A) and supporting audit work papers. We also reviewed records regarding the recording and review of financial activity, the disclosure status of related party activity, and budget control and expenditure classification for the 400-1 state program. We interviewed senior management, obtained pertinent data and examined LHA records. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our assessment of IT-related internal controls, we interviewed senior management, obtained, reviewed, and analyzed existing IT-related policies, standards, procedures, and LHA's organizational structure. To evaluate physical security, we interviewed management and security personnel, conducted walk-throughs, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas containing IT equipment. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access areas containing computer equipment were current employees of the LHA and that these areas were restricted to only authorized personnel.

To determine the adequacy of environmental controls, we conducted walk-throughs and evaluated controls in selected areas to assess whether IT services were placed in environmentally controlled areas and were subject to adequate environmental protection. 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, observation, and review of relevant documentation.

Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the authority's local area network. To determine whether only authorized employees were accessing the automated systems, we obtained a system-generated user list from LHA for individuals granted access privileges to the automated systems and compared it to the current personnel listing. We performed a test of access privileges for all employees to assess their current employment status for both CHAS and E-Mail accounts. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to the LHA personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

We reviewed inventory control procedures for computer equipment by determining whether adequate controls were in place and in effect to properly account for IT resources. We examined DHCD policies and procedures regarding fixed-asset inventory to determine whether the LHA was in compliance. We conducted a data integrity test of the inventory of computer equipment by examining and comparing

information obtained from 52% of the Authority's inventory list of 61 microcomputer workstations to data listed on each item on the inventory system of record. The data fields examined were identification tag number, location, description, and historical cost. In addition, we judgmentally selected 12 microcomputer workstations installed at the Authority and determined whether each item was correctly recorded on the inventory system of record. We also determined whether appropriate data fields were included in the inventory record to support inventory control and IT configuration management. We did not review the purchase or receipts of IT equipment since none had been acquired during the audit period.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the Authority's primary application system be rendered inoperable or should IT resources be inaccessible for an extended period of time. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Further, to evaluate the adequacy of controls to protect data files through the generation and on-site and off-site storage of backup copies of magnetic media and hardcopy files, we interviewed LHA staff regarding the creation and storage of backup copies of computer-related media and reviewed on-site and off-site storage areas.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted IT 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, in July of 2000.

AUDIT CONCLUSION

Based on our audit of the Lynn Housing Authority (LHA), we found that internal controls were in place and in effect to provide reasonable assurance that IT-related control objectives would be met with respect to physical security and environmental protection over IT resources. Regarding physical security, and environmental protection, we found that controls were being exercised over the file server room and in the surrounding offices where computer equipment was located. However, controls needed to be strengthened regarding disaster recovery and business continuity planning, the IT inventory, and systems access security.

Our review of the LHA's internal control structure indicated that senior management was aware of the need for internal controls. We determined that there was an appropriate reporting structure for the IT function, an established chain of command, clear assignment of IT responsibilities, and a documented job description for the Authority's IT employee.

We found that LHA had implemented adequate physical security controls to provide reasonable assurance that only authorized persons could access the file server room and other areas containing IT-related equipment. In addition to the controls noted above, our audit confirmed that other important physical security controls were in place at the Authority's three development sites. We found that access to the individual business offices at the various sites was restricted to LHA personnel.

Our audit indicated that adequate environmental protection, such as temperature controls, smoke detectors, fire alarms, hand-held fire extinguishers, and an uninterruptible power supply (UPS) to prevent loss of data should power suddenly fail, were in place in the central office to prevent damage to, or loss of IT-related resources. However, we recommend the LHA management consider posting emergency shut down and evacuation procedures in the file server room and evacuation procedures for the development sites. We found that good housekeeping procedures were in place within the file server room which was neat, clean, and in good order.

With respect to the appropriate use of information technology, we determined that the LHA had not promulgated adequate written policies and procedures regarding e-mail and Internet use. In addition, LHA needed to improve documented controls by developing more specific control policies, practices, and operating procedures regarding physical security and environmental protection, inventory control of computer equipment and software, logical access security, business continuity and contingency planning, disaster recovery strategy, and off-site storage of backup copies of electronic media.

Regarding the availability of automated systems, we found that the LHA had not documented a disaster recovery strategy nor established a business continuity plan. We note that the Authority's IT Section had begun the process of developing a disaster recovery strategy, however, by the end of our

audit, the strategy had not been fully documented. Once the Authority has developed their disaster recovery strategy, we recommend that the business continuity plan be tested to assess its viability. We further recommend that Authority establish a process for routinely updating the plan to take into account changes to technology, business processes, or staffing.

The LHA should ensure that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained. Furthermore, the plan should detail the assigned tasks and responsibilities to be completed and by whom. Given the absence of a comprehensive recovery plan and the Authority's dependence on the CHAS application system to perform mission-critical business functions, a significant disaster impacting the LHA's automated systems for an extended period, specifically the file server on which the CHAS application database resides, could adversely impact the Authority's ability to regain critical IT operations, such as processing tenant applications and accounting for rent money and work orders.

We found that although on-site storage of backup media was being provided for the LHA's application systems and related data files, the policies and procedures for off-site storage of backup media needed to be documented. We note that the LHA was securing computer-related media off-site at another LHA location.

With respect to IT-related inventory control, our test of a sample of the LHA's inventory listing of 298 IT resources confirmed that the majority of items tested were locatable, properly accounted for, and tagged. Our audit test indicated that the LHA IT equipment was properly tagged, and that equipment on hand was identified and properly recorded on the IT Section's inventory record for 29 of the 32 pieces of equipment judgmentally selected. However, we believe that the inventory record of IT resources could be enhanced by ensuring that all equipment is tagged and recorded, acquisition dates and historical cost figures are included for all IT equipment, and that an annual physical reconciliation of the equipment and the system of record is performed. At the time of the audit, the Authority was in the process of implementing a new IT inventory control system.

Although certain inventory controls were centrally handled by the IT Section, we found that the auditee needed to strengthen its controls to provide reasonable assurance that IT resources would be properly recorded and accounted for. At the time of our audit, both the IT Section and the Procurement Section were maintaining independent inventories, and although there was some commonality between the two inventories, each inventory record was being maintained for a separate purpose. The IT Section's inventory was to record the location of all computer assets and the Procurement Section's inventory was to maintain a listing of all purchased assets over $500. We found that neither inventory was complete nor contained a common field to identify individual assets and reconcile the two inventory records.

With respect to system access security, our audit disclosed that the processes for granting, recording authorization, and activating logon IDs and passwords were appropriate. However, control practices regarding access security policies and procedures and periodic changes of passwords needed to be improved. Our audit indicated that there is an eight character minimum requirement for password composition and that passwords were being changed annually. We recommend that LHA require password changes to be made more frequently than once a year and implement appropriate assurance mechanisms to ensure that passwords meet a minimum of eight alpha/numeric characters. Regarding access to the CHAS application system and email, we determined, however, that eighteen former LHA employees still had systems access privileges. We note that the Authority took immediate corrective action and deactivated the user accounts for these prior employees upon being made aware of this security condition.

AUDIT RESULTS

1. Disaster Recovery And Business Continuity Planning

We determined that the LHA had not developed a formal, comprehensive disaster recovery and business continuity and contingency plan for restoring processing functions in the event that automated systems were rendered inoperable or inaccessible. The LHA was aware of the need for business continuity and contingency planning; however, a business continuity and contingency plan had not been approved or implemented as of the end of our audit fieldwork.

A business continuity plan should document the LHA's disaster recovery strategy with respect to various disaster scenarios. Without a comprehensive formal and tested recovery strategy for the LHA's various application systems, the LHA might experience delays in re-establishing the processing of mission-critical functions such as tenant files and accounts receivable should a disaster occur. The lack of a detailed and tested plan to address the resumption of processing of the LAN and microcomputer systems might render data files and software vulnerable should a disaster occur. If the LAN were damaged or destroyed, the LHA could lose mission-critical, essential, and confidential data, including tenant medical and financial information.

The objective of business continuity and contingency planning is to help ensure timely recovery of mission-critical functions should a disaster cause a significant disruption to computer operations. Business continuity and contingency planning for information services is part of business continuity and contingency planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for the LHA to have an ongoing business continuity and contingency planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. The LHA should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

We found both on-site and off-site backup media to be adequately controlled. Our review of LHA physical security and environmental protection for the off-site location determined that the off-site backup media location was reasonably secured, although the addition of a fireproof safe could only enhance security. However, the LHA should conduct a risk analysis of these locations annually to determine if conditions could be improved.

At the close of the audit, we reviewed with the Lynn Housing Authority's administrative staff, the current status of their controls over disaster recovery and business continuity planning. The Authority

has installed an off-site 80 gigabyte SmartDisk hard drive with an Ethernet connection to the LAN with which they perform off site back up of their file server.

Recommendation:

We recommend that LHA management establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for all system applications. We recommend that senior management and key users review the information technology environment and perform a criticality assessment and risk analysis of all automated systems used by LHA. Based on the results of the assessment, LHA should proceed with the development of a documented business continuity plan for their mission-critical and essential functions.

Once the plan has been developed, it should be tested, then periodically reviewed and updated for any changing conditions. The LHA should specify the assigned responsibilities for maintaining the plan and for supervising the implementation of the tasks documented in the plan. Management should specify who should be trained in the implementation and execution of the plans under all emergency conditions and who will perform each required task to fully implement the plans. Further, copies of the completed business continuity and user area plans should be distributed to all appropriate staff members. A copy of the plan should also be kept in a secure off-site location.

Regarding the off-site storage of computer media backup, we commend the LHA management for utilizing the SmartDisk hard drive in addition to having one of the development sites to serve as an off-site location and suggest placing tapes in a fireproof safe for increased security.

Auditee Response:

The LHA is in the process of developing a written Disaster Recovery and Business Continuity Plan based upon the outline given to us by the State Auditor's Office. This plan will setup a framework for a Disaster Recovery team within the LHA. The Disaster Recovery team will be responsible for assessing critical applications and devising a documented plan for essential functions.

The LHA is critically dependent upon continued availability of information stored within the CHAS system. The LHA uses backup tapes and networked hard drives for daily historical backups.

At present the LHA has installed Fireboxes at both the Church sty. and S. Common locations for storage of daily backups. The LHA also has added an additional Smart Disk, giving the LHA a total of four (4) locations storing backup files.

Auditor's Reply:

The steps undertaken by LHA in multiple sites to store daily backup tapes is a good effort at protecting electronic data and the availability of IT systems. Having a business continuity plan that incorporates the multiple sites, responsibilities and assigned tasks for the staff in the event that access and use of backup copies of electronic media are required, and required testing and training drills, not unlike fire drills, will help ensure a successful recovery effort of IT systems.

2. Hardware Inventory Control

We found that inventory control over IT resources needed to be improved. We noted that inventory controls over IT-related resources needed improvement especially in the areas relating to hardware inventory items. Although the Authority's IT Section was responsible for maintaining, recording, and monitoring an inventory of IT-related assets, responsibility for inventory control was shared with the Procurement Section. We determined that the LHA's IT Section and Procurement Section maintained separate inventory records each of which listed different information regarding the IT resources. We found, however, that neither listing was complete or reconcilable to the other. This was due, in part, because there was no unique identifier for each IT resource in both inventory records and that the Procurement Section's inventory was maintained within the CHAS system, while the IT Section's inventory was maintained in a spreadsheet.

Overall, the following inventory control weaknesses were noted for computer equipment:

a) The LHA had not maintained formalized written policies and procedures over its IT related resources, which would include establishment of a perpetual inventory listing compliant with the Office of State Comptroller's guidelines for inventory item maintenance and a centralized reporting system of inventory items. We determined that written and approved policies and procedures for inventory control were not in place for the Authority's IT Section.

b) The IT Section's IT inventory, as of June 2005, did not include all relevant data fields, such as pertinent information regarding acquisition and installation dates that could be incorporated into a perpetual inventory system of record. In addition, data was not recorded for the inventory's hardware cost field.

c) The IT Section could not locate three of 56 hardware inventory items recorded on its perpetual inventory listing of June 2005.

We confirmed that the LHA's IT Section had conducted an annual inventory and had updated the inventory into a perpetual inventory of IT hardware and software inventory items as of June 2005. However, we determined that the IT Section had not maintained formal policies and procedures regarding inventory control over IT resources. Moreover, the Authority did not maintain a centralized system of

record for inventory and reporting system of hardware inventory items compliant with Office of State Comptroller's "Fixed Assets Subsystem Policy Manual and User Guide".

By updating and completing all data fields in the perpetual inventory listing, the IT Section would be able to generate a complete inventory listing of computer equipment at any point in time. The complete perpetual inventory listing could then serve as an internal control to assist the LHA in verifying the existence of all hardware inventory items. By having the LHA's IT Section conduct an inventory reconciliation with the Authority's Procurement Section on at least an annual basis, the Authority would be reasonably assured that its perpetual inventory listing would be up to date and would be comprised of all hardware items.

Although the IT Section's one employee was able to perform a physical inventory as of June 2005, historical procurement data was not obtained to complete the inventory records for the IT resources. Until such time that a single inventory system of record for all assets, including IT resources, is maintained by the Authority, the IT Section should request from the Procurement Section information regarding purchases and/or leases of IT resources to update the IT Section's IT inventory record.

At the close of the audit, we reviewed the status of the controls over hardware inventory with the Authority's administrative staff. At that time. we were informed that there were discussions underway between the Procurement Officer and the IT Section to consolidate the two inventories.

Recommendation:

The LHA should implement the following recommendations pertaining to hardware inventory control:

1. The IT Section should include in the perpetual inventory listing all pertinent data fields, such as the cost of hardware and date of acquisition and installation.
2. The IT Section should follow up on all hardware inventory items that cannot be verified as being on-site and initiate measures to locate the hardware items.
3. The LHA should initiate an inventory reconciliation process between the Procurement Section and the IT Section on at least an annual basis. The reconciliation process would consist of a comparison of all current fiscal year hardware inventory items maintained by the Procurement Section with the perpetual inventory listing maintained by the IT Section for the same fiscal year. Any variances should be documented and resolved, and the IT Section perpetual inventory listing should be adjusted as required.

Auditee Response:

The IT Section of the LHA now includes cost of hardware and date of acquisition to ensure from this point forward a maintained perpetual inventory listing with the IT department.
Annually the IT department does reconciliation with Procurement for items over $500 value at time of purchase. The LHA is in the process of revising this process.

Auditor's Reply:

The LHA will gain a better inventory control over IT resources by including cost of hardware and date of acquisition on their perpetual inventory system of record, reconciling hardware inventories maintained by the Procurement Section and the IT Section, and ensuring that appropriate filings are made should IT resources be lost or stolen.

3. System Access Security

Our audit revealed that system access security controls over the LHA's local area network needed to be strengthened to ensure that only authorized users have access to the system. We found that although LHA management had limited access security policies in place, there were no written policies or procedures requiring users to change their passwords on a regular basis nor procedures requiring a limited number of characters in their passwords. Our audit found that the MIS Coordinator distributes passwords annually to staff, and in seven instances users were using five-letter passwords rather than the industry minimum of eight-letter passwords. Also, we were able to determine the length of the passwords used by employees because the MIS Coordinator maintains a copy of the passwords he distributes. Although the system, according to the MIS Coordinator, does not allow users to pick their own passwords, the current procedure of having the Coordinator know all the passwords is risky and could lead to unauthorized access to the system.

We also found that the LHA had limited written policies and procedures in place to address authorization and activation of system users. There were no written IT policies and procedures in place to notify LHA's IT staff when an individual terminated employment at the LHA, and no written notification was being given from the LHA's Administrative Department to the IT Section concerning changes in employee status (e.g., terminations, leaves of absences, or transfers). Our audit tests revealed that for both the CHAS software application and the e-mail application all current LHA employees were authorized systems access users. However, we determined that for both the CHAS software application and for e-mail access, 18 former LHA employees still had system access privileges. We therefore determined that adequate procedures were not in place for administering and monitoring system access security controls. We note that access privileges for these former employees were deactivated by the Authority's IT Section when they were made aware of this condition.

The failure to change passwords for user accounts, or deactivate access privileges when no longer required in a timely manner, places the LHA at risk of unauthorized access or use of established privileges (using another individual's user account or using an account having higher access privileges). Formal policies and procedures for system access security should be in place to address password administration, activation and deactivation of access privileges, and monitoring of user access. The failure to develop comprehensive formal system access security policies and procedures and implement

adequate control practices places LHA's automated systems and data at risk of unauthorized access, modification, or loss.

The Commonwealth of Massachusetts' "Internal Control Guide for Departments" promulgated by the Office of the State Comptroller states, in part, "an employee's password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility." In addition, computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access. The policies and procedures should also address emergency access guidelines for critical applications to ensure that under emergency or disaster recovery situations, only authorized access is granted.

On May 18, 2006, we reviewed the status of the LHA's controls over system access security with the Authority's administrative staff. At that time, the Authority was planning to upgrade their CHAS software to improve access security.

Recommendation:

LHA should enhance written policies and procedures to address password administration, including the length and composition of passwords (a minimum of eight alpha/numeric characters), frequency of password changes, guidelines for access security, establishment of audit trails, and procedures to be followed in event of unauthorized access attempts or unauthorized access. The Authority should develop an overall security framework restricting user access to automated systems and IT resources on a need to know and need to perform basis. In addition, the Authority should develop policies and procedures to address authorized changes to user access profiles. We also recommend that procedures be established requiring written notification from the LHA's Administration Department to the LHA's IT Section of changes in personnel status of the LHA staff to help ensure timely modification or deactivation of access privileges. According to Management Computer Support, which is the vendor that supports CHAS, the next version of the software called PHA-Web has advanced security provisions over CHAS. As such, the LHA should perform a risk assessment of the PHA-Web to determine if the enhanced security features would solve their security needs.

Auditee Response:

The LHA is developing a written policy to address the recommendations outlined within the IT audit. Any changes to the LHA personnel policy regarding IT access must first be approved by the LHA Board of Commissioners.

Auditor's Reply:

We acknowledge that the Authority is enhancing their policies and procedures regarding access security to automated systems and IT resources. We would urge the Authority to implement appropriate policies and practices as soon as possible.