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. 2009-0141-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS HOUSING FINANCE AGENCY

July 1, 2007 through May 20, 2009

OFFICIAL AUDIT REPORT

JUNE 29, 2009

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Housing Finance Agency (MHFA) was established by Chapter 708 of the Acts of 1966 and amended by Chapter 23A of the Massachusetts General Laws. In 1978, the Massachusetts Home Mortgage Finance Agency was created to assist low and moderate-income homebuyers. The two agencies merged in 1982 and began doing business as MassHousing in 2001. MassHousing operates as a quasi-government entity and is governed by a nine-member Board of Directors of which the Governor appoints seven members with two serving as ex-officio members including the Director of Housing and Community Development or his/her designated representative and the Secretary of Administration and Finance or his/her designated representative. Each member of the Board serves for a seven-year term.

MassHousing's mission is to promote and provide financing for the development and preservation of quality multifamily rental housing and to create opportunities for affordable home ownership to people of varied economic means. MassHousing has three major lines of business: rental development, rental management, and home ownership. These business divisions support the creation and preservation of affordable rental and for-sale housing throughout Massachusetts.

MassHousing sells federally-authorized, tax-exempt and taxable bonds to individual and corporate investors. The sale of these bonds raises private capital for mortgages that MassHousing loans to eligible borrowers. MassHousing loans the funds at rates below those of conventional lenders to make home financing more affordable to low and moderate-income households. Investors in MassHousing bonds receive a return on their investment that is supported by the monthly mortgage payments made by the borrowers.

MassHousing’s rental housing programs have created 92,000 affordable rental units in more than 750 developments throughout the Commonwealth since its inception in 1969. Over the same period, MassHousing promoted the provision of social service programs to the MassHousing client population. Since its inception in 1969, MassHousing has provided more than $5.7 billion for rental development and more than $5.3 billion in mortgage funds for home ownership.

MassHousing's computer operations support the Agency’s administrative functions through a single data center. MassHousing’s IT infrastructure consists of 30 application systems and a local area network operating on 70 file servers to which 519 workstations and other peripherals are connected. Furthermore, the Agency, which is staffed by 350 employees, uses 56 laptop computers to provide additional IT capabilities. The mission-critical applications consist of the CODA application which supports MassHousing’s general ledger; the Benedict application which tracks multifamily loan servicing;

the RealServicing application which tracks single family homeowner loan servicing; and the PAM (Portfolio Asset Management) application which tracks the MassHousing investment portfolio and the bond debt portfolio.   These applications operate on MassHousing’s local area network (LAN).

The Office of the State Auditor's internal control examination was limited to certain operational and general controls over and within the MassHousing’s information technology 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 activities at the Massachusetts Housing Finance Agency for the period of July 1, 2007 through May 20, 2009. The audit was conducted from October 8, 2008 through May 22, 2009. Our audit scope included a general control examination of internal controls related to the organization and management of IT activities and operations, physical security, environmental protection, logical access security for MassHousing's automated systems, inventory control over computer equipment, business continuity planning, and on-site and off-site storage of backup copies of magnetic media. We also reviewed data integrity controls for the RealServicing application system, and MassHousing's policies and procedures regarding the protection of personally identifiable information.

Audit Objectives

Our primary audit objective was to determine whether MassHousing's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT control objectives would be addressed to support business functions. Our audit objective regarding IT organization and management was to determine whether roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and whether policies and procedures adequately addressed the areas under review.

We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent and detect unauthorized access to areas housing IT resources, damage, or loss of IT-related assets. Our objective regarding logical access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized personnel had access to the LAN and to the automated systems. Furthermore, we sought to determine whether MassHousing management was actively monitoring password administration.

With regard to inventory control over IT equipment, we evaluated whether an annual physical inventory and reconciliation was conducted and whether IT equipment was accurately recorded in the system of record and accounted for, and that the inventory records were properly maintained. Regarding systems and network availability, we sought to determine whether adequate business continuity plans were in effect to provide reasonable assurance that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render IT processing inoperable or inaccessible.

Moreover, we sought to determine whether adequate controls were in place to provide reasonable assurance that appropriate backup copies of application systems and data files would be available on-site and off-site to support disaster recovery and business continuity planning objectives.

We also sought to determine whether selected data elements in the RealServicing application, which is used to track the Single-Family Loan portfolio, were accurate and complete. A further objective was to determine whether MassHousing had controls in place and in effect to control and secure personally identifiable information and to determine whether control policies and procedures were adequate to comply with the Commonwealth's data breach notification requirements.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of MassHousing's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of MassHousing's organization and operations, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant functions and activities supported by the automated systems and reviewed automated functions designated as mission-critical by MassHousing. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

In our review of IT organization and management, we interviewed senior management from MassHousing and analyzed and reviewed the organizational structure and reporting lines of the IT staff. We obtained, reviewed, and analyzed selected IT-related policies and procedures to determine their adequacy. To determine whether IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of the IT staff, including their duties and job descriptions, and compared the list to MassHousing's organizational chart. We also interviewed six members of the IT staff and verified their day-to-day responsibilities.

To evaluate physical security, we interviewed management, conducted walk-throughs and inspections of the data center and administrative offices areas housing IT equipment. Through observation and tests, we determined the adequacy of physical security controls over the areas housing IT equipment. We verified the existence of physical security controls, such as door locks and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees. Further, we reviewed procedures to document and address security incidents and requested a list of individuals who were authorized to access the data center.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether the data center was neat and well organized. To determine whether proper temperature and humidity controls were in place, we sought to determine whether the data center had appropriate controls such as a dedicated air conditioning unit. Further, we reviewed control procedures to prevent water damage to automated systems, records, and magnetic backup media stored on site.

To obtain an understanding of access security controls, we reviewed MassHousing's access security policies and procedures that would provide reasonable assurance that only authorized users had access to MassHousing's network and mission-critical applications systems and data files. In addition, we reviewed security practices with IT management and evaluated selected access controls to the network and the selected mission-critical applications consisting of Benedict, CODA, PAM and RealServicing. Our test of logical access security controls included a review of user accounts for all MassHousing employees who were authorized to access these application systems. In order to verify that all users of the LAN and mission-critical application systems were current MassHousing employees, we obtained a LAN account listing containing 387 user accounts, as of February 23, 2009, and for the mission-critical user accounts totaling 358, as of January 22, 2009. We compared the system generated user account list for the LAN and the mission-critical applications to a current MassHousing employee list. We developed exception lists of the user accounts and individuals not identified as employees.

We reviewed control policies regarding logon ID, password composition and user account administration, and evaluated the appropriateness of documented policies provided to MassHousing personnel, and interviewed employees from the business divisions responsible for logical access security. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted to only authorized users, we reviewed procedures for authorizing, activating, and deactivating access to application software and related data files.

With regard to inventory control over computer equipment, we determined whether an annual physical inventory was conducted, whether computer equipment was accurately reflected in the fixed-asset inventory, and whether the system of record for inventory was properly maintained. To determine whether adequate controls were in place and in effect to properly account for computer equipment, we reviewed inventory control policies and procedures and requested and obtained MassHousing'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 confirm the existence and assess the proper recording of computer equipment, we used ACL software to generate a random sample of 70 items out of a total population of 1,372 items recorded on the inventory list dated December 10, 2008. Our purpose was to verify the location of the equipment and compare information for identification tag numbers, description, and historical cost. In addition, we judgmentally selected 100 items of computer equipment from their locations and determined whether the items were properly recorded on the inventory list.

To assess the adequacy of system availability, we determined whether formal planning had been performed to develop and maintain a business continuity plan to resume computer operations should the network application systems be inoperable or inaccessible. We also determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. To evaluate the adequacy of controls to protect data files through the backup of on-site and off-site magnetic media, we interviewed senior MassHousing staff regarding the generation of backup copies of computer-related media. In addition, we visited the off-site storage location of a private vendor that MassHousing contracts with to provide storage for magnetic media. We performed a review and comparison of the data files provided by MassHousing and the private vendor related to the inventory of Agency tapes held by the vendor at their facility.

Our tests of data integrity over the RealServicing application included a review of the critical fields of information captured on mortgage application documents. To gain an understanding of the application, we attended a training session provided by MassHousing to familiarize ourselves with the information recorded in the OnBase source documents. We conducted a data integrity test using ACL audit software to select a sample of 70 loans out of a population of 4,370 loans. We tested the sample loan records to determine whether the source documents provided by MassHousing were accurately and completely recorded in the RealServicing application. Our audit test included a comprehensive review of selected data elements comprised of name, loan number, date of application, address, loan amount, interest rate, monthly payment amount, maturity date and latest transaction date.

With respect to personally identifiable information (PII), we reviewed Chapter 93H of the Massachusetts General Laws and Executive Order 504 to identify Agency responsibilities regarding protection of PII and notification of confidentiality breaches. We interviewed senior management and completed a PII assessment questionnaire regarding the protection of personal information of MassHousing’s clients and staff.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and industry auditing practices. Criteria for the IT portion of our audit included IT management control practices as outlined in the Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology" (CobiT).

AUDIT CONCLUSION

Based on our audit, we found that MassHousing's internal controls provided reasonable assurance that IT-related control objectives pertaining to organization and management, physical security, environmental protection, inventory control over computer equipment, on-site and off-site storage of backup copies of magnetic media, and business continuity and disaster recovery would be met. We also found that controls in place provided reasonable assurance that selected data elements from the RealServicing application system were accurate and complete and that personally identifiable information would be protected from unauthorized access or disclosure. However, although appropriate access security controls were in place, controls over user account management needed to be strengthened to provide further assurance that user access privileges are consistently deactivated for users no longer authorized to access Agency systems.

Our examination of IT organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties, and clear points of accountability regarding IT functions. We found that management and staff appeared to be aware of their responsibilities and that documented job descriptions were in place that defined the responsibilities for the 30 IT staff members. Our review of internal controls found that MassHousing had adequate policies and procedures for the IT-related functions under our review.

We found that physical security controls provided reasonable assurance that IT resources located in the data center and in the on-site and off-site storage areas were adequately protected against unauthorized physical access. We found that the combination of preventive and detective controls, including management control practices, provided reasonable assurance that IT equipment would be protected against unauthorized access, damage, or theft. We also found that MassHousing's data center was locked and that access was limited to designated senior staff members. Further, we found that employees were required to have access security cards to gain entry to MassHousing's office areas and that the data center was equipped with video surveillance and motion detection equipment.

Environmental protection controls over the data center and office areas were found to provide reasonable assurance that IT resources were operating in a controlled environment. Specifically, we found that control objectives related to air conditioning; water detection; fire prevention, detection, and suppression; emergency power and lighting; and power shut-off would be met. We observed that MassHousing had

UPS units to permit controlled shutdowns and back-up generators to restore power in the event of an emergency. We observed that general housekeeping controls in the data center were adequate.

Our audit revealed that logical access security controls over MassHousing's LAN and mission-critical applications provided reasonable assurance that control objectives would be met to support administrative and business operations. We found that appropriate policies and procedures were documented; security administration had been assigned; appropriate rules for user access activation, password length, and composition were in place; and security requirements had been established. We found that employees were required to change passwords on a pre-defined time period. However, our tests of authorized LAN user accounts revealed that 14 user accounts could not be reconciled to MassHousing's employee listing. We determined that one account, for a user who had terminated employment on June 30, 2006, had not been deactivated at the time of our test. Our test of logical access to MassHousing's mission-critical applications consisting of CODA, Benedict, PAM, and RealServicing revealed that two users could not be identified on the payroll record. Our audit test identified these two active Benedict accounts as belonging to employees who terminated employment from MassHousing in August and October 2008. We recommend that MassHousing reinforce its current policy requiring prompt notification to the security administrator of changes in employee status that could warrant deactivation or a change in the level of access privileges of user accounts.

With respect to inventory control over computer equipment, we found that an accurate and complete list of computer equipment was being maintained. We also found that MassHousing performed annual physical inventories and reconciliation to address accounting requirements promulgated by the Office of the State Comptroller. Our tests indicated that hardware items were locatable, properly accounted for, and tagged. The inventory system of record for computer equipment would be enhanced by including expense terms for all leased computer equipment deployed by the Agency.

We determined that procedures regarding the generation of backup copies of magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate. We found that MassHousing had an adequate business continuity strategy and recovery plan to help ensure resumption of processing within an acceptable time frame should IT processing be rendered inoperable or inaccessible. Regarding our review of the off-site storage location, we confirmed that physical and administrative security controls appeared to provide adequate protection for MassHousing's electronic media. Our audit tests revealed that there were no discrepancies between the Agency's record of backup tapes stored off site and the vendor's inventory of Agency tapes stored at their facility.

Our review of data integrity controls over selected data fields in the RealServicing application revealed that there were documented policies and procedures over data preparation and maintenance. Our data integrity test, which was based on a random sample of 70 loan portfolios from a population of 4,370 loans, revealed that there were no discrepancies between the source documentation and the data contained within the application system.

Our review of MassHousing's efforts to comply with the requirements of MGL Chapter 93H regarding the safeguarding of personally identifiable information revealed that policies and procedures were developed to comply with the regulations. Furthermore, MassHousing has required that all staff be trained in their responsibilities of protecting sensitive and confidential information. Although not specifically required to follow Executive Order 504, MassHousing has elected to adopt the Executive Order requirements with regard to complying with MGL Chapter 93H.

AUDIT RESULTS

User Account Management

Our audit found that sound access security policies and procedures were in place and in effect; however, controls over access account deactivation could be further strengthened. Although access security over MassHousing's network appeared to be appropriate, controls needed to be strengthened to ensure that user privileges are deactivated for individuals no longer authorized to access automated systems thereby providing reasonable assurance that only authorized users have access to the LAN and mission-critical applications. Overall, we found that appropriate policies and procedures were in place, security responsibilities had been assigned, and that appropriate rules for user account activation, password composition, and frequency of password changes were in place for user access to the MassHousing network.

Our tests of logical access security for the LAN indicated that there were a small number of active user accounts that had not been deactivated or deleted for individuals who were no longer employed by MassHousing. Our tests of authorized user accounts indicated that 14 out of 387 individuals who were assigned user accounts could not be identified on a MassHousing official employee listing. These user accounts were later identified as individuals who had terminated employment with MassHousing and contractors whose accounts were not deactivated or deleted in a timely manner. For example, our audit test disclosed that a contract employee, who terminated employment with MassHousing in June 2006, still remained on the user account list as of January 2009.

Our test of MassHousing's mission-critical applications consisting of: CODA, Benedict, PAM (Portfolio Asset Management) and RealServicing, revealed that two users could not be identified on the payroll record. Our audit test identified the two active Benedict accounts as belonging to employees who no longer worked for MassHousing. Although the two individuals had terminated their employment in August and October 2008, their user accounts had not been deactivated. Our audit revealed that in this instance there was a low risk factor due to compensating controls. Since the application systems are not web-based, it would require physical access to a workstation to access the application. It was determined that the individuals' access cards had been deactivated upon termination and that their password and two-factor authentication had expired.

Our audit revealed that increased monitoring was required to evaluate access privileges and identify user accounts that should be deactivated to ensure that only authorized individuals had access to MassHousing's network and automated systems. The failure to deactivate or delete user accounts in a more timely manner places MassHousing's automated systems at risk of unauthorized access or having an individual gain higher access privileges than currently authorized.

The Control Objectives for Information and Related Technology (CobiT), issued by the Information Systems Audit and Control Association, is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners and IT functions. Additional controls recommended by the CobiT control framework include having procedures to ensure timely action for requesting, activating, suspending and closing user accounts, having a control process to periodically review and confirm access rights, and regularly performing scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse or unauthorized change.

Recommendation

We recommend that MassHousing reinforce its current policy requiring department heads, supervisors, and the Human Resources Department notify the security administrator in a timely manner of changes in employee status that could warrant deactivation or a change in the level of access privileges of user accounts. We recommend that MassHousing expand quarterly reviews of the status of all active users to the network and application systems to include confirmation of authorized access privileges for users requiring access to Agency systems. We also recommend that MassHousing management enhance their written policies on activation and deactivation of access privileges for full-time, part-time, seasonal interns and contract employees to ensure that user accounts are deleted in a timely manner.

Auditee's Response

As was noted in the draft audit report, the Agency's exposure was largely mitigated due to the following factors:

- *The user accounts that should have been deactivated were for users who no longer had access to the building as controlled by the building's card access reader system, nor did those users have remote access to the network;*
- *The user accounts that should have been deactivated were for users who were temporary workers. Temporary workers are not provided a password in writing: their fingerprint is their required password. Requiring a fingerprint – read by the biometric devices attached to our PCs – controls user access, and prevents a temporary worker from passing on his/her user privileges to another person.*

The Agency agrees with the recommendation that communication should be improved when an employee's network security status or privileges have changed or needed to be deactivated. The Agency will make the necessary revisions and updates to the procedures.

> *The Agency agrees with the recommendation that quarterly reviews of all active network users be performed. Currently, MassHousing performs a quarterly review, with required sign-offs by the application owner(s), on four core Agency applications. This review and sign-off procedure will be expanded to include all network user accounts. The Agency will make the necessary revisions and updates to the procedures.*
>
> *The Agency agrees with the recommendation that the documentation related to the activation and deactivation policy and procedures should be improved. The Agency will make the necessary revisions and updates to the procedures.*

Auditor's Reply

We commend the MassHousing's action for addressing the security concerns related to user account management. We acknowledge that MassHousing does have appropriate controls regarding password security and policies to activate and deactivate user accounts. We believe that MassHousing's efforts to improve communications regarding changes in network security status or access privileges for employees will enhance controls over user account management.