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. 2001-0616-4C

OFFICE OF THE STATE AUDITOR'S

REPORT ON

INFORMATION TECHNOLOGY-RELATED CONTROLS

AT THE BOSTON HOUSING AUTHORITY

February 1, 1999 through November 30, 2001

OFFICIAL AUDIT REPORT

AUGUST 23, 2002

TABLE OF CONTENTS

INTRODUCTION

The Boston Housing Authority (BHA) is organized under the authority of Chapter 121B of the Massachusetts General Laws. Chapter 88 of the Acts of 1989 gave the Mayor of Boston the power to appoint an administrator with the authority to manage and control operations at the BHA. In addition, the legislation authorized the Mayor to appoint the Boston Housing Authority Monitoring Committee, which is comprised of nine members, including five public housing tenants. The Committee's mission is "to periodically review matters relating to the management and performance of the BHA and to report thereon to the Mayor." Members were appointed to the Committee in December 2000.

The BHA is comprised of 15 departments, including, in part, community services, fiscal, occupancy, leased housing, risk management, and management information services (MIS). The BHA operates from a central office in Boston and manages 64 development sites throughout the city. At the time of our audit, the BHA was staffed by approximately 1,003 employees. According to the BHA's website, the Authority is the largest landlord in Boston and the largest public housing authority in New England, providing housing in various city neighborhoods for approximately 27,000 residents.

The BHA's primary mission is "to provide stable, quality affordable housing for low and moderate income persons; deliver service with integrity and mutual accountability; and create an environment to transform from dependency to economic self-sufficiency." In addition to providing public housing, the BHA provides affordable housing through several rental assistance programs, such as the federal Section 8 voucher program and the state-funded Massachusetts rental voucher program. Furthermore, through its assistance program, BHA administers approximately 11,000 rental assistance vouchers allowing an estimated 25,000 people to receive rental assistance. The BHA is governed by housing regulations issued by the United States Department of Housing and Urban Development and the Massachusetts Department of Housing and Community Development (DHCD).

The BHA is funded by both the federal and state governments. For the annual fiscal period ending March 31, 2001, the BHA received $160,802,588 from a federal operating subsidy and grants and $23,089,354 from a state operating subsidy and grants. In addition, the Authority reported rental income of $33,133,502 for that period.

From an information technology (IT) perspective, the Authority's MIS Department supports the mission of BHA by administering the IT infrastructure and helping to ensure that BHA staff know how to effectively and appropriately use the technology. At the close of the audit, the BHA IT infrastructure that supported the Authority's business functions, consisted of nine file servers

installed at the central office in Boston, one server located at a development site, and 407 microcomputer systems configured in a wide area network (WAN). The file servers at the central office were connected to microcomputer systems at 39 management sites and nine maintenance sites and to the file server at the development site through telecommunication links. BHA's primary application system is the Creative Computer Solutions (CCS) system, installed in the mid-1980s, which supports business operations through 13 modules or subsystems, such as accounts payable, fixed assets, housing eligibility, inventory control, payroll, work order, and tenant accounting. The CCS database resides on a dedicated application server. In addition, the BHA's application systems include business office applications and support systems, such as word processing.

The Office of the State Auditor's examination focused on a review of selected general controls pertaining to physical security and environmental protection at the central office in Boston and the Mary Ellen McCormack and Amory Street development sites, system access security, and inventory control over IT-related resources. We also examined control practices regarding business continuity planning and on-site and off-site storage of backup copies of magnetic media. In addition, we reviewed control practices regarding security over hardcopy confidential client records.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From February 8, 2001 through November 30, 2001, we performed an audit of selected information technology (IT) related controls at the Boston Housing Authority (BHA) for the period covering February 1, 1999 through November 30, 2001. The scope of our audit included a review of the organization and management of computer operations. We reviewed and evaluated system access security for the automated systems, specifically the Creative Computer Solutions (CCS) application system, and a review of access controls over the network on which the CCS application resides. In addition, we examined control practices regarding physical security and environmental protection over and within BHA's central office in Boston and the Mary Ellen McCormack and Amory Street development sites in South Boston and Jamaica Plain respectively. Further, we reviewed physical security and environmental protection over restricted areas housing confidential client records and on-site storage for magnetic media at the central office and the two development sites. We examined control practices regarding security over and the transfer of hardcopy confidential information regarding BHA clients.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the CCS system. With respect to the restoration of normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning and the physical security and environmental protection of backup media stored on-site. We reviewed procedures for generating and transferring backup copies of mission-critical and essential magnetic media to an off-site storage location. We examined inventory control practices for computer equipment and software. We also reviewed prior audit results documented in our audit report No. 99-0616-3, issued September 24, 1999, and determined whether corrective action had been taken by BHA regarding our recommendations.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT-related resources and whether system information would be sufficiently protected against unauthorized disclosure, change, or deletion. In addition, we sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized

users were granted access to the CCS application and the network on which the application resides and which procedures were in place to prevent and detect unauthorized access to automated systems. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to restrict access to IT resources, including confidential client records in hardcopy form, to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources. We sought to determine whether adequate business continuity planning had been performed and whether plans were in place to restore mission-critical and essential business operations in a timely manner should the CCS application system be unavailable for an extended period. Further, we sought to determine whether adequate control procedures were in place regarding on-site and off-site storage of magnetic media. Another objective was to review and evaluate control practices regarding accounting for IT-related resources, including computer equipment and software. In addition, we sought to determine whether BHA had addressed the audit results documented in our prior audit report and had taken corrective action regarding these issues.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of BHA's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of BHA's organization and operations and selected portions of the Creative Computer Solutions operations manual, we gained an understanding of the primary business functions supported by the automated systems. We reviewed automated and manual functions regarding the process for renting housing units, collection and recording of rental payments, and procurement and payment for goods and services. We documented the significant functions and activities supported by the CCS application system, and reviewed automated functions related to operations designated as mission-critical by BHA, such as the processing of payroll. We reviewed the vendor contract with the MIS Director for ongoing maintenance and support of the CCS modules.

We reviewed and evaluated the organization and management of IT operations at the central office. We inspected the central office in Boston, including the computer room, reviewed relevant documents, such as the network configuration and draft security policy, and performed selected preliminary audit tests. We determined whether BHA had taken corrective action regarding audit results documented in our prior report.

We conducted additional pre-audit work, which included reviewing the role of the central office regarding physical security and environmental protection over the business offices and restricted areas housing client records at the Mary Ellen McCormack and Amory Street

development sites. In addition, we interviewed central office management to discuss internal controls regarding physical security and environmental protection over and within the computer room at the central office, microcomputer systems installed at the central office and development sites, and on-site and off-site storage of critical magnetic media. We performed a review of internal controls related to physical security over hardcopy client records located at the central office and two development sites. With respect to inventory control, we determined the role of the central office regarding accounting for computer equipment and software. We reviewed procedures used by BHA for daily backup of the CCS database and transport of magnetic media for storage to a vendor's off-site location. In conjunction with our audit, we reviewed formal policies and procedures promulgated by BHA and the Massachusetts Department of Housing and Community Development (DHCD) regarding controls and operations with respect to the audit objectives for the areas under review. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to comply with statutes, regulations, and generally accepted control objectives for IT operations and security.

We performed audit tests at BHA's central office and at two development sites to determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and whether the IT resources were adequately safeguarded from loss, theft, or damage. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with BHA management and staff. We interviewed the administrative manager at each of the two development sites that we visited. To determine whether adequate controls were in effect to prevent and detect unauthorized access to business offices housing automated systems, we inspected physical access controls, such as the presence of security officers on duty, locked entrance and exit doors, the presence of a receptionist at the entrance point, burglar alarms, and whether visitor badges were issued.

We reviewed access control procedures, such as the list of staff authorized to access the computer room, and key management regarding door locks to the computer rooms and other restricted areas. We determined whether BHA maintained incident report logs to identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of IT-related equipment.

To determine whether adequate controls were in effect to physically secure confidential client records, we inspected restricted areas within business offices where confidential client records were stored. We determined whether doors to the restricted areas were locked and whether file cabinets used to store client records were secured. To determine whether only authorized BHA staff were granted access to client records, we interviewed central office management and administrative managers at two development sites. We reviewed sign-out/sign-

in procedures for client records at the central office. Further, we reviewed control practices regarding the disposal of client records.

To evaluate environmental protection over automated systems, we determined whether 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 were in place. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were located in the computer room or in the vicinity of IT-related equipment. To evaluate temperature and humidity control, we determined whether appropriate dedicated air conditioning units were located in business offices and computer rooms. Further, we reviewed control procedures to prevent water damage to automated systems, client records, and on-site storage for magnetic media.

We determined whether only authorized users were granted access to the CCS application system and the network on which the application operates. To accomplish this objective, we reviewed policies and procedures regarding system access security, such as procedures used to authorize, activate, and deactivate access privileges to the network and CCS application and data files. We also reviewed control practices regarding logon ID and password administration.

To determine whether controls in place provided reasonable assurance that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing access to the network and the CCS application and data files. In addition, we reviewed control practices used to activate access privileges to the network and CCS application programs and data files. To determine whether only authorized employees and outsourced staff were accessing the automated systems, we obtained the list of individuals granted access privileges to the CCS application and compared it to the current personnel roster of BHA employees and outsourced staff. We determined whether all employees and outsourced staff authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. Further, we determined whether formal system logs regarding daily network operations had been implemented and reviewed in a timely manner to detect unusual system activity or violations.

Regarding access security to BHA's network, we reviewed security procedures with the MIS Director responsible for management of the network and evaluated access controls to the network and CCS application. We reviewed and evaluated security practices regarding access procedures for the firewall and controls over modems used to access the network, including the file server on which the CCS application and data files reside. Further, we reviewed change control procedures over the firewall's router access control list that allows access through the firewall.

A firewall is a combination of hardware and software that restricts access to a network and IT resources. We also reviewed control practices regarding dial-in procedures to the network.

To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed inventory control procedures for computer equipment and software with the MIS Director and the Director of Procurement. We reviewed BHA and DHCD policies and procedures regarding inventory control. We obtained the inventory record dated April 26, 2001 with a listed total value of $1.3 million. We determined whether computer equipment installed at the central office and Amory Street and Mary Ellen McCormack development sites was tagged with state identification numbers and whether the tag numbers were accurately listed on the inventory record. We reviewed the inventory record to determine whether "data fields," such as identification number, manufacturer's number, location, and cost were listed on the record. Further, we reviewed the adequacy of procedures used by BHA to dispose of and properly account for obsolete equipment. We also reviewed control practices regarding safeguarding and accounting for laptop computers.

To determine whether the April 26, 2001 IT-related inventory record was current, accurate, and complete, we confirmed information listed on the inventory record provided by the auditee to descriptive information obtained from the actual computer equipment on hand at the central office and at two development sites and supporting documentation. In addition, we determined whether IT resources purchased from 1997 through 2001 were properly recorded on the inventory record by tracing information obtained from purchase documentation to the inventory record and verifying that purchased file servers were installed at the central office and that workstations had been installed and existed through on-site verification at two development sites. In this regard, we obtained purchase documentation for eight file servers and 272 microcomputer systems purchased during that period and attempted to confirm information to the inventory record. We then traced the file servers recorded on the inventory record to the actual equipment installed in the computer room at the central office. In addition, we confirmed selected microcomputer systems listed on the inventory record to the actual equipment on hand. Regarding the Mary Ellen McCormack development site, we confirmed nine microcomputer systems (100%) listed on the inventory record to the actual equipment located in the business office. Moreover, we traced a judgmental sample of 23 (39%) microcomputer systems installed at the Amory Street development site to the 59 items of computer equipment listed on the inventory record. In addition, we determined whether BHA had implemented a current software inventory.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers on which the CCS application operates and the microcomputer

systems be unavailable for an extended period. We interviewed the MIS Director to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. Further, we interviewed the Director of Occupancy and the Housing Manager at the Mary Ellen McCormack development site and the assistant director at the Amory Street site regarding procedures in place to resume normal business functions should access to the file server housing the CCS application or the microcomputer systems be unavailable.

We reviewed the proposed contract initiated by BHA with a vendor to provide business continuity planning for the Authority. We reviewed the contract for appropriate content, strategic objectives, and clarity of directives and procedures. In addition, to determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated system be rendered inoperable, we interviewed BHA management responsible for generating backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of backup copies of mission-critical and essential magnetic media at the central office and two development sites.

We sought to determine whether BHA had taken corrective action regarding audit results documented in our prior audit report No. 99-0616-3. To determine whether BHA had implemented adequate controls regarding gasoline purchases, we conducted interviews with the BHA Director of Procurement and the Director of Finance. We determined whether BHA continued to use the Authority's central stores facility to distribute gasoline for its vehicles. Because BHA had contracted in December 1998 with a vendor through the Commonwealth's Operational Services Division's (OSD) statewide procurement program and the City of Boston to purchase gasoline, we reviewed the control procedures used to monitor purchases, such as the assignment of a fuel card used in conjunction with a personal identification number (PIN). Further, we reviewed and evaluated a judgmental sample of paid invoices for the 2001 fiscal year to determine whether the invoices included sufficient information to monitor purchases and provide evidence of supervisory approval. We sought to determine whether BHA had strengthened controls to prevent the use of cellular phone for non-business calls and to ensure that BHA would be reimbursed should personal calls have to be made. We interviewed the BHA Director of Procurement regarding control practices for monitoring cellular phone services. We reviewed selected invoices for supervisory review and approval, evidence of reimbursement for non-business calls, reimbursement checks paid to the Authority for personal calls, and bank deposit slips for these monies. Further, we determined whether BHA had improved its record management system regarding payments for the drug elimination program. We interviewed the Director of Finance regarding the payment process for the drug elimination program. We

reviewed a random sample of 8 (22.2%) of 36 paid invoices and supporting documentation for the program made during January 2001.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT SUMMARY

Based on our audit, adequate controls were found to be in place to provide reasonable assurance that IT-related resources at the Boston Housing Authority's (BHA) central office and the Mary Ellen McCormack and Amory Street development sites were properly safeguarded and protected from damage or loss. Although control practices regarding on-site and off-site storage of backup copies of magnetic media were adequate, overall business continuity planning required strengthening to ensure availability of automated processing and electronic data. Our audit indicated that controls regarding system access security and the accounting for IT-related resources also needed to be strengthened. Further, formal policies and procedures needed to be developed or enhanced regarding physical security, environmental protection, and system access security. (See Appendix B, Summary of Internal Control Practices, page 27.)

Our review of the BHA's internal control structure indicated that senior management was aware of the need for internal controls and had implemented appropriate controls to safeguard the Authority's IT-related resources. We determined that there was a defined organizational structure for IT operations, an established chain of command, clear assignment of responsibilities, and documented job descriptions. Our audit indicated that BHA had formulated a strategic vision for the use of information technology, including plans for a new application system and improvements to the IT function. With respect to appropriate use of information technology, we determined that the Authority had promulgated adequate written policies and procedures regarding e-mail and Internet use. However, BHA needed to improve documented controls by developing more specific control practices and operating procedures regarding physical security and environmental protection, logon ID and password administration, and business continuity planning.

We found that BHA had implemented adequate physical security controls to provide reasonable assurance that only authorized persons could access the business offices and computer room at the central office and the IT resources at the Mary Ellen McCormack and Amory Street development sites. Further, we determined that security over hardcopy confidential information at the central office and the two development sites that we visited was adequate. Our audit indicated that appropriate controls, such as a designated facilities manager responsible for physical security, foot patrols conducted by the housing authority police force within buildings and surrounding grounds 24/7, and locked entrance doors during non-business hours, were in place at the central office and the Mary Ellen McCormack and Amory Street development sites. In addition at the central office, we found that BHA had implemented appropriate controls, such as security officers stationed in the building lobby 24/7, visitor registration, and ID badges

required for staff to enter the building. The computer room was located in a non-public area, a punch keypad lock system was installed, the door was always locked, and only authorized staff were granted access to the room.

In addition to the controls noted above, our audit confirmed that other important physical security controls were in place at the Mary Ellen McCormack and Amory Street development sites. We found that access to the business offices at the Mary Ellen McCormack site was restricted to one entrance door, a receptionist was on duty during normal business hours, and intrusion detection devices were installed in the building. With respect to the Amory Street site, we determined that security cameras were installed on the outside of the building housing the business offices, offices were patrolled during normal business hours by housing authority police, a list of staff authorized to access the business offices was maintained and reviewed monthly, visitor registration was required, and formal termination procedures that included return of keys were in place. Further, breaches of physical security at both development sites were required to be reported to the housing authority police.

Our audit indicated that adequate environmental protection, such as temperature controls, smoke detectors, fire alarms, hand-held fire extinguishers, sprinkler systems, and 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. Regarding the computer room, we determined that the file servers were subject to appropriate air quality and temperature controls. A fire suppression system and sprinkler systems were in place within the computer room. Emergency evacuation procedures were documented and posted adjacent to the computer room and, according to BHA management; IT staff were trained in the emergency procedures. We found good housekeeping procedures in place within the computer room in that it was neat, clean, and in good order. Further, BHA management stated that a regular inspection and maintenance program was in place regarding heat, ventilation, and air conditioning systems and the fire suppression system was tested periodically. The file servers were installed above floor level to help prevent water damage.

Regarding the Amory Street development site, we determined that appropriate environmental protection controls, such as good housekeeping procedures in the business offices, fire alarms and sprinkler systems installed throughout the building, and a UPS, were in place. However, our audit revealed that environmental protection controls needed to be improved at the Mary Ellen McCormack development site. We found that although good housekeeping procedures were in place, fire alarms and a UPS had not been installed in the business office. We recommend that BHA management review environmental protection at the development sites

to ensure that consistent controls are in place and, based on the results, BHA should strengthen controls, such as the installation of fire alarms.

With respect to system access security, our audit disclosed that the processes for granting and recording authorization and activating logon IDs and passwords were appropriate. However, control practices regarding access security policies and procedures, deactivation/deletion of logon IDs and passwords, and periodic changes of passwords needed to be improved. We determined that, as of the date of our audit, formal authorization procedures for granting access privileges to users had been implemented. Access privileges to the CCS application system were assigned to users based upon pre-determined levels of access related to position, job title, and associated responsibilities. Further, logon IDs and passwords were being used to access the CCS system and the network on which the application resides. Our audit indicated, however, that passwords were not being changed periodically. We recommend that BHA evaluate the required frequency of password changes and implement appropriate mechanisms to ensure that passwords are changed according to schedule.

Our audit revealed that procedures for deactivation/deletion of logon IDs and passwords needed to be strengthened. We found that 19 (5.5%) of 344 logon IDs and passwords used to access the CCS system remained active for individuals no longer authorized or needing access to the system. Upon our recommendation, the 19 logon IDs and passwords were deactivated. We recommend that BHA designate the Human Resources Department to notify the MIS Department's personnel charged with responsibility for access security administration to deactivate an employee's logon ID and password when access privileges are no longer required.

We recommend that BHA review the draft security policy and incorporate documented control practices in its internal control plan. The policies and procedures should include control practices for authorizing, activating, and deactivating logon IDs and passwords. To strengthen system access security, we recommend that BHA ensure that all users granted access to the automated systems understand their responsibilities regarding protection and appropriate use of their passwords by requiring users to sign a formal security statement.

Regarding our review of the firewall protecting data on the BHA network, nothing came to our attention to indicate that security controls in place were not preventing unauthorized access to the network. We recommend that BHA implement continuous monitoring of the firewall to detect any changes regarding security controls.

We found that BHA could not provide reasonable assurance that its system of record for IT-related resources, with a listed value of $1.3 million, could be relied upon. Our audit revealed that the inventory record dated April 26, 2001, was not current, accurate, or complete. We found that of eight file servers purchased from 1997 through 2001, six servers, valued at $91,000, were

not recorded on the inventory record. In addition, we found that 272 microcomputer systems purchased during the 1999 fiscal year and valued at $291,040 were not recorded on the inventory record. We determined that microcomputer systems previously designated as surplus property had not been either identified as “to be placed in surplus” on the inventory record or removed from the record when the equipment was placed in surplus. The number and cost of these computers could not be determined from BHA records. We recommend that BHA comply with the Massachusetts Department of Housing and Community Development requirements to perform an annual physical inventory and reconciliation of the inventory record. We recommend that BHA implement documented procedures, including sign-out/sign-in logs, to properly account for laptop computers.

Our audit revealed that although BHA had implemented adequate on-site and off-site storage of backup copies of magnetic media, a formal business continuity plan had not been developed to restore normal business functions in a timely manner should automated systems, specifically the mission-critical CCS system, be unavailable for an extended period. We acknowledge that BHA management was aware of the need for business continuity planning and had outsourced the development of a recovery plan. We determined that at the Mary Ellen McCormack and Amory Street development sites, informal procedures regarding the use of an alternate processing site had been developed. Given the absence of comprehensive recovery plans and the dependence of BHA on the CCS application system to perform its mission-critical business functions, a significant disaster impacting the Authority’s automated systems for an extended period, specifically the file server on which the CCS application database resides, would affect the BHA’s ability to regain critical IT operations, such as processing the payroll, processing tenant applications and work orders and accounting for rent monies. We recommend that BHA aggressively pursue the development of a business continuity plan, including alternate processing site(s) and user area plans.

With respect to prior audit results documented in audit report No. 99-0616-3, we determined that sufficient corrective action had been taken to address inadequate control practices noted in the report. (See Appendix A, Prior Audit Results, page 25.)

AUDIT RESULTS

1. System Access Security

Our audit disclosed that although certain system access security controls were in place, other control practices needed to be strengthened to provide reasonable assurance that only authorized users have access to the Creative Computer Solutions (CCS) application system and the network on which the application resides. We found that control practices regarding documented access security policies and procedures, deactivation/deletion of logon IDs and passwords, and required periodic changes of passwords needed to be improved.

Regarding authorization, we determined that control procedures granting users access to the network and the CCS application system were appropriate. We found that BHA, as of November 1, 2000, had implemented a formal process for authorizing new employees access to the network and CCS application. These procedures included having the new employee's manager complete a "User Change Form," notifying the help desk within the MIS Department to initiate a work order, and activating the user's network and system access by the network support specialist. The employee would then be assigned access to a CCS module based upon pre-determined levels of access related to the individual's position, job title, and associated responsibilities designated by the manager. Subsequent to being granted access privileges, users were assigned a unique logon ID and password through the system to access the appropriate CCS modules and were allowed to choose a password of sufficient length and composition to access the network. To gain access to the system, the user was then required to enter his/her logon ID and password. Access to system-based resources would be obtained based upon information entered in the access control table.

With respect to procedures to deactivate access privileges, our audit revealed that adequate controls were not in place to provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the automated systems. We found that, as a result, 19 logon IDs and passwords remained active for individuals no longer authorized or needing access to the CCS application system. Failure to deactivate logon IDs and passwords may allow unauthorized access to confidential client information, because the access privileges of staff that have terminated or transferred employment, or taken new positions within the Authority, may continue to be available for use. Changes in employment status that should affect system access privileges are termination of employment, change of position or job responsibilities that impact the level of access required, and extended leaves of absence when access is not required.

During the audit, we tested the user database for the presence of unauthorized users whose access privileges remained active after the users were no longer authorized to have access. We chose 344 (100%) of active logon IDs for employees and outsourced staff authorized to access the CCS system.

Based on our comparison of active user privileges to the current official personnel list, we determined that 19 (5.52%) of the user accounts selected were active for individuals who no longer worked for the Authority and had terminated employment one week to one year prior to the date that the test had been performed. Upon our notification, BHA deactivated access privileges for the 19 user accounts to the automated systems.

We determined that, at the date of our audit, BHA required department managers, rather than the Human Resources Department, to notify the help desk weekly, through the "User Change Form," regarding changes in employee job status that would require modification or deactivation of the user's access privileges.

Our audit indicated that although the draft security policy addressed logon ID and password administration, including password formation and use, periodic changes of passwords, and confidentiality requirements of passwords for the CCS application system, we found that user passwords were not being changed in a timely manner. According to BHA management, controls regarding passwords were implemented to assist users in gaining familiarity with the application system. Once users understood the system, periodic password changes were to be implemented.

Regarding policies and procedures, our audit disclosed that although control procedures regarding appropriate use of IT-related resources, including data confidentiality, e-mail and Internet use, and logon ID and password administration were included in documentation, such as the draft versions of the "Boston Housing Authority Security Policy" for the CCS system and the "Boston Housing Authority Policy on the Use of Technology Resources," the written control procedures had not yet been approved or incorporated within an internal control plan. Further, we found that BHA had not implemented adequate mechanisms to ensure that all users granted access to the automated systems understood their responsibilities regarding protection and appropriate use of their passwords by requiring users to sign a formal security statement.

Generally accepted computer industry standards dictate that IT resources be made available to only authorized users and that the resources be used for only authorized purposes. To help ensure that only authorized users have access to IT resources, appropriate controls also need to be implemented to prevent and detect unauthorized access by individuals, or other systems, not granted access to the resources. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to only authorized parties. Control practices should include formal procedures to ensure that users granted access privileges to automated systems are properly authorized, assigned logon IDs and passwords, and that access privileges are modified or deactivated when employee status changes. Controls should be in place to monitor user access accounts and to detect unauthorized access to IT resources. Appropriate corrective controls should be in effect to mitigate risks of unauthorized access. Overall, monitoring

and evaluation mechanisms should be place to provide assurance that control practices are in effect to address control objectives. Access security controls are also necessary to meet risks associated with the technological environment, including the Internet.

Failure to implement adequate controls regarding system access security could result in unauthorized system access or use. If unauthorized access were gained to the CCS system or its related data files residing on the network's file servers or microcomputer workstations, critical and important data, such as confidential information regarding BHA clients, would be exposed to the risk of unauthorized access, modification, or disclosure.

Recommendation:

We recommend that BHA evaluate the required frequency of password changes and implement a required schedule for users to change passwords periodically. We recommend that the period between password changes not exceed 60 days. In addition, to reinforce user responsibilities regarding access privileges, we recommend that the BHA require all users to sign a formal statement acknowledging the confidentiality of their passwords and commitment to protect the password from unauthorized use and/or disclosure. With respect to authorization of users to access automated systems, we recommend that BHA review all persons currently granted access to the network and CCS application system and ensure that all users have been properly authorized. In addition, we recommend that BHA monitor users with active access privileges to the CCS application and the network.

To strengthen deactivation procedures of logon IDs and passwords, we recommend that BHA coordinate notification by department managers and the Human Resources Department to the MIS Department personnel responsible for access security administration of changes in employee status, such as terminations, extended leaves of absence, or employee transfers. Documented control practices should also help ensure that the MIS Department is notified in a timely manner. Once notified of the change in employment status, the MIS Department should deactivate and/or delete the logon ID and password in a timely manner. Appropriate staff should be instructed regarding compliance with these policies and procedures.

We recommend that documented control practices regarding logon ID and password administration, including authorization and activation of access privileges be included in the Authority's internal control plan. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts.

Auditee's Response:

Regarding system access security, your report states that the BHA needs to improve control practices regarding deactivation/deletion of logon IDs and passwords, required periodic changes to passwords, and policies and procedures.
Your report discusses a finding that 19 out of 344 logon IDs were found to belong to former BHA employees. The report does not make it clear that these logon IDs were only for the CCS system, and that a comparable report for the BHA's NT network showed only one case where a network logon ID was found to belong to a former BHA employee. Without first being validated as an NT user, a person will be unable to gain access to the CCS logon screen.

We agree that our practice regarding deactivation and deletion of logon IDs needs to be refined. The MIS Department has depended on individual managers to notify us when their employees depart. Your report recommends that the BHA's Human Resources Department take on the responsibility of notifying the MIS Department of employee terminations. The BHA has decided that the MIS Department will take this responsibility on itself. MIS will write the necessary report to identify newly terminated employees, and will regularly run these reports. These reports will be used to appropriately disable or delete the effected user accounts on all BHA automated systems.

Your report indicates that BHA user passwords were not being changed in a timely manner. BHA staff have up to three passwords; One for NT network access, one for UNIX access, and one for CCS access. Users can change their own NT and UNIX passwords, but due to the antiquity of the CCS system, they do not have the option of changing their own CCS passwords. The BHA will implement a policy of forcing regular changes to users' NT and UNIX passwords. When the NT network was originally implemented, many BHA staff were new computer users. At that time, we made the decision to simplify their computer usage by not implementing a policy requiring regular password changes. The BHA plans to use the recommendation made in your independent audit report as justification for strengthening our password security policy. Our plan is to initially require password changes every quarter.

Your report indicates that IT policies and procedures have not been approved or compiled in an internal control plan. All IT policies around the use of BHA computer resources are available to all staff who use BHA computers, and can be conveniently accessed from the MIS Department's intranet web page (http://www.bhanet.org/detpages/deptinfo27.html). The policies are all accessible within one or two mouse-clicks of this page. The MIS Help Desk Policy (http://www.bhanet.org/detpages/deptinfo30.html), the User Change Policy (http://www.bhanet.org/detpages/deptinfo35.html), and the Computer Use Policy (http://www.bhanet.org/detpages/deptinfo79.html). When the Computer Use Policy was originally disseminated, it was distributed to all BHA staff, along with a signature page attesting to the fact that the employee

had read & understood the policy. Going forward, the policy and the sign-off has been given to all newly hired BHA staff.

The BHA has the ability to monitor access to its most sensitive CCS systems, via "audit trail" tracking built into sensitive CCS databases. This audit function notes the user, time, and date these records were last updated. The BHA's proxy server monitors all web pages accessed by BHA users, logging the user, date, time, and page visited.

Auditor's Reply:

We are pleased that BHA will strengthen control practices regarding the deactivation of access privileges through deactivation/deletion of logon IDs and passwords. We acknowledge that a user must be authenticated to the network before accessing the CCS system and that BHA has audit tracking capabilities to monitor update of CCS records. While the latter may serve as a good corrective control, or be used in conjunction with another mechanism as a detective control, on its own it will not identify unauthorized access. Should a logon ID and password remain active and available for use subsequent to an employee termination, the risk remains that a user may gain unauthorized access to CCS records, including confidential client information. We acknowledge BHA's management decision to grant the MIS Department the security responsibility regarding the deactivation of logon IDs and passwords for staff who have terminated employment. However, we reiterate that department managers still need to be involved regarding timely notification requiring modification or deactivation of logon IDs and passwords to ensure that all employment possibilities, such as job transfers or leaves of absence, are addressed.

We agree with BHA's decision to improve password security by requiring that passwords be changed on a scheduled basis. We suggest that BHA reevaluate the three month interval at least annually to determine whether a shortened time frame would be more appropriate.

We acknowledge that BHA had documented control practices regarding use of IT resources, data confidentiality, and password formation use and had placed these polices on-line for BHA staff with access privileges to the automated systems. To strengthen policies and procedures, we reiterate that BHA should review security policies for IT-related issues, such as logon ID and password administration for the CCS system and the network for completeness. Based on the review, BHA should incorporate or cross-reference the security policies and practices in the Authority's internal control plan. The policies and procedures can be made available in hardcopy form and/or on-line.

Subsequent to the completion of our fieldwork, BHA provided us with the Computer Use Policy and a policy sign-off form dated March 1, 2001. The sign-off form included a statement that the employee who signs the form had read the policy. We are pleased that BHA has

developed a Computer Use Policy and requires that the policy be read and that users sign a formal security agreement. To strengthen controls, we recommend that BHA ensure that all users with current access privileges sign the security statement. Further, we recommend that the security statement include language indicating that the employee has both read and understood the Computer Use Policy.

2. Business Continuity Planning

Our audit disclosed that although the BHA satellite offices that we reviewed had developed informal procedures to address recovery strategies regarding certain mission-critical and essential operations, the BHA needed to strengthen controls regarding business continuity planning. We acknowledge that the Authority was aware of the need for business continuity planning and had outsourced the development of a disaster recovery plan. However, at the time of our audit, we determined that a business continuity plan had not been approved or implemented. In addition, we determined that BHA had assessed, but not documented, potential disruptions to its network's file servers and microcomputer systems and the potential impact of a loss of processing capability on the Authority's mission-critical and essential business functions. Our audit confirmed that BHA had provided adequate on-site and off-site storage of backup copies of data files and application software residing on its file servers. In addition, we determined that BHA maintained adequate control procedures, including sign-out/sign-in logs for the storage and return of critical backup media from the off-site location.

We determined that BHA had not yet implemented or tested a formal business continuity plan for a timely, post-disaster restoration of mission-critical and essential administrative transactions processed by the Creative Computer Solutions (CCS) system, the Authority's primary application system. Our audit indicated that the Amory Street and Mary Ellen McCormack development sites had informally designated alternate processing sites to perform mission-critical functions, such as entering payroll data. However, the Authority had not formally designated or tested alternate processing sites for its central office in Boston or business offices at development sites should a disaster render IT systems at any office unusable or inaccessible. In addition, the Authority had not documented instructions regarding the replacement of the file servers and microcomputer workstations should the equipment be rendered inoperable or instructions, (e.g., personnel to contact, timetable to implement user area plans) for the staff to follow should the hardware fail to function.

Given the absence of comprehensive recovery plans and the dependence of BHA on the CCS application system to perform its mission-critical business functions, a significant disaster impacting the Authority's automated systems, such as the file server on which the CCS

application database resides, for an extended period would adversely affect the BHA's ability to regain mission-critical IT operations, including processing tenant applications and work orders and accounting for rent monies as well as other functions.

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

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, and that determinations of system criticality and the risks and exposures associated with the systems are correct. In addition, appropriate data processing and user area plans should be developed based on the relative criticality and importance of systems, and adequate resources should be made available. The Authority should strengthen its risk analysis of automated systems by including all mission-critical and essential applications processed on the network's file servers and microcomputer-based systems and should clearly understand the impact of lost or reduced processing capabilities for each system. The risk analysis should identify the relevant threats that could damage the systems, the likelihood of the threat and frequency of occurrence, and the cost of recovering the systems.

Recommendation:

We recommend that the BHA strengthen current procedures to provide reasonable assurance that mission-critical and essential business operations would be regained in a timely manner should IT operations be rendered inoperable or inaccessible. Based on the review and evaluation of the criticality of BHA's automated systems, specifically the Creative Computer Solutions application system, the Authority should ensure that the business continuity plan includes the designation of alternate processing sites, required user area plans, communication components, and instructions regarding replacement of file servers and other IT resource components." The plan should also include a listing of contact information of key personnel and documented

scenarios regarding minor to major loss of systems and appropriate responses to each situation. Business continuity requirements should be assessed on an annual basis or upon major changes to user requirements regarding the automated systems.

With respect to the development of the disaster recovery and contingency plan, BHA should document specific deliverables with dates for completion of portions of the plan. All work should be reviewed and approved by BHA management before payments are made to the consultants.

The business continuity plan should document the Authority's recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. At a minimum, the BHA should develop documented user area plans for its business office to continue its operations should the file servers or microcomputer systems be unavailable. We further recommend that the business continuity plan be tested, then periodically reviewed and updated when needed to provide reasonable assurance that it is current, accurate, and complete. The BHA staff should be trained in the execution of the plan under emergency conditions. The completed plan should be distributed to all appropriate staff members.

Auditee's Response:

> *Your report states that the BHA had not approved or implemented a business continuity plan as of the time of your audit. The BHA had procured the services of a disaster-recovery consultant, and made substantial progress preparing a plan that identified the BHA's critical systems and outlined plans for disaster recovery for each of them. Before the plan could be completed, the vendor filed for bankruptcy. While the BHA has a well-conceived draft plan and has been able to take steps to attend to the most pressing needs addressed in this draft plan, that plan is not complete. The draft plan makes recommendations about alternate data processing sites and sources for replacement hardware components, and identifies strategies for processes at different levels of criticality. We concur that the issue of business continuity planning extends beyond the scope of IT to embrace the entire organization. At this point, the BHA has begun the project to replace our CCS database system, and intends to address many of the issues highlighted in that draft plan in the specifications for the replacement system*

Auditor's Reply:

We acknowledge that BHA has made significant efforts to address the development of a business continuity plan and that the bankruptcy of the consultant had impeded the completion of the plan. We are pleased that BHA will be addressing important control practices regarding business continuity planning in conjunction with the replacement of the CCS database system. We will review business continuity planning during our next scheduled audit.

3. Inventory Control over IT-related Resources

Our audit indicated that BHA could not provide reasonable assurance that the system of record could be relied on to properly account for IT-related resources with a listed value of $1.3 million as of April 26, 2001. We determined that significant items of computer equipment, valued in excess of $380,000, had not been listed on the inventory record, and equipment designated as surplus property had not been deleted.

We found that BHA did not:

- maintain a current, accurate, and complete inventory record for IT-related resources, including computer equipment and software;
- implement documented procedures to account for laptop computers;
- demonstrate that an annual physical inventory and reconciliation of IT-related assets had been performed, as required by the Massachusetts Department of Housing and Community Development (DHCD); and
- properly account for IT-related assets designated as surplus property.

Our audit disclosed that BHA was not conducting an annual physical inventory and reconciliation for its IT-related resources for fiscal years 2000 and 2001 as required by the DHCD "Accounting Manual" for local housing authorities. According to BHA management, the last physical inventory and reconciliation had been conducted in July 1999. We determined that although computer equipment at the central office and Amory Street and Mary Ellen McCormack development sites had been tagged with identification numbers, the IT-related inventory record as of April 26, 2001 was not current, accurate, or complete. We found that of eight file servers purchased from 1997 through 2001, six servers valued at $91,000 were not recorded on the inventory record. One of our audit tests indicated that 272 microcomputers purchased during the 1999 fiscal year and valued at $291,040 were not recorded on the inventory record.

During our audit, we conducted tests of inventory records at two development sites. We found that of nine microcomputer systems listed on the inventory record, only eight computers could be located in the business offices at the Mary Ellen McCormack development site. According to BHA staff, the ninth computer had been moved to a different site; however, the new location had not been listed on the inventory record. Of the eight computers, we determined that only two microcomputers corresponded to the description listed on the inventory record. In addition, for the Amory Street development site, we were unable to confirm a sample of 23 (39%) hardware items to the 59 items of computer equipment listed on the inventory record for that site. Of the 23 items selected for review, only two microcomputers were properly listed on the inventory record; four computers were listed on the inventory record, but were recorded as being

located at the central office in Boston; and, 17 hardware items installed at the site were not recorded on the inventory record.

Our audit revealed that BHA was not properly accounting for computer equipment designated as surplus property. Of the 493 microcomputer systems listed on the inventory record, we could not determine the total number of items or specific items of computer equipment that had been disposed of, but not deleted from the inventory record since the purchase and installation of 272 microcomputer systems in 1999. We found that a vendor invoice dated December 29, 2000, in the amount of $2,160, indicated that computer equipment had been removed from BHA offices. However, neither the invoice nor the "Disposed Computer Equipment Fixed Assets Report," dated April 25, 2001, indicated the total number or specific items of computer equipment designated as surplus property and removed from BHA offices for disposal.

Our audit disclosed that BHA was not properly accounting for its laptop computers. We found that although 34 laptops were recorded on the inventory record, sign-out/sign-in control procedures, including required staff signatures and supervisory approval and written instructions for the distribution and return of laptops, had not been implemented. Because of the lack of formal documentation, there was no record of which staff had received a laptop computer or the date received or returned. As a result, at the time of our audit, BHA could not provide a current, accurate, and complete record of the status of laptop computers. Regarding software inventory, we found that the inventory record did not include a list of application software or purchase costs. However, licenses for CCS modules and business applications were maintained at BHA's central office.

At the time of our audit, we determined that BHA had designated a staff member to maintain and update the inventory record and that the inventory record contained adequate "data fields," such as tag number, manufacturer's number, location, and cost.

Good management practices and generally accepted computer industry standards advocate that a perpetual inventory be maintained for all IT-related resources, including software, and that sufficient polices and procedures be in effect to ensure the integrity of the inventory record. The DHCD "Accounting Manual," last updated October 1, 2000, requires that all local housing authorities properly record fixed assets and associated costs and perform an annual physical inventory and reconciliation and make any necessary adjustments. Further, prudent business practices advocate that the software inventory be used to help prevent unnecessary software expenditures, theft, unauthorized installation of software, and software copyright infringements.

The lack of a current, accurate, and complete inventory record for IT-related resources hinders the BHA's ability to monitor IT-related equipment, such as file servers and

microcomputer system and software and to detect lost or stolen items. Further, without an accurate and complete inventory record, information provided by BHA to DHCD, its oversight agency, or other parties, through financial records, might be incorrect.

Recommendation:

We recommend that BHA review DHCD's "Accounting Manual" regarding inventory control procedures for property and equipment, including IT-related assets. BHA should perform a physical inventory of IT-related resources at the central office and development sites. Based on the results of the physical inventory, BHA should correct the inventory record to reflect computer equipment purchased or deleted since the last reconciliation conducted in 1999. Further, we recommend that BHA perform an annual physical inventory and reconciliation in compliance with DHCD regulations. We recommend that BHA develop a software inventory record, including "data fields," such as version number and cost. Regarding surplus property, BHA should review its inventory records and promptly delete all IT-related equipment that has been disposed of.

We recommend that BHA develop control procedures regarding the distribution and return of laptop computers. The procedures should include sign-out/sign-in logs that include staff signatures, supervisory approvals, and a statement regarding appropriate use of laptops.

Auditee's Response:

> *Your report indicates that the BHA could not provide reasonable assurances that the CCS inventory database could be relied on to account for IT fixed assets. The BHA concurs with this finding. The BHA will conduct a physical inventory and reconcile its IT resources, including both hardware and software, with the records maintained in the CCS inventory database. Further, we will strengthen procedures to ensure that newly acquired equipment is recorded in the CCS inventory database, and that equipment being disposed of is removed from the CCS inventory database. The BHA will also institute a sign-in/sign-out procedure to account for the location of all BHA laptop PCs. This physical inventory will be conducted annually on an ongoing basis.*

Auditor's Reply:

We agree with BHA's decision to strengthen control practices regarding inventory control over IT-related resources, such as conducting an annual physical inventory and reconciliation and recording computer equipment on the inventory record and removing items designated as surplus in a timely manner. We also concur with the implementation of sign-out/sign-in logs to improve the accounting for laptop computers. We will review inventory control over IT-related assets at our next scheduled audit.

Appendix A
PRIOR AUDIT RESULTS

Prior Audit Results Resolved

1. Inadequate Accountability for Gasoline Distributed from the Central Stores Facility

Our prior audit indicated that BHA did not maintain adequate controls for gasoline distributed from its central stores facility. Specifically, we determined that purchase requisitions were not reconciled with gasoline tank readings, supervisory approvals were not required for gasoline requisitions, and adequate controls were not in place regarding gasoline tank reading keys used to withdraw gasoline from the tanks.

Our current audit disclosed that in December 1998, BHA had implemented new procedures for purchasing gasoline. We determined that BHA was obtaining its fuel through a contract with a vendor operating under the Massachusetts Operational Services Division (OSD) statewide procurement program and the City of Boston's fuel depot in South Boston. Under both programs, the BHA issues fuel cards with personal identification numbers (PIN) to staff. The BHA's Department of Procurement and Finance Department review the monthly invoices submitted to the Authority. The invoices include "data fields," such as driver's name, PIN, vehicle number, purchase date, location, and cost.

We believe that BHA has implemented sufficient controls to monitor and manage gasoline purchases for the Authority.

2. Lack of Reimbursement for Non-Business Use of Cellular Phones

Our prior audit disclosed that BHA had expended an estimated $1,875 for non-business-related cellular telephone calls made to outside Boston and out-of-state destinations during the 1998 fiscal year. Further, there was no evidence that the cost of these non-business calls had been reimbursed. BHA's "Cellular Phone Policy" requires that cell phones be used only for Authority business and that the cost of personal calls be reimbursed to the Authority.

Our current audit revealed that, during the 1999 fiscal year, BHA had implemented new control procedures for cellular telephone services. BHA consolidated cellular telephone services into a contract with a vendor through the OSD statewide procurement program, adopted a "minutes per month" plan to control additional charges, distributed full cell phone features to only senior staff, and converted approximately 100 telephones to radio features only. In addition, a different purchase order number was assigned to invoices for each region to enable regional managers to review and sign invoices before they are submitted for payment.

Our audit tests indicated that invoices included sufficient information, such as user name, type of telephone call, and date, time, and amount of call to monitor cellular telephone call charges and that the invoices included evidence of supervisory review and approval. In addition, we found that invoices noted reimbursement for non-business calls, corresponding checks for the charges were payable to the BHA, and bank deposit slips indicated that payment for the calls had been deposited in the Authority's account.

We believe that BHA has implemented sufficient control procedures to monitor cellular telephone calls.

3. Availability of Documentation for the Drug Elimination Program Needs Improvement

Our prior audit disclosed that BHA could not provide invoices and supporting documentation for payments made for the Drug Elimination Program funded through the United States Housing and Urban Development grants during the 1998 fiscal year in a timely manner. These grant monies were awarded to the BHA to improve efforts to combat drug-related crime at the development sites.

During our current audit, the BHA provided paid invoices and supporting documentation in a timely manner for selected payments made during the month of January 2001.

Our audit indicated that the delays providing information for review noted in the prior audit have been corrected.

Appendix B
Summary of Internal Control Practices
Boston Housing Authority
As of November 30, 2001

Pg. ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
12, 14	System Access Security	Provide reasonable assurance that only authorized users are granted system access to the automated systems	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	Insufficient	Yes	Adequate
12, 22	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safe-guarded, accounted for in the inventory record, and reported on, when appro-priate, to oversight entity	Maintenance of an up-to-date inventory record; hardware tagged with ID tags; annual physical inventory and reconciliation performed	None	Yes	Adequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.
None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:

Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Appendix B
Summary of Internal Control Practices
Boston Housing Authority
As of November 30, 2001

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
10	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, computer rooms, microcomputer systems, and client records in hardcopy form so that, loss or damage is prevented	Control over access to offices, computer rooms, file servers, and microcomputer systems, designated facilities manager, intrusion devices, locked doors, foot patrols	In Effect	No	N/A
11	Environmental Protection	Provide reasonable assurance that IT-related resources adequately protected from loss or damage	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures	In Effect	Yes	Adequate, for emergency procedures
13, 19	Business Continuity Planning	Provide reasonable assurance that BHA can restore essential and mission-critical functions in a timely manner should file servers and microcomputer systems be rendered inoperable.	Current, formal, tested business continuity plan; periodic review and modification of plan; plan implemented, distributed, and staff trained in its use	Insufficient	No	N/A
13, 19	On-site storage	Provide reasonable assurance that magnetic media are available should computer systems be rendered inoperable	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is in a separate on-site location	In Effect	Yes	Adequate
13, 19	Off-site storage	Provide reasonable assurance that critical and important media are available should computer systems be rendered inoperable	Same as above. Storage area in a separate off-site location	In Effect	Yes	Adequate