A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2002-0006-4T

INDEPENDENT STATE AUDITOR'S REPORT ON EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES

July 1, 2001 through March 6, 2002

OFFICIAL AUDIT REPORT
JULY 23, 2003

2002-0006-4T

TABLE OF CONTENTS

INTRODUCTION

The Executive Office of Health and Human Services (hereinafter referred to as EOHHS, Executive Office, or Office), a cabinet-level agency, was established in 1971 and is organized under Chapter 6A, Section 2, of the Massachusetts General Laws and operates within the purview of the Governor of the Commonwealth. Chapter 6A, Section 16, as amended by Chapter 177, Section 6 of the Acts of 2001, placed 15 state agencies, including the Departments of Mental Health, Mental Retardation, Medical Assistance and Social Services within the Executive Office. (See Appendix B, page 25, for a complete list of EOHHS agencies.) At the time of our audit, these state agencies employed approximately 28,500 staff. The Secretary of EOHHS, appointed by the Governor, served as the Chief Executive Officer and was the Governor's chief policy advisor regarding all health and human service issues. In addition to the Secretary, the Office is comprised of 42 staff, including two assistant secretaries and two undersecretaries. According to the EOHHS website, the Secretariat oversees the expenditure of an annual budget totaling approximately $8.9 billion for the agencies placed within the Office. The EOHHS administrative office is located in Boston.

The EOHHS primary mission is “to provide effective leadership and oversight in the delivery of health and human services that promote health and safety, independence, and quality of life for individuals, families and communities throughout the Commonwealth of Massachusetts.” According to management, the Executive Office provides advocacy for clients of the 15 agencies within the Secretariat’s jurisdiction.

At the time of our audit, the EOHHS computer operations were supported by two file servers and 49 microcomputer workstations configured in a local area network (LAN). The file servers were connected through a wide area network (WAN) to the Information Technology Division (ITD) mainframe, which provides connectivity for access to the Web-based Human Resource Compensation Management System (HR/CMS) and to the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth’s accounting system. The Executive Office performs its administrative functions using business-related applications, such as word processing and other office suite products.

During our audit, EOHHS was implementing the Massachusetts Confidential Access to Resources through an Electronic Storehouse (MassCARES), a Web-based system which has as its objective the sharing of client information among the Office’s 15 agencies and the ongoing collection of data from selected Executive Office agencies. Further, MassCARES enables citizens to access information regarding approximately 23,500 health and human service providers within the Commonwealth. An eligibility wizard will allow citizens to determine eligibility for a variety of programs and services. EOHHS plans to develop additional tools, such as case monitoring and client service targeting.

Our Office's examination focused on selected general controls, such as physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From January 22, 2002 through March 6, 2002, we performed an audit of selected information technology (IT) related controls at the Executive Office of Health and Human Services (EOHHS) for the period covering July 1, 2001 through March 6, 2002. The scope of our audit included an examination of control practices, procedures, and devices regarding physical security and environmental protection over and within the administrative office and the room housing the file servers at EOHHS. We reviewed and evaluated system access security for the Secretariat's automated systems, including the file servers and microcomputer workstations. In addition, we examined inventory control practices for computer equipment and software.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the automated systems. With respect to the restoration of normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning, including provisions for on-site and off-site storage of backup copies of magnetic media. We evaluated physical security and environmental protection controls over backup media stored on-site. We reviewed procedures for generating and transferring backup copies of essential magnetic media to an off-site storage location.

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 that system information was sufficiently protected against unauthorized disclosure, change, or deletion. We sought to determine whether adequate physical security and environmental protection controls over IT resources were in place and in effect in order to restrict access to only authorized users so that unauthorized use, damage, or loss of IT resources would be prevented. In addition, we sought to determine whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to the business-related applications and applications residing on the network and that procedures were in place to prevent unauthorized access to automated systems. Another objective was to review and evaluate control practices regarding accounting for IT-related resources, including computer equipment and software. 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 automated system be unavailable for an extended period. Further, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of the EOHHS mission and business objectives. Through pre-audit interviews with senior managers and staff and reviews of documents, such as descriptions of the Executive Office's organization and operations and the Office's statutory authority, we gained an understanding of the primary business functions supported by the automated systems. We reviewed the EOHHS role regarding the management, direction, and control over the IT-related operations of the 15 agencies placed within the Executive Office. We documented the significant functions and activities supported by the Office's automated systems and reviewed automated functions related to operations designated as mission-critical or essential.

We reviewed and evaluated selected control practices regarding the organization and management of IT operations at the Boston office, such as a current Office organization chart and job descriptions for IT managers and staff. We inspected the administrative offices in Boston, including the file server room, reviewed relevant documents, such as the network configuration, and performed selected preliminary audit tests. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, and generally accepted control objectives for IT operations and security.

We interviewed EOHHS management to discuss internal controls regarding physical security and environmental protection over and within the file server room, microcomputer workstations installed throughout the administrative office, and on-site and off-site storage of mission-critical magnetic media. Regarding inventory controls over IT-related resources, we determined the role of the Executive Office regarding accounting for computer-related equipment and software. We reviewed procedures used by EOHHS for daily backup of the database and transport of the magnetic media for storage at an off-site location.

To determine whether physical access over IT-related resources, including computer-related equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the administrative office. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with senior management and staff. To determine whether adequate controls were in effect to prevent and

detect unauthorized access to offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, the presence of a receptionist at the entrance point, and whether visitors were required to sign in/out.

We reviewed access control procedures, such as the list of staff authorized to access the file server room and key management regarding door locks to the administrative office's entrance, the file server room, and other restricted areas within the administrative office. We determined whether the Office maintained incident report logs to identify security-related events, such as unauthorized entry attempts, threatening phone calls, or thefts of computer-related equipment.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems installed in the administrative office and file server room 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 only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in the file server room. Further, we reviewed control procedures to prevent water damage to automated systems, client records in hardcopy form, and magnetic backup media stored on-site.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer workstations. To determine whether Executive Office control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the Chief Information Officer (CIO) and the Network Manager responsible for management of the network and evaluated selected access controls to the automated systems. In conjunction with our review of network security practices, we reviewed control procedures regarding dial-in procedures to the network.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the Network Manager responsible for access to the file servers and microcomputer workstations on which the Office's application systems operate. In addition, we reviewed control practices used to assign staff access to the application programs and data files. To determine whether controls in place were adequate to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and

deactivating access to application software and related data files. Because EOHHS had not maintained sufficient documentation regarding authorization to access automated systems, we could not confirm whether access privileges to the automated systems were granted to only authorized users. To determine whether all users with active privileges were current employees, we obtained the list of individuals granted access privileges to the business-related applications and compared 42 (100%) users with active access privileges to the Office's personnel roster of current employees. Further, we determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed inventory control procedures for computer-related equipment and software with the CIO and the network manager. In conjunction with our audit, we reviewed formal policies and procedures promulgated by Office of the Massachusetts State Comptroller (OSC) regarding inventory control. We sought to determine whether the Executive Office had complied with these documented control practices. We obtained the inventory record dated February 20, 2002. We determined whether computer equipment installed at the administrative office 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 state identification number, manufacturer's model number, serial number, location, and cost were listed on the record. Further, we reviewed the adequacy of procedures used by EOHHS to dispose of surplus equipment. We also reviewed control practices regarding safeguarding and accounting for the two-laptop computers. We determined whether a software inventory record had been developed.

To determine whether the IT-related inventory record, as of February 20, 2002, was current, accurate, and complete, we attempted to confirm all pieces of equipment recorded on the inventory list, including file servers, microcomputer workstations, printers, and laptop computers to the actual computer equipment installed at the administrative office. Because computer equipment had not been tagged with state identification numbers, we compared serial numbers attached to the computer equipment to the corresponding numbers listed on the IT inventory record. We determined whether the serial numbers were accurately recorded on the inventory record. Further, we traced 100% of computer equipment installed at the administrative office to the items listed on the inventory record. Because the Office had not purchased computer equipment or software since the 1999 fiscal year, we did not trace purchase documentation to the inventory record and to the actual equipment on hand.

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 and the microcomputer workstations be unavailable for an extended period. We

interviewed the CIO 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 reviewed and evaluated procedures in place to resume normal business functions should the file servers or the microcomputer workstations be rendered inoperable.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed EOHHS management responsible for generating backup copies of magnetic media for administrative work processed at the Office. Further, we reviewed the adequacy of provisions for on-site storage of backup copies of mission-critical and essential magnetic media at the administrative office. We did not review the off-site storage location for backup copies. We did not review ITD backup procedures for transactions processed through MMARS and HR/CMS.

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 CONCLUSION

Based on our audit, we found that adequate physical security and environmental protection controls were in place and in effect at the Executive Office of Health and Human Services (EOHHS) to provide reasonable assurance that IT-related resources were properly safeguarded and protected from damage or loss. Our audit indicated that sufficient control practices were not in place to provide reasonable assurance that the IT-related resources, including computer equipment and software, were properly accounted for in Executive Office records. With respect to system access security, we determined that, although EOHHS had implemented certain informal procedures regarding granting and recording of access privileges and deactivation of logon IDs and passwords, documentation of these stated control practices needed to be improved.

Regarding availability of systems, we determined that control practices needed to be strengthened to provide reasonable assurance that normal business operations could be resumed at the Executive Office in a timely manner should the file servers or microcomputer workstations be unavailable for an extended period. Further, we found that, at the close of our audit, control practices regarding on-site and off-site storage of backup copies of magnetic media for administrative work processed at EOHHS were adequate.

Our review of internal controls indicated that the Executive Office was aware of the need for internal controls and had a defined organizational structure for the Office, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for information technology staff. With respect to appropriate use of information technology, we determined that formal policies and procedures needed to be developed regarding physical security, environmental protection, system access security, and inventory control over IT-related resources. Failure to adequately document required control procedures may result in important controls not being implemented or exercised. In addition, when controls are not documented, the nature and extent of operative controls cannot be referred to or reviewed. (See Summary of Internal Control Practices, page 22.)

Our audit disclosed that appropriate physical security controls had been implemented over and within the state office building housing the Executive Office. These controls included on-duty State Police officers, security devices, such as stand-alone and hand-held metal detectors used to screen persons and personal items, and restricted access to the building after normal business hours. With respect to the EOHHS business office, we determined that there was one entrance/exit to the office, a receptionist was located at the front entrance, and keys to the front door and business offices were assigned to appropriate staff. According to Office management, the entrance door was locked after normal business hours. Our audit indicated that the file server room was located in a non-public area that could not be accessed from outside the building, the door to the room was locked at all times, and access to the room was restricted to

two staff from IT operations via a punch keypad system. To strengthen physical security controls, we recommend that the Executive Office designate a staff person responsible for physical access security and maintain a list of staff authorized to access IT-related resources.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply were in place in the building housing the Executive Office to help prevent damage to, or loss of, IT-related resources. Our audit disclosed that the file server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We found that an uninterruptible power system (UPS) was in place to prevent sudden loss of data. To improve environmental protection controls, we recommend that hand-held fire extinguishers be located within the file server room. In addition, we recommend that the Office post evacuation and emergency procedures in the file server room and that staff be trained in their use.

Our tests of access security to the file servers and microcomputer workstations indicated that control practices needed to be improved to provide reasonable assurance that access to systems, data, and programs is restricted to only authorized users and to safeguard information against unauthorized use, disclosure, or modification. We found that, although the Executive Office had developed appropriate procedures regarding authorization and recording of access privileges to automated systems and activation of logon IDs and passwords, these control practices had not been documented. Further, EOHHS could not provide sufficient documentation to confirm that all active users had been authorized to access automated systems. Regarding procedures to deactivate access privileges, we found that informal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. Audit tests of access security that compared 49 (100%) users with active privileges to the Office's personnel roster of current employees indicated that all users were current employees.

According to EOHHS management, the Office has complied with control procedures for logon ID and password administration required by the Executive Office for Administration and Finance's (EOAF) Information Technology Division (ITD). These procedures include password formation and use, length of passwords, and frequency of password change. Further, management stated that staff are required to change their passwords in compliance with ITD's schedule for password changes.

Our audit revealed significant deficiencies regarding the accounting for IT-related resources at the Executive Office. We determined that at the time of our audit, EOHHS did not maintain a current, accurate, and complete inventory record for computer equipment and software. We determined that the Executive Office had not purchased IT resources since the 1999 fiscal year. Because the Office could not provide purchase documentation for IT resources purchased prior to 1999, we could not determine whether all equipment purchased was located at EOHHS and properly listed on the inventory record.

We believe that the Executive Office had not obtained sufficient understanding of statutory requirements, Office of State Comptroller (OSC) guidelines, or good management practices regarding asset-related management and control. We found that EOHHS had not complied with the Internal Control Act, Chapter 647 of the Acts of 1989, the OSC's "Internal Control Guide for Departments," promulgated in 1996, and the "MMARS Fixed Asset Subsystem Policy Manual and User Guide," as of August 2001. We determined that the IT-related inventory listing did not include appropriate fields, such as state identification number, cost, date of acquisition, or date of last update. Because EOHHS had not maintained cost information, we were unable to determine aggregate costs of equipment and software installed at the Executive Office. We found that EOHHS had not complied with OSC requirements regarding tagging of IT-related equipment. Further, our audit indicated that surplus property was not properly accounted for.

We believe that EOHHS should obtain a comprehensive understanding of fixed-asset management and control, develop formal polices and procedures, comply with OSC internal control guidelines, and maintain current, accurate, and complete inventory records. EOHHS should conduct a physical inventory of IT-related equipment. Based on the results, the Office should develop a current, accurate, and complete inventory record. We recommend that the Executive Office designate staff who will be responsible for maintaining, updating, and reconciling the inventory record; and ensure that computer-related equipment is tagged with state identification numbers. An annual physical inventory of the Office's inventory record, including IT resources, should be performed according to OSC guidelines.

We found that EOHHS had not developed a comprehensive business continuity plan that outlined a sound strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. Further, the Executive Office had not documented procedures to provide reasonable assurance that normal business operations could be resumed should IT equipment become damaged, inoperable, or inaccessible. We acknowledge that, in conjunction with its advocacy activities, the Office's major use of its automated systems was to process correspondence regarding clients of the 15 agencies under its purview. However, we believe that the Office should, at a minimum, document user area plans and designate an alternate processing site where daily administrative work could be restored.

Our audit indicated that control procedures regarding backup of magnetic media needed to be strengthened. We determined that EOHHS had implemented procedures for generating backup copies of magnetic media. Schedules for performing backups and descriptions of data files and software backed up had been documented. However, although documentation was in place indicating which backup tapes were stored off-site, no logs were maintained demonstrating the authorized schedule for the transport and return of backup copies. In addition, we found that physical security and environmental protection over the on-site storage location needed to be improved. Our audit revealed that backup tapes were being

stored in the file server room. As a result, should a disaster occur within the room, backup tapes could be damaged or destroyed. We recommend that the Office store backup tapes in a fireproof safe within the file server room or, alternatively, relocate media to a more physically secure and environmentally-protected on-site location. We did not visit the storage facility housing off-site backup copies of computer-related media.

Auditee's Response:

General Lack of Documentation

. . . There is a general finding of lack of documentation of IT policies and procedures; a finding this office would not argue with. One could argue that an office historically constituted of thirty-eight staff members and one IT person is manageable without much of the formal documentation that a larger office would require. However, as the role of IT within the secretariat office increases, we recognize the validity of this finding and the need for steps to address it.

Physical Access Security

Another issue you raise is the designation of a staff person to be in charge of physical access security. That role has been carried by the network administrator although not in an official capacity. We expect to formally address this matter as part of HIPAA security requirements and the designation of a departmental Security Officer.

Server Room Environment

You make several recommendations as to the server room environment and some have been accomplished. You recommend the installation of a fire extinguisher and the installation of a fireproof safe to protect backup media stored locally. Both of these were accomplished shortly after your first visits. Further, evacuation routes are now mapped and attached to the server room door. As the report correctly states, only two staff have access to the server room and both have been instructed in the evacuation procedures so this item is also fully addressed. Although not mentioned in your report, we have begun the process of upgrading the air conditioning in that room to support the larger server environment that we expect the Office for Children to build over the next years. I would expect that the Executive Office will increasingly locate our environment in the Chelsea MITC data center as the consolidation of HHS IT services is undertaken over the next three years.

Business Continuity Policy

> *Again, the historically modest size of the Executive Office and absence of client and transaction systems has mitigated historic risks in this area. But we are sensitized to the need for improvements in this area going forward. We have briefed systems staff on current protocols for state government official actions in the case of major or catastrophic emergency events, and are working to find alternative - and more secure - data center space for our key systems assets.*
>
> *This should provide a brief status on several of the points raised in this audit. We stand committed to correcting any issues that the report has raised, and look forward to modeling exemplary compliance . . .*

Auditor's Reply:

We are pleased that EOHHS will develop formal IT-related policies and procedures, particularly, as indicated by management, of the increasing importance of information technology within the Executive Office. We agree with management's efforts to strengthen physical security controls by designating a staff person to be in charge of physical security. We are pleased that the Office has taken corrective action to improve environmental protection by installing a fire extinguisher in the file server room, posting evacuation routes, and training IT staff in evacuation procedures. We agree with management's decision to improve temperature controls in the file server room.

We concur with management's efforts to improve business continuity planning and to strengthen controls over on-site storage by locating backup copies of magnetic media in a fireproof safe. We will review physical security and environmental controls at our next scheduled audit.

AUDIT RESULTS

1. Inventory Control over IT-related Resources

Our audit disclosed that inventory control practices over IT-related resources, including computer equipment and software, needed to be strengthened. We determined that, although physical security and environmental protection over automated systems at the Executive Office were adequate, EOHHS could not provide reasonable assurance that sufficient control practices were in place and in effect to properly account for and, if appropriate, report on IT-related resources. We found significant deficiencies regarding the Office's system of record for IT-related resources, as of February 20, 2002.

We determined that EOHHS did not:

- have formal policies and procedures in place regarding fixed-asset management, requiring tagging of computer-related equipment; conducting an annual physical inventory and reconciliation; maintaining a current, accurate and complete inventory record; and accounting for surplus property;
- maintain a current, accurate, and complete inventory record for IT-related resources, including computer-related equipment and software;
- include appropriate "data fields" in the inventory record, such as state identification number, location, date of acquisition, installation date, and cost;
- comply with Office of the State Comptroller's (OSC) requirements regarding tagging of equipment and maintaining consistent tagging procedures;
- demonstrate that an annual physical inventory and reconciliation of IT-related resources had been performed;
- comply with the Internal Control Act, Chapter 647 of 1989; and,
- comply with the OSC's asset-related internal control requirements, such as the "Internal Control Guide for Departments," as of February 1996 and the "MMARS Fixed Asset Subsystem Policy Manual and User Guide," as of August 2001.

a. Record-Keeping Practices

We determined that, contrary to Office of the State Comptroller's written internal control guidelines for fixed-asset management, promulgated under the authority of the Internal Control Act of the Acts of 1989, EOHHS had not performed a periodic physical inventory and reconciliation; complied with all requirements for affixing state identification numbers on computer equipment; or properly recorded costs of computer-related equipment on the inventory record. Our audit indicated that the IT inventory record, as of February 20, 2002, lacked integrity, and, as a result, could not be relied upon as a current, accurate, complete, and valid representation of the Executive Office's IT-related equipment. We found that 38 (38%) of 99 items of computer-related equipment installed at EOHHS were not listed on the inventory record. These items included two file servers, one printer/scanner, one microcomputer workstation, and

an additional 34-microcomputer workstations no longer used by the Secretariat. Further, we found that a software inventory record had not been developed.

We determined that, contrary to the requirements of the OSC's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," EOHHS had not properly accounted for all fixed-asset transactions, including the proper recording and reconciliation of Generally Accepted Accounting Principles (GAAP) Fixed Assets and Non-GAAP Assets. GAAP Fixed Assets are comprised, in part, of assets with a useful life of one year or more. With respect to equipment, computer software, and all electrical and computer components, asset costs must be in excess of $50,000. The OSC requires that all Departments maintain an inventory of Non-GAAP Fixed Assets on either the MMARS Fixed Asset Subsystem or in an in-house system. Non-GAAP Fixed Assets are defined as assets, including computer software and electrical and computer components with a historical cost between $1,000 and $49,999.

With respect to the composition of the inventory record, we determined that important "data fields," such as state identification number, acquisition date, installation date, location, and cost were not listed on the inventory record. Our audit indicated that a serial number was the only "data field" entered into the inventory record for computer equipment and manufacturer's model number and serial numbers were the only "data fields" listed on the record for printers. The lack of sufficient information could hamper EOHHS's ability to properly identify and monitor IT-related resources and to confirm that all equipment obtained by the Executive Office was listed on the record and was on hand.

Due to the lack of cost figures listed on the 2002 inventory record and the Secretariat's inability to provide sufficient documentation regarding IT purchases prior to the 1999 fiscal year, we could not determine the total valuation for IT-related resources. According to EOHHS management, the Office had not purchased computer-related equipment since the 1999 fiscal year.

b. Tagging of IT-related Resources

Our audit revealed that contrary to Office of the State Comptroller's requirements regarding the permanent tagging of property and equipment with a state identification number, EOHHS had not tagged computer-related equipment with a permanent tag number. The OSC's "Internal Control Guide for Departments," as of February 1996, states that, "all equipment should have an individual property control identification number, a complete inventory of all property should exist, noting the current location, and all inventoried equipment should be properly recorded and valued at historical cost." Further, the MMARS Fixed Asset Subsystem Policy Manual and User Guide" requires that "(p)hysical property other than land and buildings shall be marked with some type of permanent tag affixed to a readily available area of the asset." The User Guide also requires that "this tag must have a unique identification number that will be associated with the asset and become a part of the asset's permanent record."

c. Surplus Property

Our audit indicated that EOHHS had not complied with Operational Services Division regulations requiring that "(i)tems declared as surplus, salvage or scrap under the appropriate code will remain the responsibility of the declaring agency until disposal, as authorized by the State Surplus Property Office." We found that the Executive Office had not listed 34-microcomputer workstations in the inventory record. Although no longer in use, the equipment was still under the Office's control and should have been listed in the inventory record. Information regarding equipment designated for disposal or as surplus should remain on the inventory record until the items are transferred out of the Office and the responsibility for the asset is actually transferred, in compliance with OSD regulations. Because the inventory record lacked cost figures, we could not determine the value of the computer equipment.

Sound management practices and generally accepted industry standards advocate that a perpetual inventory record be maintained for all property and equipment, including hardware and software, and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. Chapter 647 of the Acts of 1989 states, in part, that "the agency head shall be responsible for maintaining accountability for the custody and use of resources and shall assign qualified individuals for that purpose, and periodic comparison should be made between resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Moreover, the OSC's "Internal Control Guide for Departments" promulgated under Chapter 647 of the Acts of 1989, requires that "fixed assets be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to provide control of inventories."

The absence of adequate controls over the management of the EOHHS IT-related resources placed computer-related equipment at risk of loss, theft, or unintended damage. The lack of a current, accurate, complete inventory record for computer-related equipment and software can hinder the Executive Office's ability to account for IT-related resources, detect lost or stolen items, and ensure that these resources were being used only for their intended purpose. The absence of tagging procedures for computer equipment, including affixing a tag on the equipment and entering a corresponding number in the inventory record, further hampered the Executive Office's ability to ensure that all IT-related resources were properly accounted for. Because software was not listed on the inventory record, the Executive Office did not have an accurate and complete accounting of software installed on the automated systems. As a result, the Executive Office was hindered in its ability to determine whether unauthorized or illegal copies of software were installed on the automated workstations. Further, because costs for IT resources were not listed on the inventory record or maintained in an ancillary file,

the Executive Office did not have readily available aggregate costs of computer-related equipment and software.

Because the Executive Office had not performed an annual physical inventory and reconciliation, it could not be determined whether any items, such as those declared surplus property, had been removed from the inventory record. As a result, the inventory record and corollary records of surplus property could be inaccurate and incomplete.

It is our understanding that EOHHS management was aware of the control deficiencies regarding the management and control of fixed assets and would address the issues noted above.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that EOHHS management obtain an understanding of the Internal Control Act, Chapter 647 of the Acts of 1989, and that management control practices and procedures required by the Office of the State Comptroller regarding the safeguarding of, accounting for, and reporting on IT-related resources. We recommend that EOHHS strengthen current practices to ensure compliance with policies and procedures documented in the OSC's "Internal Control Guide for Departments," "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment.

We recommend that EOHHS perform a physical inventory and reconciliation of its IT resources, including computer-related equipment and software. Based upon OSC guidelines, the Executive Office should ensure that they have in place an accurate and complete inventory record of fixed assets, including IT resources. Regarding the composition of the inventory record, we recommend that the EOHHS include sufficient "data fields," such as state identification number, location, purchase date, installation date, and cost in the inventory record to properly identify, account for, and monitor equipment. The EOHHS should enter all equipment into the inventory record at the date of acquisition and delete items, as needed, in a timely manner. We recommend that the Office perform an inventory record reconciliation, concurrent with its annual physical inventory, and make any required adjustments to its inventory record. The Executive Office should implement adequate controls, including monitoring and evaluation procedures, to provide reasonable assurance that the inventory records of its IT-related resources are accurate, complete, valid, and verifiable and are maintained on a current basis. To maintain proper internal control, staff members who are not responsible for maintaining the inventory record of property and equipment should perform the periodic reconciliation. Further, when appropriate, the inventory record, once reconciled, should be used as the basis for generating the Commonwealth's required asset-

management reports (e.g., GAAP Reports). The inventory record should be amended to reflect inter-office transfers of computer-related equipment.

EOHHS should develop and implement formal policies and procedures regarding the safeguarding of, accounting for, and reporting on its property and equipment, including IT-related resources. The formal policies and procedures should include, but not be limited to, the following items: maintaining an inventory record; performing, at minimum, an annual physical inventory and reconciliation; tagging procedures for computer-related equipment; accounting for and monitoring of property and equipment; and disposal of surplus property. In conjunction with the development of policies and procedures, the Office should include procedures regarding the maintenance of a perpetual inventory, which should be reconciled, at least annually, to the physical assets. The perpetual inventory should indicate dates last updated and reconciled. The policies and procedures, once approved by Secretariat officials and senior management, should be distributed to the appropriate staff, and the staff should be instructed in their use.

We recommend that the Executive Office ensure that all computer equipment is tagged with state identification numbers. Although our examination of fixed-asset accounting did not extend beyond IT-related assets, we recommend that the Office determine whether appropriate tagging procedures are being followed and records maintained for other property and equipment under the Secretariat's responsibility.

EOHHS should include software in its IT-related inventory record. The software inventory should identify all software products installed and available for use on all file servers and microcomputer workstations. With respect to information that should be included in the software inventory record, the record should identify the name of the software product, date of installation, type of license (e.g., workstation or LAN version), version number, date of acquisition, license period (if applicable), and the cost or annual license fee per item.

EOHHS should fully utilize the training regarding fixed-asset management provided by the Office of the State Comptroller and from other sources.

Auditee's Response:

Inventory Control

In the way of status, a major finding of the report was a lack of inventory control and procedures to protect Commonwealth assets. Since the time of the audit visits, our office has created a Microsoft Access database that tracks all the fields recommended in your report with the exception of software installed on each PC. We consider the likelihood that significant unauthorized or illegally installed software is present on EOHHS PCs to be minimal because users do not have sufficient privileges to install software without an administrator password. However, to address this finding, we will add these data fields to our tracking database in the near future. Further, all computer assets of significant value (monitors and CPU's) have been permanently tagged with a corresponding control number that is tracked back to the serial numbers in the inventory system. Our staff have promised to send a sample page of our new system to the auditors who performed the audit to make sure it is satisfactory and they were willing to look it over and get back to us with details.

Surplus Property

The issue of surplus property requires documentation of existing procedures and a more formal process to be sure these policies are adhered to. The thirty-four computers that are identified in the report in storage in the server room have been surplused to the Department of Youth Services for use in their educational classrooms. All required documentation for this transaction is on file in our office. In the future, I expect us to be fully compliant with this finding.

Auditor's Reply:

We are pleased that EOHHS has made efforts to strengthen controls over IT-related resources, such as tagging all computer-equipment, enhancing the IT-related inventory record with the addition of appropriate "data fields," and developing formal procedures to account for surplus property. We agree with management's decision to develop IT-related policies and procedures as stated in the auditee's response, page 11. We reiterate that the documentation should include policies and procedures regarding the safeguarding of, accounting for, and reporting on IT-related resources. We also reiterate that the Executive Office should maintain a current, accurate, and complete inventory record for computer equipment and software, comply with all Office of the State Comptroller's requirements for fixed-asset management, and perform an annual physical inventory and reconciliation. We will review inventory control at our next scheduled audit.

2. System Access Security

Our audit disclosed that control practices regarding system access security needed to be strengthened to provide reasonable assurance that only authorized users were granted access to the Executive Office's automated systems. We determined that control procedures authorizing users to access the Office's file servers and microcomputer workstations were appropriate. These procedures included having the supervisor notify the Office's information technology operations through e-mail of a newly hired staff member. The authorization level of a new employee was based upon pre-determined levels of access assigned to the specific job title and associated responsibilities designated by the employee's supervisor. Subsequently, the network manager activated the authorized levels of system access for each new employee. Although we found that these procedures were appropriate, we determined that EOHHS was not consistently applying the notification procedures regarding authorization to access the systems. As a result, we were unable to confirm that only authorized employees were allowed to access automated systems.

We determined that, although the procedures noted above provided an appropriate authorization and activation process, EOHHS was not requiring users who were granted access to the Office's automated systems to sign a formal security statement acknowledging that they understood their responsibilities regarding the protection and appropriate use of their logon IDs and passwords. In addition, at the time of our audit, we found that control procedures regarding authorization and activation of user access privileges were not documented and referenced in an internal control plan.

Our audit indicated that control practices regarding logon ID and password administration were determined by the Information Technology Division. Further, we found that ITD was responsible for documented policies and procedures regarding logon ID and password administration, such as password formation and use, required periodic changes of passwords, password protection and data confidentiality. According to Executive Office management, subsequent to being granted access privileges, users were assigned a unique logon ID and were required to choose a password of sufficient length and composition as required by the Executive Office for Administration and Finance's Information Technology Division (ITD). To gain access to the system, the user was required to enter his/her logon ID and password. According to Executive Office management, users were required to comply with ITD's schedule for password changes.

With respect to procedures to deactivate access privileges, we determined that EOHHS had implemented appropriate procedures to provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the automated systems. During the audit, we tested the Office database for the presence of unauthorized users whose access privileges remained

active. We tested 42 (100%) of users with active privileges to the current official personnel list. Based on our comparison, we found that, as of the test date, all 42 users were current Executive Office employees.

Our audit revealed that EOHHS had not developed policies and procedures regarding notification of IT operations upon a change in employee job status that would require modification or deactivation of users' access privileges. Changes in employment status that can 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. According to senior management, the Executive Office was aware of the lack of adequate documentation regarding authorization of users to access automated systems; activation, deactivation, and deletion of logon IDs and passwords; and they planned to address these deficiencies.

Generally accepted computer industry standards indicate the need to prevent unauthorized system access through the implementation of formal control procedures. 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 authorize, activate, and deactivate logon IDs and passwords when employee status changes. Failure to implement adequate controls regarding system access security could result in unauthorized system access or use. If unauthorized access were gained to the Executive Office's data files residing on the network's file servers or the microcomputer workstations, it would raise the risk of unauthorized disclosure, modification or deletion of critical and important data, such as confidential information regarding its agencies' clients.

Recommendation:

We recommend that control practices regarding authorization and activation of access privileges be documented and included or cross-referenced in an internal control plan. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that EOHHS strengthen policies and procedures to help ensure that IT operations is notified in a timely manner of all changes in employee status that could impact access privileges, such as terminations, extended leaves of absence, and inter-departmental changes in authorization levels. Once notified of the change in employment status, the network manager should deactivate and/or delete the logon ID and password in a timely manner.

Regarding logon ID and password administration, we recommend that the Executive Office determine an appropriate schedule for required password changes. We recommend that the Office document policies and procedures regarding password formation and use, minimum length of passwords, and frequency of password changes. In addition, we recommend that to reinforce user responsibilities regarding access privileges, the

Executive Office require users to sign a formal statement acknowledging the confidentiality of their password and that commitment to protect the password from unauthorized use and/or disclosure.

We recommend that the Office obtain and review the "Administration and Finance Policy on the Use of Information Technology" promulgated by EOAF. Based upon the review, EOHHS should consider including control practices and procedures documented within the Policy, such as acceptable uses for IT resources, data confidentiality, and network security in the Office's formal policies and procedures. We also recommend that the documented policies and procedures address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts. Appropriate staff should be instructed regarding implementation and adherence to access security policies and procedures.

Auditee's Response:

Password Policies

> *. . .Policies on password length, composition, reuse, and expiration are set by the Information Technology Division, from which the Executive Office receives its network services. Those policies are enforced by requirement of ITD, at their administrative level, and we support those policies. Further in the document you state that we have not documented those policies and we do not disagree with that finding. The policy is ITD's to document, though it remains our responsibility to distribute those policies to staff, which this office previously has not. We will take the steps necessary to address this finding. . .*

Auditor's Reply:

We are pleased that Executive Office management will distribute ITD documented control procedures to staff. We reiterate that, to strengthen controls over system access security, the Office should document control practices regarding authorization to access automated systems, activation of logon IDs and passwords, and deactivation of access privileges and comply with the "Administration and Finance Policy on the Use of Information Technology," promulgated by EOAF. In addition, we continue to recommend that the Executive Office document the granting of access privileges to users and require users to sign a formal security statement.

Appendix A
Executive Office of Health and Human Services
Summary of Internal Control Practices
as of March 6, 2002

Pg. Ref.	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
8	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, file server room, microcomputer workstations, and client records in hardcopy form so that loss or damage is prevented	Control over access to offices, computer rooms, file servers, and microcomputer workstations, designated facilities manager, intrusion devices, locked doors, foot patrols	In Effect	No	N/A
9	Environmental Protection	Provide reasonable assurance that IT-related resources are adequately protected from loss or damage	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures	In Effect	No	N/A

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 A
Executive Office of Health and Human Services
Summary of Internal Control Practices
as of March 6, 2002

Pg. Ref.	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
9,17	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	Adequate	Yes, by ITD	N/A
9,12	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record, and reported on, when appropriate, to oversight entity	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	None	No	N/A

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 A
Executive Office of Health and Human Services
Summary of Internal Control Practices
as of March 6, 2002

Pg. Ref.	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
10	Business Continuity Planning	Provide reasonable assurance that EOHHS can restore mission-critical and essential functions in a timely manner should file servers and microcomputer workstations be rendered inoperable.	Current, formal, tested business continuity plan; periodic review and modification of plan; plan implemented, distributed, and staff trained in its use	None	No	N/A
10	On-site storage	Provide reasonable assurance that backup 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 a separate on-site location	Insufficient	Yes	Adequate
11	Off-site storage	Provide reasonable assurance that critical and important backup media are available should computer systems be rendered inoperable	Same as above. Storage area in a separate location	Insufficient	Yes	Adequate, except for logs documenting transport and return of backup copies

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
Executive Office of Health and Human Services
List of Agencies
as of March 6, 2002

- Division of Health Care and Finance Policy
- Division of Medical Assistance
- Department of Mental Health
- Department of Mental Retardation
- Department of Public Health
- Department of Social Services
- Department of Transitional Assistance
- Department of Youth Services
- Massachusetts Commission for the Blind
- Massachusetts Commission for the Deaf and Hard of Hearing
- Massachusetts Office for Refugees and Immigrants
- Massachusetts Rehabilitation Commission
- Office of Child Care Services
- Soldiers' Home – Chelsea
- Soldiers' Home - Holyoke