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. 2002-0030-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE FISCAL AFFAIRS DIVISION

JULY 1, 2000 THROUGH SEPTEMBER 6, 2002

OFFICIAL AUDIT REPORT
AUGUST 20, 2003

TABLE OF CONTENTS

INTRODUCTION

The Fiscal Affairs Division (hereinafter referred to as FAD or the Division) is organized under Chapter 7, Section 4A of the Massachusetts General Laws and is placed within the purview of the Executive Office for Administration and Finance (EOAF). At the time of our audit, FAD was comprised of a Budget Director, a Deputy Budget Director, and was staffed by 27 employees. The Budget Director was appointed by the Secretary of EOAF with the approval of the Governor of the Commonwealth. In addition to managing the Division and preparing operating budget recommendations for all state agencies and departments, the Director served as Assistant Secretary for Fiscal Policy. For the fiscal year ending June 30, 2002, FAD received a state appropriation totaling $2,260,561. The Division's administrative office is located at the State House in Boston.

FAD's primary mission is "to review and evaluate all requests for appropriations and estimates of revenue, prepare the Governor's budget recommendations for submission to the Legislature, and administer the provisions of all appropriation acts." Further, the Division develops and manages financial planning activities of state government and assesses the financial and programmatic impact of state agency activities. According to the Division's website, "FAD analyzes the projected impact of new and existing legislation to ensure that the Commonwealth's projected revenues support projected levels of spending, and oversees spending authorized by the Legislature." In conjunction with state agencies, FAD develops policy alternatives and works to ensure fiscal stability under changing circumstances.

From an information technology (IT) perspective, the Division's IT Department supports FAD's mission by administering the IT infrastructure and providing assistance to the staff regarding effective and appropriate use of the technology. At the close of our audit, the Division's IT infrastructure consisted of seven file servers, 60 microcomputer workstations, and 14 laptop computers. FAD's business functions were supported by six file servers and 30 microcomputer workstations configured in a local area network (LAN). Of the remaining 30 microcomputer workstations, six were being installed for future use, seven were in storage, six were used for testing new applications, eight workstations were not in use, and three were being used as standalone microcomputers for functions, such as printing and scanning documents. The file servers were connected through a wide area network (WAN) to the Information Technology Division's (ITD) mainframe which provided connectivity to the Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management and Accounting Reporting System (MMARS), the Commonwealth's primary accounting system. File servers provided services, such as e-mail and access to the Internet. The Structured Query Language (SQL) server provided a database to which state agencies would connect to access budgetary information.

Primary applications operating on the microcomputer workstations included business-related applications, such as word processing, spreadsheets, and WEB-related applications for graphics and editing.

Our Office's examination focused on selected general controls, such as physical security and environmental controls, 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 April 9, 2002 through September 6, 2002, we performed an audit of selected information technology (IT) related controls at the Fiscal Affairs Division (FAD) for the period covering July 1, 2000 through September 6, 2002. The scope of our audit included an examination regarding control practices, procedures, and devices, regarding physical security and environmental protection over and within FAD's administrative offices. Further, we reviewed physical security and environmental protection controls over restricted areas housing confidential state agency records in hardcopy form. We reviewed and evaluated system access security to the automated systems and examined control practices regarding the accounting for computer-related equipment and software. In conjunction with our audit, we reviewed policies and procedures implemented by FAD regarding controls and operations for the areas under our review.

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 tapes of magnetic media. We evaluated physical security and environmental protection controls over backup copies stored on-site at the administrative office. We reviewed procedures for generating and transferring backup copies of mission-critical 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 whether 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 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 were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources. In addition, we determined whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to FAD's business-related applications and network-based applications, such as the database residing on the SQL server, and that procedures were in place to prevent and detect unauthorized access to automated systems.

Another audit objective was to review and evaluate control practices regarding accounting for computer-related equipment and software. We also 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 systems 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 FAD's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of FAD's organization and operations, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant functions and activities supported by the automated systems, and reviewed automated functions related to operations designated as mission-critical by FAD, such as the development of the Governor's annual budget recommendations.

As part of our pre-audit work, we reviewed and evaluated the organization and management of IT operations at the administrative office. We inspected the administrative office in Boston, including the file server room, reviewed relevant documents, such as the network configuration and internal control plan, business continuity plan, and performed selected preliminary audit tests. We interviewed FAD management to discuss internal controls regarding physical security and environmental protection over and within the room housing the file servers, microcomputer workstations installed in the business offices, and on-site and off-site storage of mission-critical and essential magnetic media. In addition, we discussed physical security over state agency records in hardcopy form located at the administrative office. In conjunction with our audit, we reviewed written, authorized, and approved policies and procedures for control areas under review. 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.

To determine whether physical access over IT-related resources, including computer 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, including the file server room. We also reviewed and evaluated physical security at a work office and file room situated in a separate location at the State House. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with FAD management and staff. 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 state police on duty, locked entrance and exit doors, the presence of a receptionist at the entrance point, burglar alarms, and whether sign-in/sign-out logs were required for visitors.

We reviewed physical access control procedures, such as the lists of staff authorized to access the file server room, and key management regarding door locks to the administrative office's entrance, file server room and other restricted areas within the administrative office. We determined whether the Division 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 controls were in effect to physically secure state agency records, we inspected restricted areas within the administrative office where records were stored. We determined whether doors to the restricted areas were locked and whether file cabinets used to store records were secured. We obtained an understanding regarding record retention and disposal of documents.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS) and surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether 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 business offices and the room housing the file servers. Further, we reviewed control procedures to prevent water damage to automated systems, agency records, 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 systems. To determine whether Division 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 IT Director and LAN Manager responsible for management of the network and evaluated selected controls to the automated systems. In conjunction with our review of network security practices, we reviewed control practices 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 LAN Manager responsible for access to the file servers and microcomputer workstations on which the Division'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 the Division did not document the granting and recording of 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 FAD users with active privileges were current employees, we obtained the list of individuals with access privileges to the network and microcomputer workstations and compared 29 (100%) users with active access privileges to the Division'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. In addition, we reviewed control practices regarding read-only access to specific data files residing on FAD's automated systems granted to selected employees of EOAF and the Governor's Office.

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 LAN Manager. In conjunction with our audit, we reviewed formal policies and procedures promulgated by Office of the Massachusetts State Comptroller (OSC) regarding inventory control and determined FAD's compliance with these procedures. We obtained the inventory record dated May 10, 2002 with a listed value of $329,024. 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. Further, we determined whether the serial numbers attached to the equipment were accurately recorded 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 inventory record. Further, we reviewed the adequacy of procedures used by FAD to dispose of and properly account for surplus equipment. We also reviewed control practices regarding safeguarding and accounting for the 14 laptop computers. We reviewed software inventory control practices and procedures for software inventory with a listed value of $93,883 as of September 6, 2002.

To determine whether the IT-related inventory record, as of May 10, 2002, was current, accurate, and complete, we confirmed information recorded on the inventory list provided by the Division to descriptive information obtained from the actual computer equipment on hand and supporting documentation. We compared tag numbers listed on the inventory record to the corresponding numbers attached to the seven file servers and 60 microcomputer workstations and 14 laptop computers. We determined whether the tag numbers were accurately recorded on the inventory record. In addition, we determined whether equipment purchased during the 2001 fiscal year was properly listed on the inventory record by tracing information obtained from purchase documentation to the inventory record and verifying that purchased microcomputer workstations and laptop computers existed through on-site verification at the administrative office. In this regard, we selected, on a judgmental basis, 45 microcomputer workstations, with a listed value of $69,375 and five laptop computers, with a listed value of $13,485, for review. We then traced the microcomputers and laptops to the inventory record and to the actual equipment installed at the administrative office. FAD did not purchase IT-related equipment during the 2002 fiscal year.

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 IT Director and LAN Manager 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 Division management responsible for generating backup copies of magnetic media for administrative work processed at the Division and applications, such as the database of budgetary and fiscal information, residing on the file servers. Further, we reviewed the adequacy of provisions for on-site 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 Fiscal Affairs Division (FAD) to provide reasonable assurance that IT-related resources were properly safeguarded and protected from damage or loss. With respect to inventory control over IT-related resources, we determined that sufficient control practices were in place to provide reasonable assurance that the IT resources, including computer-related equipment, were properly accounted for in Division records and were installed at the administrative office in Boston. Our audit indicated that FAD had implemented appropriate practices and procedures regarding granting and recording of access privileges and deactivation of logon IDs and passwords. However, other security 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.

Regarding availability of systems, adequate control practices for on-site and off-site storage of backup copies of magnetic media were found to be in place. With respect to disaster recovery and business continuity planning, our audit indicated that control practices needed to be strengthened to provide reasonable assurance that normal business operations could be resumed at FAD in a timely manner should the file servers or microcomputer workstations be unavailable for an extended period.

Our review of internal controls indicated that FAD was aware of the need for internal controls, had a defined organizational structure for the Division, 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 or strengthened regarding physical security, environmental protection, and system access security. Documented control practices regarding inventory control over IT-related resources were adequate. Failure to adequately document required control procedures may result in important controls not being implemented or exercised. In addition, the absence of documented controls can inhibit the review of the nature and extent of operative controls. (See Summary of Internal Control Practices, page 12.)

Our audit disclosed that appropriate physical security controls had been implemented over and within the Massachusetts State House where the Division's offices are located. These controls included on-duty state security personnel; security devices, such as standalone 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 FAD's administrative office, we determined that

there was one entrance/exit to the office that was being used, a receptionist was located at the front entrance, and a punch keypad system was used to secure the office door. According to management, the entrance door was locked after normal business hours. Furthermore, we determined that physical security over the work office area and file room, both of which were situated in a separate location from the administrative office, was adequate. We found that the work office area also had a single entrance/exit and a punch keypad system that was used to secure the entrance door. According to management, the combination code to the punch keypad systems would be changed after staff terminated employment at the Division. 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 three staff from IT operations via a punch keypad system. We also determined that confidential agency documents were located in a physically secure area and kept in locked file cabinets.

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 FAD 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. A hand-held fire extinguisher was located within the file server room. Evacuation and emergency procedures were documented and available in the administrative office. According to management, staff had recently been trained in the use of these emergency procedures. To strengthen physical security and environmental controls, we recommend that the Division develop formal policies and procedures.

Regarding system access security, our audit revealed that, although FAD had developed appropriate procedures regarding the granting of access privileges to automated systems and activation of logon IDs and passwords, these control practices had not been documented. 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 29 (100%) FAD users to the Division's personnel roster of current employees indicated that these users were current employees. Further, we determined that control procedures regarding granting of limited access privileges to selected Executive Office for Administration and Finance and Governor's Office staff were appropriate.

Regarding logon ID and password administration, we determined that passwords were not being changed periodically. Further, FAD had not developed control documentation regarding password formation and use, length of passwords, and frequency of password change. At the

close of our audit, management stated that they would consider developing a schedule for password changes.

To strengthen system access controls, we recommend that FAD document procedures regarding authorization, activation, and deactivation of access privileges. We also recommend that the Division document the granting and recording of authorization to access automated systems. Regarding logon ID and password administration, we recommend that FAD 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. Documented procedures should be included in the Division's Internal Control Plan. In addition, we recommend that to reinforce user responsibilities regarding access privileges, the Division should require users to sign a formal statement acknowledging the confidentiality of their passwords and commitment to protect the password from unauthorized use and/or disclosure.

Our audit revealed that adequate control practices and procedures were in place to provide reasonable assurance that IT-related resources were properly accounted for in Division records. We determined that, at the time of our audit, FAD maintained a current, accurate, and complete inventory record for computer-related equipment with a listed value of $329,024. We found that FAD had complied with the Internal Control Act, Chapter 647 of the Acts of 1989 and associated requirements regarding fixed-asset management promulgated by the Office of the State Comptroller as of 2002. We determined that the IT-related inventory listing included appropriate fields, such as state identification number, serial number, date of acquisition, and cost. IT-related equipment installed in the administrative office, work office, and file server room had been tagged with state identification numbers. According to Division management, an annual physical inventory and reconciliation was being performed. Adequate procedures were in place to properly safeguard and account for laptop computers. Further, our audit indicated that FAD was aware of Operational Services Division requirements regarding surplus property and that surplus property was properly accounted for in agency records.

Our audit revealed that a software inventory record with a listed value of $93,883 was being maintained and that software licenses were on file at the Division's administrative office.

We determined that FAD 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. We acknowledge that the Division was aware of the need for business continuity planning and had developed informal procedures, including manual processing procedures and selected microcomputer workstations designated for emergency use to resume normal business operations should IT equipment be damaged or become inoperable or inaccessible. According to management, because FAD was within the purview of the Executive

Office for Administration and Finance, the Division would have ready access to EOAF offices for use as an alternate processing site. Because of the critical nature of the Commonwealth's budgeting process and fiscal stability, we recommend that the Division, at a minimum, document user area plans and coordinate additional contingency planning with EOAF.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site backup of magnetic media. We determined that FAD had implemented procedures and schedules for generating backup copies of magnetic media, and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies. We also found that physical security and environmental protection over the on-site storage location was adequate. We did not visit the storage facility housing off-site backup copies of magnetic media.

Auditee Response:

> We agree with most of your findings and are pleased, but would like to correct [one discrepancy]. . .
>
> . . . (y)ou mention "that authorization of users to access automated systems was not documented." I just wanted to clarify that we do maintain a list of authorized users by uaid [logon ID] and social security number, which is updated when we gain and lose employees. . .
>
> . . .Finally, we are planning on reviewing your findings to incorporate into our IT procedures.

Auditor's Reply:

We are pleased that the Fiscal Affairs Division will incorporate our recommendations regarding information technology related controls into its procedures. Regarding authorization to access automated systems, we acknowledge that the Division has maintained a list of users with active access privileges. We recommend that, to strengthen controls, the Division enter the date that a user is authorized to access automated systems.

Appendix
Summary of Internal Control Practices
Fiscal Affairs Division
as of September 6, 2002

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 workstations, and client records in hardcopy form so that loss or damage is prevented	Control over access to offices, computer rooms, file servers, microcomputer workstations, laptop computers, designated facilities manager, intrusion devices, locked doors, foot patrols	In Effect	No	N/A
10	Environmental Protection	Provide reasonable assurance that IT-related resources are adequately protected form loss or damage	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures	In Effect	Yes	Adequate, for emergency and evacuation procedures

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
Summary of Internal Control Practices
Fiscal Affairs Division
as of September 6, 2002

Pg. Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
10,11	System Access Security	Provide reasonable assurance that only authorized users are granted system access to automated systems	Passwords required to access automated systems, changes of passwords required; formal rules for password formation and use; formal procedures for authorization, activation, and deactivation of logon IDs and passwords	Insufficient, Informal procedures in place	No	N/A
11,12	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, software inventory maintained	In Effect	Yes	Adequate
12	Business Continuity Planning	Provide reasonable assurance that essential mission-critical functions can be resumed 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	Insufficient	No	N/A

Appendix
Summary of Internal Control Practices
Fiscal Affairs Division
as of September 6, 2002

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Doc.
12	On-site storage	Provide reasonable assurance that backup of magnetic media are available should automated systems be rendered inoperable	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage area are adequate; storage area is in a separate on-site location	In Effect	Yes	Adequate
12	Off-site storage	Provide reasonable assurance that critical and important media are available should automated systems be rendered inoperable	Same as above. Storage area in a separate location	In Effect	Yes	Adequate