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. 2005-1215-4T

INDEPENDENT STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE OFFICE OF THE COMMISSIONER OF PROBATION

July 1, 2003 through January 31, 2005

OFFICIAL AUDIT REPORT

JUNE 8, 2005

2005-1215-4T

TABLE OF CONTENTS

INTRODUCTION

The Office of the Commissioner of Probation (OCP) was established under the provisions of Chapter 276, Section 98 and Section 99, of the Massachusetts General Laws (MGL). The OCP's primary mission is to administer justice through investigations, community supervision of offenders/litigants, diversion of appropriate offenders from institutional sentences, reduction in crime, mediations, service to victims, and the performance of other appropriate community service functions. At the time of our audit, OCP had a total of 107 employees working in the central office administering all Massachusetts probation services, at the John W. McCormack State Office Building in Boston, Massachusetts and two satellite offices.

The Office of the Commissioner of Probation establishes standards for probation practices, provides training to probation personnel, and sets qualification standards for individuals seeking appointment as probation officers. The OCP oversees Probation Officers in the District, Superior, Juvenile, Probate and Family, and Boston Municipal Court probation departments throughout the Commonwealth, and conducts research on statewide crime and delinquency trends. The OCP works in collaboration with local social service agencies to provide innovative programs such as the Fatherhood and Motherhood Programs, Warrant Apprehension, the Night Light Program, and the Anger Management Program that directly affect communities across the Commonwealth.

The Administrative Office of the Trial Court (AOTC) provides administrative oversight as well as strategic and tactical planning to OCP operations. From an information technology perspective, the AOTC supports the mission and business objectives of the District Courts by administering the IT infrastructure, including mission-critical applications installed on the file servers and mainframes located at the AOTC's Information Technology Division in Cambridge. In addition, the AOTC provides IT services and technical support to individual courts and maintains master inventory records for the courts under its jurisdiction.

The Commonwealth's effort to provide for more effective criminal justice sentencing and to specifically address the issue of prison overcrowding resulted in the initiation of an electronic monitoring program established in May 2001 and administered by the OCP. The program, which had over 450 offenders at the time of our audit, seeks to monitor individuals ordered by judges to wear electronic bracelets as a condition of their probation, as well as parolees as ordered by the Massachusetts Parole Board. Probation officers throughout the Commonwealth have received training in applying the electronic bracelet on the probationer and are responsible for the supervision of their assigned probationers. The program is administered through two offices, one located in Boston that is open 24 hours a day, seven days a week, and the other location in Springfield, Massachusetts. The two offices report alerts and violations to authorized probation officers.

At the time of our audit, the Office of the Commissioner of Probation's business operations were supported by technology consisting of 76 microcomputer workstations configured in a Local Area Network (LAN). Relay switches and routers provided connectivity to the Administrative Office of the Trial Court's Wide Area Network (WAN). Mission-critical application systems used by OCP include the Probation Receipt Accounting System (PRA), Court Activity Record Information System (CARI), and the Warrant Management System (WMS). In addition, the OCP uses the Human Resources/Compensation Management System (HR/CMS) payroll system and the Massachusetts Management Accounting and Reporting System (MMARS) that are maintained by the Office of the State Comptroller.

The Office of the State Auditor's examination focused on a review of certain IT-related general controls over the Office's computer operations.

AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) audit of controls at the Office of the Commissioner of Probation (OCP) covering the period of July 1, 2003 through January 31, 2005. The scope of the audit, which was conducted from October 12, 2004 through January 31, 2005, included a general control examination of IT organization and management, physical security, environmental protection, system access security, inventory control for computer equipment, business continuity planning, and on-site and off-site storage of backup copies of computer media.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place throughout areas housing computer equipment and the computer room. Our objective regarding system access security was to determine whether adequate administrative controls were in place for user account management for authorized access to automated systems. In addition, we determined whether adequate controls were in place for the activation, maintenance, and deactivation of access privileges to provide reasonable assurance that only authorized OCP personnel had access to the CARI system.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded, accounted for, and safeguarded against unauthorized use, theft, or damage. We sought to determine whether an effective business continuity plan was in place that would provide reasonable assurance that mission-critical IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. We sought to determine whether adequate controls were in place for on-site and off-site generation of backup media to support system and data recovery operations.

Audit Methodology

To determine audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant IT operations, reviewing and evaluating certain IT-related internal controls, and interviewing senior management at the OCP central office. To obtain an understanding of the internal control environment, we reviewed the OCP's organizational structure and primary business functions. We performed a high-level risk analysis, and assessed the strengths and weaknesses of the internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our examination of organization and management, we interviewed senior management, obtained, reviewed, and analyzed existing IT-related policies, standards, and procedures, as well as the IT organizational structure. We also examined whether the OCP had an established chain of command, adequate level of oversight, segregation of duties, and clear points of accountability.

To evaluate physical security, we interviewed management, conducted walk-throughs of the OCP computer room at the central office, and reviewed procedures to document and address security violations and/or incidents. We examined the existence of controls, such as office door locks, remote cameras, and intrusion alarms. We determined whether access to areas housing computer equipment was restricted to authorized personnel.

To determine the adequacy of environmental controls, we conducted walk-throughs and examined the computer room and office areas housing IT equipment to determine whether resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of relevant OCP documentation.

We reviewed control practices regarding system access security, such as procedures used to authorize, activate, and deactivate access privileges to the AOTC mainframe and OCP's microcomputer workstations. We confirmed users with active access privileges to documentation authorizing the employee to access the OCP's automated systems. To determine whether only authorized employees were accessing the automated systems, we obtained the list of individuals granted access privileges to OCP's CARI application as of October 12, 2004, and compared it to a personnel list dated October 9, 2004. We reviewed and evaluated control practices regarding logon ID and password administration. For the CARI application, we determined whether all employees authorized to access the application system were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for and safeguard computer equipment, we initially reviewed inventory control procedures for property and equipment and obtained an inventory of computer equipment. We examined OCP's efforts to comply with the Administrative Office of the Trial Court's "Fiscal Systems Manual" regarding inventory control and whether generally accepted inventory controls were in place. We verified that appropriate fields of information were contained in the inventory system of record, such as identification tag number, location, description, acquisition date, and historical cost for computer equipment. We conducted a test of OCP's IT-related fixed asset inventory by selecting through a random number generator program a sample of 50 (22.7%) out of 219 IT-related items from OCP's computer equipment inventory dated October 13, 2004. OCP's IT-related inventory list as of October 13, 2004 was valued at $190,510.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume business operations should the application systems available through the network be inoperable or inaccessible. In addition, we determined whether the criticality of IT processing capabilities or application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Further, to evaluate the adequacy of controls to protect data files through the backup of on-site and off-site magnetic media and hardcopy files, we interviewed AOTC and OCP staff regarding the creation and storage of backup copies of computer-related media.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. Criteria for the IT portion of our audit included IT management control practices as outlined in the Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology" (CobiT). The CobiT control model provides IT-related control objectives and generally accepted control practices.

AUDIT CONCLUSION

Based on our audit at the Office of the Commissioner of Probation (OCP), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to organization and management, environmental protection, and on-site and off-site storage of backup of computer media would be met. We also found that appropriate controls were in place to provide reasonable assurance that OCP personnel having access to the CARI application system were authorized users, and that system access controls were in place to support user account management. Although we found that control objectives for physical security and inventory control of IT resources would provide reasonable assurance that control objectives would be met, our audit revealed that certain policies and procedures in these areas should be enhanced. In addition, our audit revealed that the OCP, in conjunction with AOTC, had not developed a business continuity plan to ensure timely resumption of processing capabilities should mission-critical application systems be rendered inoperable or inaccessible.

Our examination of organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties, and clear points of accountability regarding IT functions. We found that IT management and staff were aware of their responsibilities, and that IT-related job descriptions and job specifications reflected current responsibilities. Although we did find documented policies and procedures, the level of documentation for IT control areas could be enhanced.

We found that OCP had implemented adequate physical security controls to provide reasonable assurance that only authorized persons could access the computer room and other areas housing IT-related equipment. The OCP central office is located in a state office building where security is provided by the Massachusetts State Police. The OCP office had specific security controls, such as a keypad lock combination for all office entry doors and a receptionist at the entryway. However, our audit revealed that the computer room door was not always locked during business hours. Although our audit revealed that the computer room had a manual lock, we observed that the door to the computer room was not locked at all times. In addition, OCP had not developed a list of individuals authorized to access the computer room. We recommend that OCP improve their physical security controls by requiring that the computer room door be closed and locked at all times and that a list of individuals authorized to access the computer room be maintained.

Subsequent to completion of our fieldwork, the auditee indicated: *A keypad lock was installed on Tuesday April 5, 2005. A list has been developed by the security officer for the employees who are* *authorized to enter the room and they have been given the code. No vendors will be given the access code. The room will be cleared of any items that do not belong in the area or is not computer or telephone related. The code will be changed when an employee leaves the employment of the OCP. The code will be changed on a predetermined interval if there are no changes in any employment status.*

Our examination of environmental protection over the computer room indicated that controls in place provided reasonable assurance that OCP's IT resources will be protected from damage and loss. We found that control objectives related to air conditioning, fire prevention and detection, emergency power and lighting, emergency shut down, and general housekeeping for areas housing computer workstations would be met. In addition, OCP has an uninterrupted power supply to permit OCP to safely shut down computer equipment without the loss of data in the event of a power loss. However, we observed that the OCP computer room was used for storing materials not related to IT processing. We recommend that OCP management remove from the computer room any articles not pertaining to IT processing.

Our review of system access security controls revealed that adequate administrative control practices were in place to provide reasonable assurance that only authorized users were granted access privileges to the application systems available through OCP's network. We found that policies and procedures were in place regarding proper use of IT resources, including Internet use and e-mail and confidentiality of passwords. We found that all users granted access to automated systems were required to sign a formal security statement indicating that the users understood their responsibilities regarding appropriate use of IT resources and protection and appropriate use of their passwords. Our audit test of 34 (100%) active users having access to the CARI application system revealed that adequate controls were in place to provide reasonable assurance that access privileges were properly authorized and that access would be deactivated for users no longer authorized, or needing, access to CARI. Our test confirmed all 34 users with active privileges to the CARI application system were current OCP employees. Regarding password administration, we found that employees were required to change passwords on a predefined basis, however, control documentation did not adequately address password formation and use, length of passwords, and frequency of password changes. We recommend that the OCP, in conjunction with AOTC, strengthen control documentation to adequately address password formation and use, length of passwords, and frequency of password changes.

With respect to inventory control of computer equipment, we found that OCP was adhering to policies and procedures set forth in AOTC's Fiscal Systems Manual to safeguard and properly account for IT resources. In addition, we found that OCP was adhering to the regulations promulgated by the Office of the State Comptroller requiring that an annual physical inventory and reconciliation be performed. Our review of OCP inventory system of record dated October 13, 2004 and consisting of 219 IT hardware items contained appropriate data fields, such as historical cost, location, description, date received, tag number, and manufacturer. We found that cost amounts were complete for the 219 pieces of equipment and provided a total value of computer equipment at $190,510. However, we recommend that OCP include a description of the condition of each IT resource in the inventory system of record. Although we found the integrity of the system of record to be generally adequate, our test revealed that four out of the 219 IT resources had duplicate tag numbers. Our audit test of 50 randomly selected IT resources confirmed that all of the items selected were located where listed in the inventory record. However, 17 items tested had incorrect identification tag numbers. We recommend that OCP management review the accuracy of all identification tags listed on the inventory listing and strengthen the monitoring of the system of record to ensure proper accounting for IT resources.

Subsequent to completion of our fieldwork, the auditee indicated: *A description of the condition of the equipment column will be added to the excel spreadsheet on the equipment inventory list when the next annual fixed asset inventory is completed. (June 30, 2005). An internal form has been developed before any equipment can be moved in the office, transferred to another probation office, declared surplus, or deemed unusable and destroyed. The signed approval of the First Deputy Commissioner or designee must be made before any equipment is moved from its present location. The data box number at each work location will identify location for all computer equipment.*

Our audit revealed that procedures were in place at AOTC regarding the generation and storage of on-site and off-site backup copies of magnetic media. However, our audit disclosed that AOTC had not formulated with OCP a comprehensive business continuity strategy or user area plan regarding the recovery of business operations, should IT processing capabilities be rendered inoperable or inaccessible. In addition, we found that OCP had not performed a criticality assessment of the CARI application system and the associated risk, and had not identified an alternate processing site. To address the possibility of a disruption or loss of processing capabilities or access to application systems, OCP should, in concert with AOTC, develop appropriate recovery and contingency plans for network operations and access to automated systems. Generally accepted control practices and industry standards for computer operations support the need for organizations to have an on-going business continuity planning process that will assess the relative criticality of information systems and develop appropriate contingency plans, if required. If the application systems were inoperable or if AOTC's or OCP's networks were down for an extended period, the disruption of IT processing capabilities, including access to online data, could have an adverse impact on OCP's business functions.

AUDIT RESULTS

Disaster Recovery and Business Continuity Planning

Although OCP had a strategy to maintain their business operations in case of a disaster, a formalized documented business continuity plan for recovering IT capabilities for the AOTC systems used by OCP did not exist. OCP should work in conjunction with AOTC to develop a formal business continuity, or user area, plan to provide reasonable assurance that critical business operations could be regained effectively and in a timely manner should a disaster render automated systems or network capabilities inoperable. Although backup copies of mission-critical and essential software and data files were being generated by AOTC, specific arrangements had not been made to provide for an alternate IT processing site. In addition, OCP had not formally designated an alternate site to relocate business operations. The latter is important to ensure that appropriate network capabilities are provided and IT resources are made available should business operations need to be relocated. In addition, the OCP had not assessed the relative criticality of required IT processing and access to automated systems. Furthermore, OCP had not assessed potential risks and exposure to data processing operations. Without adequate disaster recovery and contingency planning, including required user area plans, OCP was at risk of not being able to recover business operations within an acceptable period of time should automated systems or network operations be disrupted for an extended period of time. Furthermore, the absence of a comprehensive and tested disaster recovery and business continuity plan could result in unnecessary costs and significant processing delays.

Disaster recovery and business continuity plans should be well documented and tested to reduce the time to recover business operations. In addition, well-formulated business continuity, or user area, plans help reduce the risk of errors and omissions should business operations be regained through other or degraded processing capabilities. An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate the need for a comprehensive and effective backup and disaster recovery and business continuity plan. Contingency planning should be viewed as a process to be incorporated with the functions of the organization, rather than as a project with successful completion upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans.

Recommendation:

We recommend that the OCP work in conjunction with the AOTC to develop a comprehensive and formal business continuity strategy. The OCP should implement procedures to provide reasonable assurance that the criticality of the automated system is evaluated and that business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the IT environment. We recommend that the OCP develop user area plans to be used in concert with AOTC's recovery efforts for AOTC-based systems.

The business continuity plan should document OCP's recovery strategies with respect to various disaster scenarios and outline any necessary contingencies. The business continuity plan should also describe the responsibilities involved in the transfer and safeguarding of the backup copies of data files, software, and system documentation from off-site storage to the site involved for the restoring of data, once a site is identified. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical business operations within required time frames. We further recommend that the business continuity plan be tested and periodically reviewed in conjunction with AOTC and updated, if necessary, to ensure that it is current, accurate, and complete. The completed business continuity plan should be distributed to all appropriate staff members, who must be trained in the execution of the plan under emergency conditions.

Auditee's Response:

> *In the event of any major catastrophe or building closure, alternative work sites will be the ELMO office in the Suffolk County Court House in Pemberton Square and or the Probation Training Academy in Clinton. Employees may also be temporarily assigned to probation offices through-out the Commonwealth. All of the employees will have viewing capabilities to perform their duties. The CARI Manager will give temporary printing capabilities at any off site location. The Trial Court mainframe computer in Cambridge backs up all of the computer information each night. The state police also maintain a back up file.*

Auditor’s Reply:

We understand that OCP is aware of the need for business continuity planning for its mission-critical and essential IT processing capabilities and access to application systems. We also acknowledge that OCP has made efforts to address the development of a business continuity plan and identify potential alternate business processing sites. However, we recommend that OCP management work in conjunction with AOTC to develop a comprehensive business continuity plan for required network capabilities and application systems. We recommend that business continuity plans and procedures be periodically reviewed and updated as necessary. This is especially critical in the future as OCP increases its reliance on information technology to perform its primary business functions.