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. 2006-1265-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON THE EXAMINATION OF
INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS
AT THE PLYMOUTH COUNTY DISTRICT ATTORNEY'S OFFICE

July 1, 2004 through February 10, 2006

OFFICIAL AUDIT REPORT
MAY 3, 2006

2006-1265-4T

TABLE OF CONTENTS

	Page
INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	3
AUDIT CONCLUSION	7
AUDIT RESULTS	9
1. IT Organization and Management	9
2. Physical Security and Environmental Protection Controls	10
3. Disposal of Surplus Computer Equipment	12

INTRODUCTION

The Plymouth County District Attorney's Office (PCDA) was established under the provisions of Chapter 12, Section 13 of the Massachusetts General Laws (MGL). The PCDA provides law enforcement, prosecutions, crime prevention and victim services to the 27 cities and towns that constitute Plymouth County. The PCDA has a staff of approximately 127 employees and 20 state police personnel assigned to investigate criminal cases. The PCDA works in conjunction with the judicial branch and law enforcement communities to prosecute nearly 21,000 criminal cases per year in both Superior and District Court levels. In addition, the PCDA, in coordination with the State Police Investigation Unit assigned to Plymouth County, conducts approximately 500 investigations per year, and has established and maintains an array of crime prevention and victim services in the cities and towns comprising Plymouth County. The PCDA received an appropriation of $5,747,214 of state funds for fiscal year 2005 and an appropriation of $6,034,575 of state funds for fiscal year 2006.

The PCDA's computer operations are supported by the PCDA Information Technology (IT) Department. At the time of our audit, the IT Department, which consisted of two individuals, supported and managed the Department's local area networks (LAN) to which approximately 180 microcomputer workstations are connected. The IT Department manages IT resources at PCDA's five remote sites housing file server sites, workstations and other peripherals. The LANs are connected by the PCDA's wide area network (WAN), which allows access to the Commonwealth's statewide WAN through redundant high-speed connections. The LANs consist of 16 servers, which include file/print servers, a Citrix server, database servers, report servers, and intranet information servers, and the microcomputer workstations. The WAN consists of industry standard CISCO routers and Verizon hardware. The network configuration allows employees access to: PCDA's case management system; legal research software; shared peripherals; the Internet; and management applications.

The PCDA's primary case management application, the DAMION application system, was developed by Constellation Justice Systems. DAMION is a relational database, which provides the PCDA with case management information, court hearings, court dispositions, and provides document generation capabilities. The statewide WAN provides access to the Human Resources/Compensation Management System (HR/CMS), the Massachusetts Management Accounting and Reporting System (NewMMARS), and MassMail (e-mail system) through a group of file servers located at the Commonwealth's data center in Chelsea.

The PCDA receives technology support from the Massachusetts District Attorneys Association (MDAA). The MDAA is an independent association chartered to provide baseline technology services to the eleven elected District Attorneys of the Commonwealth. The MDAA assists in long term planning for common technology projects, coordinates the implementation of statewide projects such as MassMail, and is the liaison for the various District Attorneys to the Information Technology Division of the Executive Office for Administration and Finance.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the PCDA's IT environment and selected financial-related controls.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) and financial-related control audit at the Plymouth County District Attorney's Office (PCDA) from August 18, 2005 through February 10, 2006. The audit covered the period July 1, 2004 through February 10, 2006.

The scope of our audit included an evaluation of IT-related general controls at the PCDA. Areas reviewed included IT-related organization and management, physical security, environmental protection, system access security, inventory control over computer equipment and software, on-site and off-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning. Our audit scope also included an examination of inventory control and related policies and procedures pertaining to drug seized cash and automobiles.

Audit Objectives

The primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support its automated systems and to safeguard IT-related assets. We sought to determine whether the IT-related internal control environment, including policies, procedures and organizational structure provided reasonable assurance that control objectives would be achieved to support the PCDA's mission. We determined whether adequate physical security and environmental protection controls were in place to protect IT resources and to safeguard computer equipment, software, and data files from unauthorized use, damage, or loss. The areas reviewed were the PCDA's main administrative office, including the file server room, and selected satellite offices containing computer equipment. We sought to determine whether adequate controls were in place to prevent unauthorized access to systems and data residing on PCDA's workstations. A further objective was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related fixed assets were properly recorded, accounted for, safeguarded against unauthorized use, theft or damage, and properly disposed of in accordance with Commonwealth regulations.

Regarding system availability, we sought to establish whether IT operations could be regained within an acceptable period of time through a comprehensive business continuity strategy should systems be rendered inoperable or inaccessible. We also sought to determine whether adequate controls were in place to provide reasonable assurance that on-site and off-site storage of backup copies of magnetic media were in place to assist recovery efforts.

Regarding our review of financial-related areas, we sought to assess whether adequate control policies and procedures existed for cash and automobiles in the custody, care, and control of the PCDA resulting from law enforcement related seizures.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior management to discuss the PCDA's IT control environment. To obtain an understanding of the activities and internal control environment, we reviewed the PCDA's organizational structure and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation, and assessed relevant IT-related internal controls. To evaluate physical security at the PCDA offices and at individual courthouse offices housing PCDA offices, we interviewed senior management and security personnel, conducted walkthroughs, observed security devices and visible means of access, and reviewed procedures to document and address security violations and/or incidents. We requested a list of key holders to the PCDA's offices and the file server room and, through observation and review of policies and procedures, determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as office door locks, visitor logs, motion detectors, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees of the PCDA. Further, to determine the adequacy of physical security controls regarding microcomputer workstations, we conducted site visits to office areas at certain administrative satellite offices located in courthouses throughout the county.

To determine the adequacy of environmental controls, we conducted walkthroughs and evaluated controls in selected areas in order to assess the sufficiency of control-related policies and procedures. We examined the areas housing IT equipment at the PCDA administrative offices as well as PCDA's offices at the individual county courthouses to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; water and heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; and

humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and a review of relevant documentation.

Our tests of system access security included a review of policies and procedures used to authorize, activate, and deactivate access privileges to the PCDA file servers through the microcomputer workstations located at the PCDA's administrative and courthouse offices. To determine whether only authorized employees were accessing the automated systems, we obtained the list of individuals granted access privileges and compared it to the current personnel listing. We reviewed and evaluated control practices regarding logon ID and password administration. 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 adequate controls were in place and in effect to properly safeguard and account for computer equipment and software, we initially reviewed inventory control policies and procedures and obtained an inventory of IT resources. We examined the hardware inventory record for identification tag numbers, locations, descriptions, acquisition dates, and historical cost. We conducted an inventory test applying ACL audit software, selecting a sample of 60 items out of a population of 591 hardware items listed on the PCDA inventory, dated August 16, 2005. In addition, we judgmentally selected 17 items (2.9 %) and traced the equipment from the physical location to the master list. Regarding our examination of software items, we compared the software inventory dated September 7, 2005 to the software licenses on hand. We also examined 18 newly-purchased computer items for fiscal year 2005, obtained the original invoice documentation, and traced the items to the current perpetual inventory listing. Regarding our examination of surplus equipment, we verified that the 35 computer items designated as obsolete equipment on the perpetual inventory had been segregated in anticipation of having hard drives digitally cleaned for disposal purposes. We also reviewed PCDA's compliance with the Operational Services Division 802 CMR 3.0 regarding disposal of surplus equipment.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the application systems become inoperable or inaccessible. With respect to business continuity planning, we interviewed management to determine whether the criticality of application systems had been assessed, risks and exposures to computer operations had been evaluated, and a written, tested business continuity plan was in place and in effect. In addition, to evaluate the adequacy of controls to protect data files through the generation and on-site and off-site storage of backup copies of

magnetic media and hardcopy files, we interviewed PCDA staff, reviewed backup procedures, and examined tape rotation logs.

To determine whether controls in place for seized assets in connection with PCDA cases were adequate, we performed selected audit tests of cash and automobiles under the custody, care, and control of the PCDA. We systematically selected every twentieth item from a population of 331 case accounts or 16 items appearing on the August 31, 2005 inventory of cash seized assets. Further, we selected 13 cases representing the highest dollar valued seizures in the custody of the PCDA and traced these items to the safe deposit boxes held at the local bank. These seized assets represent 57.2% of the total value of all the case accounts. To assess the inventory controls over vehicles in custody, we performed tests of the seized vehicle inventory listing dated September 5, 2005 and evaluated the adequacy of the storage facility housing the automobiles. We judgmentally selected 12 out of 49 vehicles and confirmed the vehicle identification number of the vehicles selected to the official system of record maintained by the PCDA.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000. CobiT's control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices.

AUDIT CONCLUSION

Based on our audit at Plymouth County District Attorney's Office (PCDA) we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to system access security, on-site and off-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning. However, our audit revealed that controls needed to be strengthened for IT organization and management, physical security, environmental protection, and for the accounting and safeguarding of surplus computer equipment.

Our examination of IT organization and management controls revealed that there was an established chain of command and there were documented IT-related policies and procedures in place. In conjunction with our review of the internal control environment, we determined that the PCDA had developed and implemented written, authorized, and approved IT-related internal control policies and procedures. However, our observations of staffing levels for the IT Department, considering the volume of work performed, indicated that PCDA management should perform a formal assessment of technical field staffing requirements to determine whether adequate staff are available to maintain IT support services.

Our audit revealed that physical security controls at the PCDA main office needed to be strengthened. Although PCDA management has policies and procedures regarding physical security controls, our audit observations and interviews revealed that certain procedures were not being consistently followed and physical security for the main office could potentially be compromised. Physical security controls must be strengthened to ensure the safety of personnel and the safeguarding of IT resources.

Regarding environmental protection, we found adequate controls such as fire prevention and detection devices; smoke detection and fire alarms, a fire suppression system and fire extinguishers in the file server room and administrative office areas. However, environmental protection controls should be strengthened in the storage area housing hard copy court records. We found that this area did not have smoke, heat, or fire detection devices. In addition, general housekeeping in the corridor between the record storage area and the IT Department needed to be strengthened.

Regarding system access security, we found that controls for the PCDA's application systems provided reasonable assurance that users were properly authorized and that only authorized users had access to the PCDA's data files and programs residing on workstations and file servers. We found that administrative controls over user IDs and passwords provided reasonable assurance

that access privileges would be deactivated or appropriately modified should personnel terminate employment or incur a change in job requirements. During the course of our audit, nothing came to our attention to indicate that there were weaknesses in PCDA's access security controls.

With respect to IT-related fixed-asset inventory control, we found that the PCDA was adhering to the policies and procedures promulgated by the State Comptroller's Office and had conducted annual physical inventories. Our tests indicated that hardware items were locatable, properly accounted for, and tagged. We believe that the IT-related inventory record could be enhanced by including acquisition dates and historical cost figures for all equipment. It is our understanding that PCDA management intends to include this information in the inventory record when they conduct their next physical inventory. We also verified that software products were being accounted for in the PCDA's inventory records and we confirmed that software product licenses were available. However, our audit revealed that controls over the disposition of surplus equipment needed to be strengthened. Our tests revealed that there were 35 computer items designated as surplus dating back to 2003, which had not been reported to the State Surplus Property Officer and were being stored in a passageway.

We found that the PCDA had an adequate business continuity strategy and plan to help ensure resumption of processing within an acceptable time frame should processing be rendered inoperable or inaccessible. We determined that procedures regarding the generation of backup copies of magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate. We recommend that PCDA management continue to test all elements of the plan under its immediate control and update the plan to reflect any changes in technology.

Our audit tests of seized cash and vehicles revealed that control policies and procedures were in place and in effect to adequately account for and safeguard assets in the care, custody and control of the PCDA. We found that the cash for individual case accounts was being held in safe deposit boxes under the direct control of the PCDA at a local bank awaiting legal resolution. We found the seized vehicles were being stored at a secure facility maintained by the Massachusetts State Police. However we observed that the many late model vehicles were left unprotected from the elements and were not subjected to basic maintenance and as a result the potential residual value may be diminished. We recommend that the PCDA enhance their storage procedures by increasing the use of auto protection covers and by providing basic maintenance to vehicles in custody to preserve their value.

AUDIT RESULTS

1. IT Organization and Management

Our examination of the Plymouth County District Attorney's Office (PCDA) IT organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties, adequate span of control and clear points of accountability. In conjunction with our review of the internal control environment, we determined that the PCDA had developed and implemented written, authorized, and approved IT-related internal control policies and procedures and documented IT strategic and tactical plans. However, we believe that the PCDA's technology staffing level is precariously low at the present time. The IT Department has seen a 50% reduction in staff over the past two years and currently has only two employees. These two employees are responsible for the operational activities including database management, application reviews, help desk support, data entry, and data security. The PCDA relies on the IT Department for meeting the technology needs of approximately 127 employees, and the daily operation of 11 file servers and 180 microcomputers located at the main office and at five remote sites. The combination of significant IT staff reductions together with increases in technology requirements leaves the PCDA vulnerable should either staff member be incapacitated or leave their position. We recommend that PCDA management perform a formal assessment of technical field staffing requirements to adequately maintain support services.

Sound business practices require adequate staffing to support the business functions of the enterprise. In addition management must be aware that any personnel changes could adversely impact processing capabilities at the PCDA and hinder timely recording of case information. Without adequate staffing levels, PCDA management is vulnerable to disruptions and associated problems such as delays in data entry of case resolution as well inadequate oversight of the technology environment.

Management may not have been aware of the potential effects of having a reduced IT staff with the level of casework increasing and may not have made IT staffing levels a priority in a constrained budget environment.

Recommendation:

We recommend that PCDA management perform a formal assessment of technical staffing levels required to adequately maintain IT support services to process case information in a thorough and efficient manner. We further recommend that the PCDA establish a separate

budget for the IT department to help plan for future technology requirements. In addition, PCDA senior management should consider formulating a plan for succession, cross training, and staffing of key IT positions.

Auditee's Response:

> *Management will perform this evaluation with attention to maintenance of services to support our mission of prosecution of criminal cases. We will develop a plan for succession, cross-training and staffing of these key positions. In the short term, we are considering hiring part-time or temporary help or offering overtime to our regular employees to assist with some of the IT duties which currently may not be completed in an acceptable time frame.*

Auditor's Reply:

We are pleased that PCDA has initiated actions to improve controls over IT human resource management by developing plans to cross train staff to meet short-term workload demands. On a long-term basis, we re-emphasize our recommendation that management perform a formal assessment of technical staffing requirements to ensure a proper allocation of staff resources can be made with regard to information technology.

2. Physical Security and Environmental Protection Controls

Our audit disclosed that although we found certain physical security controls in place to safeguard IT-related resources and staff, we found that physical security controls at the Plymouth County District Attorney's main office in Brockton need to be strengthened. Our audit revealed that access to the areas housing the microcomputer workstations was limited to only employees. We also observed that the file server room was found to be locked and was located in an area inaccessible to the general public. All entrances are alarmed during non-business hours. However, our audit revealed that security controls to the entrance of the building needed to be strengthened, since the main entrance was not always locked and there were other visible means of egress to the front side of the office from the street. Although we observed certain compensating controls such as the presence of PCDA employees at the entrance doorway, given the sensitive nature of work promulgated from the PCDA, we believe that security controls should be strengthened to ensure that the doorway is consistently locked.

We found the area used for storing, repairing, and installing computer equipment to be located on the street level with just a regular glass entrance door as a barrier. PCDA

management used a piece of hard cardboard to block a street access view but it provides minimal protection for the office.

Regarding environmental protection, we found adequate controls such as fire prevention and detection devices; smoke detection and fire alarms, a fire suppression system and fire extinguishers in the computer room and main portion of administrative offices. However, we observed that several pieces of obsolete IT equipment were left on the floor in the hallways connecting the IT Department to the record storage area. The equipment may have been left there as a matter of convenience, but it has created a cluttered condition that is not conducive to passageway mobility and does not meet generally accepted business standards for good housekeeping. We observed that the areas housing original hard copy court records did not have smoke, heat, or fire detection equipment. We believe that the age and the deteriorating condition of the building as well as budgetary constraints contributed to the difficulty in implementing controls to safeguard IT equipment and confidential records.

Generally accepted computer industry standards advocate the need for sufficient physical security and environmental protection controls to provide reasonable assurance that damage to, or loss of, IT-related assets will be prevented.

Recommendation:

We recommend that the PCDA management should enhance physical security controls at the entrance to the building and consider the installation of grates over all street-level doors and windows. Management should consider the installation of smoke, heat, and fire detection devices in areas of the building, which do not have these devices in place.

Auditee's Response:

> *In our fiscal year 2007 budget request to the Legislature, we have requested an additional $91,000 for plant improvements and security enhancement. We are making every attempt to improve our physical situation for our employees. In the event that this request is not funded we plan to at least make nominal security improvements within the confines of our budget. With regard to the case files mentioned, our office is in the process of converting to digital document storage and will soon begin with superior court case files. This will decrease dramatically our need for physical storage areas.*

Auditor's Reply:

We commend the initial actions initiated by PCDA to improve physical security and environmental protection controls. We suggest that PCDA management, to the extent possible, attempt to implement our recommendations in order to safeguard IT resources and case file information. We will review the improvements made during a follow-up audit.

3. Disposal of Surplus Computer Equipment

Our examination of inventory control regarding the storage and accounting of surplus and obsolete IT equipment revealed that the PCDA needed to strengthen their policies and procedures. Our tests of the PCDA perpetual computer inventory record dated August 16, 2005 revealed that there were 35 items classified as surplus equipment. Our audit revealed that the PCDA failed to comply with Commonwealth of Massachusetts regulations for disposal of surplus property. Operational Service Division (OSD) regulations, 802 CMR 3.00 require that departments file a request listing all Commonwealth assets they intend to dispose of. Our tests revealed that there were computer items designated as surplus dating back to 2003 that had not been reported to the State Surplus Property Officer.

By not properly reporting surplus inventory items on the state surplus list in a timely manner, the PCDA may have denied other state entities the opportunity to utilize the equipment. Also the IT section has been storing surplus equipment in a hallway resulting in poor security over the equipment and obstacles to passageways. PCDA management may have deemed the formal processing of obsolete equipment as a low priority and not attempted to dispose of the equipment as required by statute. At the conclusion of our audit, IT management staff was in the process of developing procedures to ensure compliance with state regulations concerning the disposition of surplus property.

Recommendation:

The PCDA should develop and maintain procedures to comply with Commonwealth of Massachusetts regulations for the disposal of surplus property. We further recommend that the disposal of any and all equipment must be coordinated through OSD's State Surplus Property Officer.

Auditee's Response:

> *We have updated our internal control procedures to reflect the process of notifying the State Surplus Officer of any and all surplus equipment. We have contacted the Officer for guidance on our current obsolete inventory and have received approval to dispose as all of the personal computers mentioned have no modems and, thus, no ability to connect with the internet. We have researched the cost of a dumpster and will complete this process over the next few months. We will continue to review and comply with the state regulations regarding surplus property.*

Auditor's Reply:

We are pleased that the PCDA has revised their internal control policies to reflect the requirements for the surplus and disposal of obsolete computer equipment promulgated by the Commonwealth's Operational Services Division. The PCDA perpetual inventory record should reflect all surplus equipment, including the date the equipment was designated as surplus and the date of disposal.