The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2010-0046-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DISABLED PERSONS PROTECTION COMMISSION

November 10, 2007 through June 4, 2010

OFFICIAL AUDIT REPORT

JULY 21, 2010

TABLE OF CONTENTS

INTRODUCTION

The Disabled Persons Protection Commission (DPPC) was established in 1987 under Chapter 19C of the Massachusetts General Laws to establish and uphold rules pertaining to the protection of persons with disabilities. The DPPC's primary mission is to protect adults with disabilities from the abusive acts or omissions of their caregivers through investigations, oversight, public awareness, and prevention. The Commission oversees investigations conducted on DPPC's behalf by the following state agencies: the Department of Developmental Services (DDS), the Department of Mental Health (DMH), and the Massachusetts Rehabilitation Commission (MRC). The DPPC, operating from an office located in Braintree, also conducts training programs, sponsors education and outreach, investigates reports of retaliation against individuals who report abuse, and provides information and referrals on various abuse-related issues. At the time of our audit, the DPPC had 29 employees working in conjunction with five State Police investigators to protect the rights of persons with disabilities. The DPPC functions as an independent state agency, with three commissioners who report directly to the Governor and the Legislature. The Commission received an appropriation of $2,266,873 in state funds for fiscal year 2009 and an appropriation of $2,222,655 in state funds for fiscal year 2010.

The DPPC's Management Information Systems (MIS) function is responsible for managing all technology requirements of the Commission. MIS supports five file servers, 42 microcomputer workstations, and six laptop computers. MIS is also responsible for managing the routers and switches to support local area and wide area network access. The Commonwealth's Information Technology Division (ITD) provides users with network communications, including access to the Internet and the Massachusetts Management Accounting and Reporting System (MMARS), MassMail, and the Human Resources/Compensation Management System (HR/CMS).

The DPPC's primary application system is a customized product, called FileMaker Pro, which uses over 27 integrated database modules to support business functions. The FileMaker Pro application database contains confidential information regarding client background information, abuse allegations, investigations, and enforcement activities.

The Office of the State Auditor's internal control examination was limited to an evaluation of certain IT general controls over and within the Commission's IT environment, and a review of DPPC's process for the timely resolution of cases.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws (MGL), we performed a follow-up audit of certain information technology (IT) general controls. Our audit, which was conducted from February 8, 2010 through June 4, 2010, covered the period of November 10, 2007 through June 4, 2010. The scope of the audit consisted of an evaluation of the status of prior audit results in our audit report No. 2007-0046-4T, issued December 21, 2007, regarding caseload management, disaster recovery and business continuity planning, and on-site and off-site storage of backup media. In addition, we examined controls over physical security and environmental protection, inventory control over computer equipment, and whether the DPPC had appropriate policies in place regarding the protection of personal information.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results. Our objective regarding caseload management was to determine whether the DPPC had taken corrective action to ensure that the Commission was complying with requirements for completing investigation reports within the statutory time period. We also sought to determine whether the DPPC had in place adequate disaster recovery and business continuity plans to provide reasonable assurance that computer operations would be regained within an acceptable period should a disaster render the Commission's computerized functions inoperable or inaccessible. In addition, we sought to determine whether adequate procedures were in place for on-site and off-site media storage to support system and data recovery operations.

Since DPPC had relocated its offices, we sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Furthermore, we sought to determine whether a reconciliation of DPPC's inventory system of record was conducted after the relocation was completed and whether computer equipment was accurately recorded in the system of record and accounted for. Our audit objective regarding the protection of personally identifiable information was to determine whether DPPC was in compliance with the requirements set forth through MGL Chapter 93H and Executive Order 504.

Audit Methodology

To determine whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2007-0046-4T, we performed pre-audit work that included gaining an understanding of the DPPC's mission and business objectives, and reviewing prior audit work papers. We reviewed the extent to which the DPPC had implemented corrective action regarding our prior

recommendations for compliance with statutory reporting requirements of abuse cases under its jurisdiction and had addressed disaster recovery and business continuity planning and on-site and off-site storage of backup media.

To determine whether the DPPC was processing abuse cases within the mandated statutory time period, we reviewed and evaluated the documentation of the case management process and information for case tracking. We completed an aging of report completion statistics for fiscal year 2008 to February 2010. To verify DPPC's compliance with statutory requirements and regulations regarding timely resolution of cases, we compared the date of initial case intake to the date of initial assessment and response, the date of initial investigation report, and the date of completion of the investigation report. We also reviewed DPPC's caseload covering fiscal years 2008 to 2010 and the timeline for case resolution over this period. Since cases are distributed from DPPC to the Department of Mental Health, Department of Developmental Services and the Massachusetts Rehabilitation Commission, we interviewed investigation managers from each of these entities to solicit their input regarding the case process and reasons for delays in case resolution.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether the DPPC had performed any formal planning to resume IT operations should the Commission's application system be rendered inoperable or inaccessible. In addition, we determined whether risks and exposures to computer operations had been evaluated. We conducted interviews with management and support staff to determine whether the criticality of the FileMaker Pro application system had been assessed and whether a continuity of operations plan (COOP) and business continuity plan (BCP) were in place and had been adequately reviewed and tested. To evaluate the appropriateness of controls to protect backup copies of data files stored at the Commission, we reviewed relevant policies and procedures and conducted interviews of DPPC staff regarding the on-site backup copies of computer-related media. In addition, we verified off-site storage procedures for DPPC data files with staff members from the Commonwealth's Information Technology Division located at the Massachusetts Information Technology Center in Chelsea, Massachusetts.

To evaluate physical security, we interviewed management, conducted walk-throughs and inspections of the file server room and administrative office areas. Through observation and tests, we determined the adequacy of physical security controls over the areas housing IT equipment. We verified the existence of physical security controls, such as door locks and intrusion alarms, and determined whether individuals identified as being authorized to access DPPC offices were current employees.

To determine whether adequate environmental 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, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether the file server room was neat and well organized. To determine whether proper temperature and humidity controls were in place, we sought to determine whether the file server room had appropriate controls, such as a dedicated air conditioning unit.

To determine whether adequate controls were in place and in effect to properly account for computer equipment, we reviewed the computer inventory prior to the office relocation and reconciled the computer equipment listing at the former location to the current perpetual inventory record, dated February 19, 2010. We obtained and tested the inventory record of computer equipment, and interviewed the individual responsible for inventory control. To determine whether the computer equipment inventory record, dated February 19, 2010, was current, accurate, and valid, we conducted a complete test consisting of 142 computer-related items. To evaluate whether the system of record accurately and completely reflected the computer equipment, we verified the location, description, and serial numbers of hardware items listed on the inventory system of record and traced the items to the actual equipment's physical location. We reviewed the inventory record for adequacy of data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We determined whether computer equipment was properly tagged with state identification numbers and whether the identification numbers and equipment serial numbers for the computer equipment were accurately recorded on the inventory system of record. To determine whether the DPPC complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed supporting evidence that an annual physical inventory and reconciliation of IT equipment had been completed.

To assess whether the DPPC was in compliance with the requirements for the protection of personal information set forth through MGL Chapter 93H and Executive Order 504, we determined whether documented policies and procedures were in place regarding protection of sensitive data and whether hardcopy files were safeguarded. Furthermore, we determined whether required documentation, including the self-audit questionnaire, the information security plan, and the electronic security program, had been filed with the Commonwealth's Information Technology Division and approved.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office 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 version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Our examination of the status of audit results from our prior audit report No. 2007-0046-4T, issued December 21, 2007, indicated that corrective action had been taken to address control objectives regarding disaster recovery and business continuity planning and on-site and off-site storage of backup media. However, our audit tests revealed that DPPC, together with the other agencies assigned to conduct Chapter 19C investigations, were unable to process and complete all investigation reports within the statutory timeframe.

We found that adequate controls were in place relating to physical security, environmental protection and inventory control over computer. Our audit revealed that appropriate controls were in place regarding the protection of personal information, establishment of procedures for breach notification, and compliance with reporting and self-audit requirements under Executive Order 504.

Our examination of caseload management revealed that DPPC had made strong efforts to improve the efficiency of the investigative process by streamlining certain forms and procedures in investigating cases. Despite the efforts of DPPC staff and management, we found that 87% of the cases for the period of July 1, 2007 to February 28, 2010 that had been determined to meet the criteria for a DPPC investigation were not completed within the 30-day statutory requirement. We acknowledge that DPPC relies on the Massachusetts Rehabilitation Commission, the Department of Mental Health, and the Department of Developmental Services to conduct over 90% of the investigations on its behalf. DPPC has cultivated a strong partnership with these agencies to resolve cases and develop an action plan for persons with disabilities who have been or are being abused. Although each agency plays a crucial role in the investigative process, any delays encountered by these agencies inhibits DPPC's ability to expedite the completion of each investigation along with an action plan. Moreover, an increasing caseload, complexity of some of the cases, and level staffing have also contributed to the difficulty in completing investigation reports within the 30-day period. Without action plans being completed in a timely manner, persons with disabilities may be at risk of further abuse.

We determined that the DPPC had control practices in place to provide reasonable assurance that normal business operations could be resumed in a timely manner should the file servers and workstations become unavailable for an extended period. Our audit disclosed that the DPPC had developed an emergency procedures plan along with a continuity of operations plan (COOP) for their business functions. With respect to on-site and off-site storage of computer media, we determined that procedures regarding the generation and storage of backup copies of magnetic media at secure on-site and off-site locations were adequate. We confirmed that backup copies of DPPC's automated systems were being generated on a

daily basis by the Commonwealth's Information Technology Division (ITD) and that the backup tapes were being stored at a secure off-site location.

Our audit revealed that physical security controls were in place and in effect to provide reasonable assurance that computer equipment would be protected from unauthorized access and operating in a controlled environment. We found that the file server room was locked and that access was limited to authorized staff members. We observed that the new offices in Braintree, Massachusetts to which DPPC relocated in June 2009 provides a facility that is more conducive to conducting interviews with abuse victims and enhances the Commission's overall business functionality.

Our examination of environmental protection over the file server room and office areas revealed that appropriate control mechanisms were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss. Specifically, we found control objectives related to general housekeeping, air conditioning, fire prevention and detection, and emergency power and lighting would be met. With regard to fire detection and suppression controls, we observed the presence of an automatic fire suppression system, hand-held fire extinguishers, smoke detectors, and alarms. We found that each of the servers was equipped with an uninterruptible power supply system should there be a temporary loss of power.

With respect to inventory control over computer equipment, our audit tests confirmed that all items of computer equipment that were listed on DPPC's inventory system of record prior to the relocation were accurately recorded and accounted for including two items which were deemed as surplus equipment. We found that DPPC performed semi-annual physical inventories and reconciliations to address accounting requirements promulgated by the Office of the State Comptroller. Our tests indicated that hardware items were locatable, properly accounted for, and tagged.

Our audit revealed that the DPPC had developed policies and procedures to be in compliance with Chapter 93H and Executive Order 504 regarding protection of personal information. We confirmed that all required documentation, including the self-audit questionnaire, the information security plan and the electronic security program had been filed with the Commonwealth's Information Technology Division and approved. We found that DPPC maintained documentation to demonstrate that the Commission's staff were trained in accordance with the requirements of Executive Order 504.

AUDIT RESULTS

1. Prior Audit Results Unresolved – Caseload Management

Our examination of caseload management revealed that DPPC had made a concerted effort to enhance the efficiency of the investigative process by amending the report forms used by all individuals performing DPPC investigations. We found that improvements had been made in the forms used to capture information related to the potential abuse of persons with disabilities. According to management, the oversight and legal units have been restructured to improve DPPC's effectiveness in processing cases.

Our analysis of 19C case investigations completed during our audit period indicated that DPPC has become more proficient in completing investigations within the 30-day statutory requirement. We also found that the DPPC had appropriate policies and procedures in place to identify and respond to cases whereby victims of abuse may be in immediate physical or emotional danger requiring action by law enforcement. However, we found that 87% of the cases for the period of July 1, 2007 to February 28, 2010 that had been determined to meet the criteria for a DPPC investigation were not completed within the required timeframe.

Summary of Chapter 19C Case Investigations

Fiscal Year	Number of Complaint Investigations	Number Completed within 30 days	Number Completed over 30 days	Percent Completed within 30 days	Percent Completed over 30 days
2008	1,976	196	1,780	9.9	90.1
2009	1,959	281	1,678	14.3	85.7
2010 thru 2/28/10	1,378	198	1,180	14.4	85.6

DPPC relies on the Massachusetts Rehabilitation Commission, the Department of Mental Health, and the Department of Developmental Services to conduct over 90% of the investigations on its behalf. DPPC has cultivated a strong partnership with these agencies to resolve cases and develop action plans for persons with disabilities who are being abused. We note that each agency performs a crucial role in the investigative process providing valuable input to assist DPPC in finalizing investigations and in developing action plans. The increased number of cases, combined with the complexity of some of the cases, along with resource limitations, has increased the difficulty of DPPC to finalize investigations and develop action plans within the 30-day period. Without action plans being completed in a timely manner,

persons with disabilities may be at risk of further abuse. We acknowledge that the nature and extent of certain cases involve criminal investigations that require extensive time to resolve.

We determined that a shortage of resources has impacted the Commission's ability to complete investigation reports of Chapter 19C abuse investigations within the 30-day required timeframe. We found the investigators lacked critical resources, such as notebook computers and communication devices that would enhance the efficiency and effectiveness of the investigation. According to investigators interviewed, more efficient data capture could be achieved with access to technical resources having voice recognition software.

The difficulty in completing cases in a timely manner has resulted in delays in implementing remedial action plans, which are a significant part of providing protective services to victims of abuse. Without completed action plans, the potential for further abuse of victims with disabilities still exists. Moreover, the increasing caseload, which has grown by 12% over the last three years, combined with the continued delays in completing investigation reports, could significantly impact DPPC's effectiveness and operational efficiency.

The Commonwealth of Massachusetts Regulation 118, Section 5.02 outlines specific timeframes for the completion of investigations with appropriate recommendations for remediation. Specifically, the regulation requires that investigation reports must be completed within 30 calendar days of the initial report of abuse. The regulation stipulates "*The second potion of the report shall be known as the 'Investigation Report' and shall be submitted to the Commission by the investigator within 30 calendar days from the date the report of abuse was referred by the Commission for investigation.*"

Recommendation

We recognize that current budgetary constraints have limited DPPC's ability to complete Chapter 19C investigation reports within the statutory timeframe. We acknowledge the efforts of DPPC management to improve the efficiency of the investigative process by restructuring the oversight and legal units and by revamping forms to capture intake or case information. We encourage DPPC to continue to solicit additional resources to expand its use of technology by obtaining notebook computers and compatible software to be used by field investigators to facilitate the timely completion of their assigned cases. We urge continued collaboration and communication between the investigative agencies and DPPC to improve the timely completion of investigation reports in order to implement the necessary action plans to assist victims of abuse. We further recommend that the Commission continue its efforts to enhance the efficiency of the investigation process.

Auditee's Response

DPPC's Executive Director provided the following response:

> *The finding of the Office of the State Auditor's Report completed on June 4, 2010 is supported and accepted by DPPC. The Commission staff will continue to implement and work towards the completion of your recommendation.*
>
> *Regarding your recommendation concerning additional revenue services, DPPC will continue to meet with representative from ANF to explain the agency's resource limitations and caseload increases. In addition, DPPC has taken steps such as securing a new location, getting donated equipment to save money and pursuing grant opportunities to maintain and enhance operations. DPPC will continue to seek additional grants and other donated materials as without additional resources, the core mission of DPPC could be jeopardized. Through DPPC's continuous quality management efforts and in cooperation with other investigative agencies, DPPC will continue to enhance the efficiency of the investigation process to improve the timely completion of investigations and most importantly, to enhance the safety of persons with disabilities who are victims of abuse.*
>
> *Again, I understand and appreciate the value and importance of the external review process regarding State agency operations and will work diligently to continue to solicit additional resources to enhance the efficiency of the investigation process.*

Auditor's Reply

We commend the Commission's efforts to continue to address the need for additional resources and by taking steps to improve operational efficiency. We acknowledge that the new office location saves resources and provides an improved setting for conducting investigations and interviews with individuals associated with complaints of abuse. Furthermore, we acknowledge DPPC's effort to obtain donated IT equipment and grant funding needed to support the goals of the Commission. We reiterate our recommendation that DPPC management continue its cooperation and communication with the other investigative agencies to improve the timely completion of investigation reports.

2. Prior Audit Results Resolved – Business Continuity and Off-Site Storage

Our prior audit indicated that controls needed to be strengthened to ensure that mission-critical applications could be recovered within an acceptable period and that processing could be continued should IT systems be rendered inoperable due to an unforeseen event. Our prior audit had disclosed that a formal disaster recovery and business continuity plan was not sufficiently detailed or tested for the timely restoration of computer operations with regard to the FileMaker Pro application and related database management systems to support case management. With regard to off-site storage of backup media, we

had found that adequate controls were not in place to support efforts for timely restoration of DPPC's automated systems. We had recommended that DPPC implement a disaster recovery and business continuity plan for its application system, databases, and network capabilities critical to the Commission's operation and test the plan on a periodic basis. We further recommended that DPPC find a secure and easily accessible off-site location for storing backup media.

Our current audit indicated that the DPPC had taken corrective action by developing, implementing and testing a comprehensive disaster recovery and business continuity plan for its mission-critical FileMaker Pro application. Our audit disclosed that user area plans had been developed and that all employees responsible for business continuity tasks and activities had been trained in their specific duties. We found that the DPPC had also developed an emergency procedures plan along with a continuity of operations plan (COOP) for its business functions. With respect to the generation and storage of backup copies of magnetic media, we found that DPPC generated backup copies every two hours during business hours and ITD performed a nightly backup to the Massachusetts Information Technology Center in Chelsea. Our audit revealed that the backup tapes were being stored at a secure vendor facility.