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. 2007-0046-4T

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

July 1, 2005 through November 9, 2007

OFFICIAL AUDIT REPORT

DECEMBER 21, 2007

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 investigate abuse allegations and assign and oversee investigations and protective services performed by the Department of Mental Retardation (DMR), the Department of Mental Health (DMH) and the Massachusetts Rehabilitation Commission (MRC). The DPPC, operating from an office located in Quincy, 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 28 employees working in conjunction with five State Police investigators and two part-time Massachusetts District Attorney Association training coordinators 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 $1,746,915 in state funds for fiscal year 2006 and an appropriation of $1,873,986 in state funds for fiscal year 2007.

The DPPC's Management Information Systems (MIS) function is responsible for managing all technology requirements of the Commission. MIS supports 42 microcomputer workstations, eight file servers and six laptop computers. MIS is also responsible for managing the file servers, routers and switches to support local area and wide area network access, and data file exchanges with various state agencies. The Commonwealth's Information Technology Division (ITD) provides users with network communications, including access to the Internet, and access to 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 database relationship modules to support business functions. The FileMaker Pro application database, which was deployed in 1991, is an Oracle database that 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, we performed an information technology (IT) general controls examination of IT-related activities at the Disabled Persons Protection Commission (DPPC) for the period of July 1, 2005 through November 9, 2007. The audit was conducted from March 26, 2007 through November 9, 2007.

The scope of our audit included an evaluation of IT-related controls pertaining to documented policies and procedures, physical security, environmental protection, system access security, inventory control for computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of back-up copies of magnetic media. Our audit scope also included an evaluation of DPPC's ability to meet the statutory requirements for the timely resolution of cases concerning abuse of persons with disabilities receiving assistance from a caregiver.

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 DPPC's IT-related internal control framework, including policies, procedures and practices, 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 and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access into the DPPC's automated systems. Further, we sought to determine whether DPPC management was actively monitoring password administration.

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

A further objective was to determine DPPC's ability to meet the statutory requirements of Massachusetts General Laws (M.G.L.) Chapter 19C and 118 CMR to process, track, investigate, and provide adequate oversight and timely resolution of cases of abuse involving persons with disabilities.

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 personnel. To obtain an understanding of the internal control environment, we reviewed the DPPC's organizational structure, primary business functions, and relevant policies and procedures. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities, and upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of documented IT-related policies and procedures, we interviewed senior management and reviewed, analyzed, and assessed relevant IT-related internal control documentation. For the areas under review, we determined whether policies and procedures were in place, in effect, and communicated to appropriate staff.

To evaluate physical security, we interviewed senior management, conducted physical inspections, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as office door locks, locked entrance and exit doors, the presence of personnel at entry points, and whether the DPPC offices were equipped with intrusion alarms. We reviewed management policies and procedures regarding the distribution access key cards to employees. We requested and obtained a list of master key holders to the file server room and determined whether individuals identified as being authorized to access areas housing computer equipment were current employees.

To determine whether adequate environmental controls were in place to properly safeguard areas housing computer equipment from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in place, we inspected the file server room to ensure the presence of appropriate dedicated air conditioning units and/or Heating, Ventilation and Cooling systems (HVAC). In addition, we reviewed environmental protection controls related to general housekeeping procedures in the file server room, as well as the office areas housing

computer equipment. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to system applications residing on DPPC file servers. We reviewed control practices regarding logon ID and password administration and password composition by evaluating the appropriateness of documented policies and guidance provided to the DPPC personnel. We determined whether all individuals authorized to access system applications were required to change their passwords periodically, and, if so, the frequency of the changes. In order to verify that all users of the automated systems were current DPPC employees, we obtained a system generated user list containing 64 user accounts as of July 12, 2007. We compared this list to a DPPC employee listing dated May 1, 2007. We determined whether there were any changes in employment status between May 1, 2007 and July 12, 2007. The employee listing consisted of 26 full-time employees and three part-time employees. We determined that out of a total of 26 full-time and three part-time employees, all were considered by DPPC to be authorized users. In addition, we determined that there were seven user accounts assigned to non-DPPC employees consisting of five State Police officers and two District Attorney Coordinators and 28 user accounts maintained by the DPPC for administrative and technical purposes. Our audit did not include an examination of controls over network security.

With regard to inventory control over computer equipment, we evaluated whether an annual physical inventory was conducted, whether computer equipment was accurately reflected in the fixed asset inventory, and whether the computer inventory system of record was properly maintained. We also evaluated whether the computer equipment was properly accounted for in the system of record. To determine whether adequate controls were in place and in effect to properly account for DPPC's computer equipment, we reviewed inventory control policies and procedures and requested and obtained DPPC's inventory system of record for computer equipment dated March 3, 2007. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related fixed assets. We tested the inventory using a judgmental sample from both list-to-floor. To determine whether the system of record for computer equipment for fiscal year 2007 was accurate and valid, we used a judgmental sample of 71 items (54%) out of a total population of 132 items. We traced the inventory tags, location and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should network application systems be inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. To evaluate the adequacy

of controls to protect data files through the back-up of on-site and off-site magnetic media and hardcopy files, we interviewed DPPC staff regarding the creation of back-up copies of computer-related media.

To review whether the DPPC was processing abuse cases under its statutory mandate, we obtained, reviewed, and evaluated the documentation of the case management process and database tracking information for DPPC cases. 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 the fiscal years 2005 to 2007 versus the timeline for case resolution during this period. Since cases are distributed from DPPC to the Department of Mental Health, Department of Mental Retardation and 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**.**

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) 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), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Disabled Persons Protection Commission (DPPC), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to documented policies and procedures, physical security, environmental protection, inventory control over computer equipment, and access security would be met. However, our examination determined that controls over disaster recovery and business continuity planning and off-site storage of back-up computer media should be strengthened. Regarding our examination of caseload management, we found that DPPC lacked the necessary resources to process and complete investigation reports of abuse cases within the timeframe mandated by statutory requirements and regulations.

Our review of IT internal controls found that the DPPC had developed and documented policies and procedures for IT-related functions, except for business continuity and contingency planning. Our audit revealed that physical security controls at the DPPC administrative office and their file server room provided reasonable assurance that IT resources would be protected against unauthorized access. We found that employees were required to have access security cards to gain entry to DPPC office areas. We also found that the DPPC file server room was locked and that access was limited to designated senior staff members.

Our examination of environmental protection over the office areas and the DPPC file server room revealed that appropriate control mechanisms were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss resulting from environmental hazards. Specifically, we found that control objectives related to general housekeeping, air conditioning, fire prevention and detection, and emergency power and lighting would be met. We also observed that DPPC had hand-held fire suppression devices, and the area housing the file server room had an automatic fire suppression system. However, we observed that certain IT-related equipment was located on the floor of the server room. We recommend that management consider placing this equipment off the floor, in either cabinets or shelves, to prevent damage from flooding. Subsequent to the completion of fieldwork, the Commission indicated that the computer equipment had been elevated approximately 30 inches above floor level.

Regarding system access security, we found that controls for the application systems provided reasonable assurance that users were properly authorized and that only authorized users had access to the DPPC's programs and data files residing on the file servers and workstations. We found that there were comprehensive formal policies and procedures in effect for the activation, deactivation and/or changes to the level of user privileges. However, we found that DPPC needed to implement policies and procedures to ensure an appropriate frequency of password changes over its application systems. Our audit tests

revealed that the timeframe for changing passwords was not adequate, due to the sensitive nature of the data, and that the policies should require more frequent changes. We also recommended that password composition be expanded to eight alpha/numeric characters to conform to the Commonwealth's Information Technology Department standards. Subsequent to the completion of fieldwork, the Commission indicated that it had implemented a requirement that passwords consist of at least eight alpha/numeric characters and be changed on a more frequent basis.

With respect to inventory control over computer equipment, we found that the DPPC was adhering to the policies and procedures promulgated by the State Comptroller's Office and had conducted an annual physical inventory and reconciliation of computer equipment. Our audit revealed that DPPC's inventory record contained adequate fields of information to identify, describe and locate the computer equipment. Our tests revealed that all 71 computer-related items tested out of the population of 132 items were locatable, properly accounted for, and tagged.

With respect to business continuity and off-site storage of computer media, we found that controls needed to be strengthened to ensure continued processing of mission-critical applications should an unforeseen event occur. Our audit 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 systems to support case management.

Although appropriate procedures and controls were in place for on-site storage, we found that DPPC lacked adequate controls over off-site storage for weekly back-up copies of computer media for application systems and data files. Our audit revealed, contrary to sound business practices, that an employee of the DPPC was taking weekly back-up media, including confidential information pertaining to abused victims, to his personal residence. We recommend that DPPC management find a secure, easily accessible, off-site location, sufficiently far enough away from its primary processing site, to store its back-up copies of computer-related media.

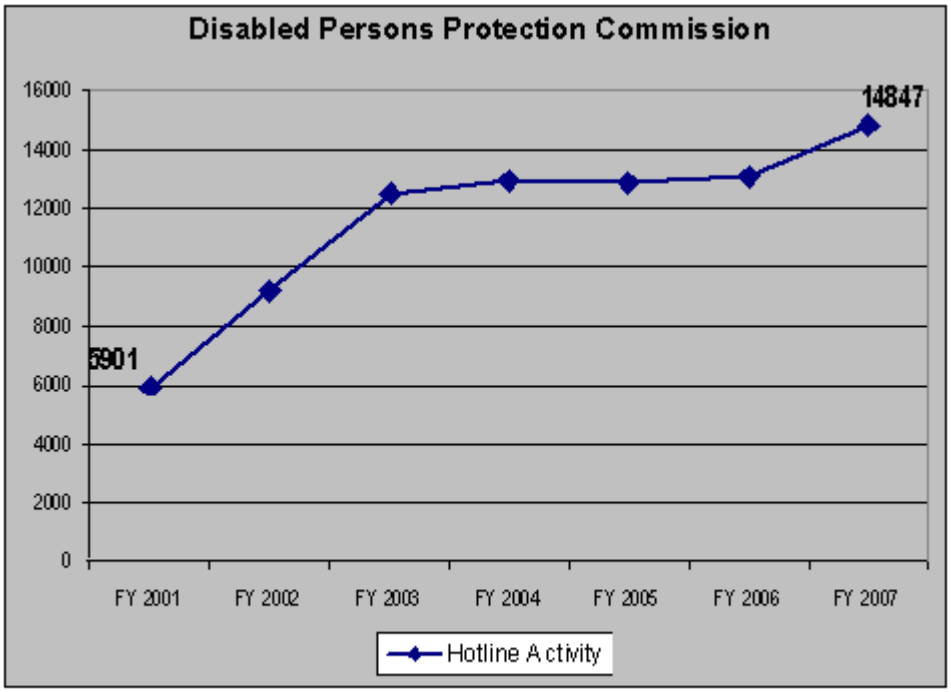
Regarding our review of the DPPC's case management process, we found that the case intake and initial case classification process was efficient and effective. We also found that DPPC had cultivated a strong partnership with investigative agencies to resolve cases and develop an action plan for disabled persons being abused. Regarding our examination of DPPC's caseload management, we found that due to resource limitations, the DPPC was not able to comply with statutory requirements and state regulations requiring the resolution of cases within 30 calendar days from the date the case was referred for investigation. Without action plans being completed through investigation reports in a timely manner, persons with disabilities may be at risk of further abuse.

AUDIT RESULTS

1. Caseload Management

Our audit revealed that investigations needed to be completed by DPPC in a more timely manner to ensure investigations are resolved in accordance with statutory and regulatory requirements, and that action plans to assist persons with disabilities who have been victims of abuse can be implemented. Our audit revealed that current DPPC management has done an admirable job in informing human service providers, law enforcement agencies, and the general public about applicable laws and regulations, as well as about the resources available to persons with disabilities who are victims of abuse. However, we determined that a critical shortage of resources, combined with an increasing caseload, has significantly impacted DPPC's ability to meet statutory requirements in completing cases on a timely basis. Without an increase in resources, DPPC's ability to comply with mandates may significantly worsen, and continued protective services for abused victims may be jeopardized.

The DPPC's hotline serves as the main source of cases reported to the Commission. The DPPC has experienced significant increases in the number of hotline calls, and consequently the number of investigations it must oversee. Our audit revealed that in fiscal year 2007, the Commission received a total of 14,847 calls to its hotline, representing a 152 percent increase from fiscal year 2001.



Our audit of the abuse tracking database revealed that the DPPC had controls in place and in effect for the initial assessment of abuse reports. We found that DPPC investigators conducted risk

assessments of initial abuse reports within the 24- hour timeframe mandated by Massachusetts General Law Chapter 19C for the protection of victims and a determination as to whether the cases met the established criteria. Those cases found to meet this criteria were referred by DPPC to appropriate human service agencies (the Department of Mental Health, the Department of Mental Retardation, or the Massachusetts Rehabilitation Commission) for investigation and for the development of protective service action plans.

The Commonwealth of Massachusetts Regulation (CMR) 118, Section 5(3) 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 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…*"

Our audit of closed investigations from fiscal year 2005 through fiscal year 2007 revealed that although DPPC has a dedicated and knowledgeable investigative staff, the volume and nature of the cases is exceeding DPPC's capabilities, as well as the other agencies involved, to process the cases in a timely manner. We found that in fiscal year 2005, 1,077 (89 %) of the closed cases exceeded the 30-day statutory mandate for completing an investigation report. Our analysis indicated that 874 (84%) cases from fiscal year 2006 and 653 (77%) cases from fiscal year 2007 were not resolved within the required timeframe. We also acknowledge, however, that there are a number of cases that cannot always be processed within the required timeframe, due to pending law enforcement investigations, legal issues and the complexity of the individual abuse cases.

The difficulty in completing cases in a timely manner has resulted in delays in implementing remedial action plans, which is a significant part of providing protective services to abused victims. Without completed action plans, the potential for further abuse of victims with disabilities may still exist. Additionally, the increasing caseload, combined with the continued delays in completing investigation reports, could significantly impact the efficiency and effectiveness of DPPC.

Recommendation:

We recommend that DPPC continue to ensure its independence by seeking additional financial resources in order to effectively and efficiently address the complex incidents of abuse and neglect committed against persons with disabilities. We further recommend that DPPC closely monitor its allocation of resources against the increasing caseload per investigator. We continue to urge collaboration and communication between the investigative agencies and DPPC to ensure the timely resolution of abuse cases within the established and critical 30-day timeframe. We encourage DPPC to

continue to solicit additional resources to address the growing caseload demand on its own investigative staff.

Auditee's Response:

The second and final area identified in the auditor's report as needing strengthening is the completion of statutory abuse investigations in a timelier manner so that protective actions may be implemented more timely. As the audit identified, DPPC's "critical shortage of resources combined with an increasing caseload has significantly impacted DPPC's ability to meet statutory requirements." The Commission staff is comprised of dedicated and highly skilled professionals in the area of abuse investigation and the protection of individuals with disabilities. DPPC, in cooperation with other agencies, continually monitors, assesses and modifies the process to insure that the limited resources available are used in the most effective and efficient manner. The Commission shares the opinion of the Auditor's Office that DPPC requires an increase in its resources to maintain its independence, but more importantly, to continue to provide the protection necessary for one of the Commonwealth's most vulnerable populations; persons with disabilities.

Auditor's Reply

We commend the efforts made by the Commission to attempt to resolve and close cases in a timely manner. The Commission should continue to monitor its resources, seek additional funding from all sources whenever possible, and collaborate with other human service agencies to ensure timely action on cases.

2. Business Continuity Planning and Off-Site Storage

We determined that the Disabled Persons Protection Commission (DPPC) had not formalized a comprehensive disaster recovery and business continuity plan for restoring critical functions in the event that automated systems were rendered inoperable or inaccessible. We acknowledge that DPPC was aware of the need for business continuity planning. However, at the time of our audit, we determined that DPPC's business continuity plan consisted of a draft copy of their Continuity of Operations Plan.

To ensure that a formal business continuity plan is documented and available, the DPPC should document recovery strategies with respect to various disaster scenarios. Without a comprehensive, formal, and tested recovery strategy, DPPC may experience delays in re-establishing mission-critical functions, such as its FileMaker Pro application, various database information, and acquiring and installing IT resources needed to restore IT processing, as well as to timely recover backup information from off-site storage. The lack of a detailed, tested plan to address the resumption of processing capabilities may hinder the recovery of essential and confidential data should a disaster render IT systems inoperable. Without a formal, tested recovery strategy, DPPC may experience difficulties delivering

essential services to abused persons in an efficient and effective manner in accordance with its stated mission.

The objective of business continuity planning is to help ensure timely recovery of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for the DPPC to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate contingency and recovery plans. To that end, DPPC should assess the extent to which it is dependent upon the continued availability of information systems for all required processing and operational needs, and develop its recovery plans based on the critical aspects of its information systems.

Our audit revealed that contrary to sound business practices for providing appropriate controls for off-site storage of back-up media, DPPC permitted storage of back-up media at an employee's personal residence. Since we could not validate the security of the off-site location, there is no assurance that the back-up media was secure and would be readily available to assist recovery efforts. In addition, the ability to provide adequate security of the off-site information may be at risk.

Recommendation:

We recommend that DPPC management work to develop, implement and test a disaster recovery and comprehensive business continuity strategy for its application system, databases, and network capabilities critical to the Commission's operation. We recommend that DPPC formally assess the impact of the loss of IT operations, and determine the extent to which contingency plans can be developed to address recovery of critical business operations. We further recommend that the DPPC develop user area plans appropriate to the Commission's IT processing environment and information accessibility requirements. Once a formalized plan has been adopted, we recommend that DPPC test the plan to assess its viability and establish a process for routinely updating the plan based on changes to recovery efforts, technology, business processes, or staffing. The DPPC should ensure that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained.

Regarding the off-site storage of weekly back-up copies of computer media, we recommend that DPPC management find a secure and easily accessible off-site location and prohibit storing back-up media at employees' personal residences.

Auditee's Response:

The audit result relating to DPPC's disaster recovery and business continuity plan and the need for its strengthening, the Commission recognizes that the written plan provided for the audit is incomplete and it was presented as a draft for the purpose of the audit. The Commission continues to develop and test controls that will insure that critical information and business continuity is protected against unpredictable and unpreventable events. Regarding the Commission's practice of storing back-up tapes in a fireproof safe at the IT Coordinator's home office has been addressed. The Commission has leased a safety deposit box at Bank of America on Hancock Street in Quincy Center. Back-up tapes are changed two times weekly with the most current back-up tape being stored in the safety deposit box. In addition to securing a safety deposit box, and to strengthen DPPC's Continuity Of Operations Plan (COOP), the Commission is negotiating with the Commonwealth's Information Technology Division (ITD) to secure server space in the ITD data storage facility in Chelsea Massachusetts to initiate electronic information vaulting. Ultimately, DPPC's plan is to have a separate and parallel data network running at the ITD Chelsea location. This network will be a mirror image of DPPC's working databases and allow the Commission to resume normal IT operations with no loss of data in the event of a total loss of the Quincy IT equipment. However, the cost of hardware and software prevents the development and implementation of this system at this time

Auditor's Reply

We acknowledge that the Commission is aware of the need for business continuity planning for its mission-critical and essential application systems. However, we urge the Commission to work toward developing a comprehensive business continuity plan. We recommend that DPPC establish recovery plans and procedures to address business continuity planning, and that the plans be periodically reviewed, tested, and updated as necessary.

We are pleased that storage of offsite back-up media will be remedied through the Commission's leasing of a safety deposit box, and that the tapes will be stored in a secure location rather than at an employee's personal residence.