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. 2006-0247-7T

OFFICE OF THE STATE AUDITOR'S REPORT
ON THE EXAMINATION OF BUSINESS CONTINUITY PLANNING
AND SELECTED INFORMATION TECHNOLOGY CONTROLS
AT THE DEPARTMENT OF MENTAL RETARDATION
NORTHEAST REGION (REGION III)

December 15, 2005 through May 15, 2008

OFFICIAL AUDIT REPORT
DECEMBER 3, 2008

TABLE OF CONTENTS

INTRODUCTION

The Department of Mental Retardation (DMR) is organized under Chapter 19B, Sections 1 to 18, of the Massachusetts General Laws and is placed within the purview of the Executive Office of Health and Human Services. The DMR is comprised of 24 area offices that operate within four regions located throughout the Commonwealth.

DMR's primary mission is to provide a variety of support services, such as residential services, employment assistance, help for families to care for family members at home, transportation, treatment, monitoring, and care to the Commonwealth's mentally retarded citizens. During the 2008 fiscal year, DMR provided a variety of services to its clients. Through various state-operated programs and contracts with 250 private providers, DMR assisted approximately 32,000 clients. In conjunction with community-based programs, DMR served approximately 926 clients in six developmental centers, such as Monson Developmental Center, Glavin Regional Center, and the Hogan Regional Center. The Hogan Regional Center functions as the Northeast Region's intermediate care facility (ICF-MR).

DMR's Northeast Region (hereinafter referred to as Northeast Region or Region III) includes 65 cities and towns in Essex County and certain areas of Middlesex County. Region III is comprised of five area offices located in Arlington, Beverly, Haverhill, Lowell, and Wakefield and the Hogan Regional Center's ICF in Hathorne and provided services to 7,531 individuals and their families during fiscal year 2008. The Northeast Regional Office's administrative and business offices are located on the grounds of the Hogan Regional Center, Hathorne, Massachusetts. The Office is managed by the Northeast Regional Director. The regional office is responsible for the management of the regional staff, area offices and community-based programs in the cities and towns located within Region III. The Hogan Regional Center is managed by a Facility Director.

Regarding housing options, Region III, through Northeast Residential Services (NRS), managed 67 state-operated community homes that provided services to 287 clients. The Region also contracted with 45 vendors who provided services in over 587 residential locations to 1,804 clients. In addition, the Hogan Regional Center provided residential services to 150 clients, various day services to live-in clients and community residents, and short-term evaluation and treatment. (See Appendix I, page 20 for a graphical representation of the physical organization of the Northeast Region.)

As of the close of fiscal year 2008, 1,583 Department staff were employed in Region III. The staff included 494 employees who worked at the Hogan facility and reported to the Facility Director, 225 who worked for the regional and five area offices, and 864 who worked for the NRS. These employees reported to the Northeast Regional Director and were paid by State appropriation. In addition, 18 staff from DMR central office departments in Boston, such as investigations, legal, human rights, and quality enhancement were located at the regional office. Four University of Massachusetts staff were assigned to the Northeast Region to ensure that revenue would be received by Region III for services rendered to facility residents at Hogan and individuals who received case management and other community services. Furthermore, University of Massachusetts staff billed the Social Security Administration (SSA) for DMR staff who monitored individuals' SSA benefits and/or clients who participated in entitlement programs, such as Medicaid and Supplemental Security Income (SSI).

Computer operations at the Hogan Regional Center were supported by one file server and approximately 218 microcomputer workstations configured in a local area network (LAN). The workstations that were installed at the Center in the administration, recreation and seven other buildings were connected through fiber optic lines to the file server in the administration building. File servers installed at Region III's five area offices were connected to the file server at Region III through DMR's Central Office The file server installed at Region III and the servers installed at five area offices were connected through a dedicated phone line to the DMR Central Office. The DMR file server was connected to the Commonwealth's wide area network (WAN) to provide access to the Information Technology Division's (ITD) mainframes and file servers installed at the Massachusetts Information Technology Center (MITC). The WAN provides access to the Human Resource Compensation Management System (HR/CMS) and to other mission-critical applications, including Meditech and the Home and Community Services Information System (HCSIS) installed at MITC.

With respect to the Management Information Systems (MIS) function at the Northeast Region, an Executive Office of Health and Human Services (EOHHS) Site Manager/Network Administrator is responsible for managing data files residing on the file server and for generating backup copies of programs and data files onto magnetic media. Because the EOHHS site manager functions as the IT Staff Training Coordinator, he is also responsible for training in the Region and application assistance to computer users. A DMR employee functions as a database manager. The EOHHS is responsible for the management of the file servers and the associated network, including the workstations.

Region III uses several mission-critical and essential applications to carry out its mission and business functions. Access to mission-critical applications, such as Meditech and HCSIS, was provided through the WAN to the mainframe and file servers at MITC. Meditech collects information on all DMR inpatients and outpatients receiving services; HCSIS's five modules reports information, such as a patient's individual health record, death data, and medication occurrences.

Physician orders for patients, diet plans and medications for inpatients were accessed through Datastat, an application controlled by the Pharmacy Distribution Center located in Tewksbury, Massachusetts. In addition, an R-Base application installed on a standalone workstation at Region III was used to account for client funds for approximately 275 residents at the Hogan facility and group homes in the Northeast Region. Furthermore, data files on Region III's file server included human resource information regarding industrial accidents, Northeast Residential Services' client information, legal databases, and Purchase of Service contracts.

Our Office's examination focused on a review of business continuity planning, including provisions for on-site and off-site storage at Region III, physical security and environmental protection over and within the MIS Office and the file server room, and inventory control over computer equipment and grounds equipment maintained at the Hogan Regional Center.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an information technology audit at the Department of Mental Retardation's (DMR) Northeast Regional Office (Region III) for the period covering December 15, 2005 through May 15, 2008. The audit was conducted from December 15, 2005 to September 30, 2006, and from March 24, 2008 to May 15, 2008. The scope of our audit included an examination of controls regarding business continuity planning, including provisions for the storage of backup copies of magnetic media, and physical security and environmental protection controls over and within the Management Information Systems (MIS) Office, file server room, and on-site storage area. We examined inventory control practices for computer equipment and grounds equipment.

Audit Objectives

Our primary audit objective was to determine whether Northeast Region management had taken corrective action to resolve audit results regarding business continuity planning identified in our prior IT audit report (No. 2002-0247-4T). In conjunction with our examination, we sought to determine whether an effective business continuity plan had been implemented that would provide reasonable assurance that mission-critical and essential IT operations could be restored within an acceptable period should automated functions be rendered unavailable or inaccessible. Furthermore, we determined whether backup copies of magnetic media were being stored on site and off site.

We determined whether adequate physical security controls were in place and in effect over and within the MIS Office and file server room to restrict access to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources. We sought to determine whether sufficient environmental protection controls were in place within the file server room to provide a proper IT environment and to detect damage or loss of IT resources. In addition, we determined whether adequate controls were in place to properly account for computer equipment installed in business offices at the Hogan Regional Center and for grounds equipment maintained at the Center.

Audit Methodology

To determine the audit areas to be examined during our IT audit, we reviewed the prior IT audit results regarding business continuity planning that were documented in our prior IT audit report No. 2002-0247-4T, issued May 13, 2002. Through interviews with management and staff from the DMR Central Office and Northeast Region, reviews of relevant documents, such as selected portions of the Northeast Region's "IT Policies and Procedures," we gained an understanding of the status of business continuity planning and backup procedures for magnetic media at the Region. We identified mission-critical and essential business functions and the application systems used to support them. We conducted a preliminary review of internal controls related to physical security and environmental protection controls over and within the MIS Office that houses the file server room. Furthermore, we conducted a walkthrough of the MIS Office and the file server room and reviewed key management for the MIS Office.

To gain an understanding of software applications and data files backed up at the Northeast Region, staff responsible for generating backup copies, and whether backup procedures were documented, we identified written documentation regarding backup schedules and interviewed the MIS Director and Network Administrator. We initially interviewed Region management to identify physical security and environmental protection controls over the on-site storage location for backup copies at the Hogan Regional Center. We conducted a site visit to on-site storage area.

As part of our pre-audit work, we reviewed the Northeast Region's network configuration. We determined the roles of DMR Central Office, Northeast Region, and the Executive Office of Health and Human Services regarding inventory management of computer equipment. We also determined the role of DMR Central Office and the Northeast Region regarding the maintenance of grounds equipment at the Hogan Regional Center. We performed a risk analysis for the audit areas under review. Based upon our pre-audit procedures, we developed the audit scope and objectives.

To determine whether adequate controls were in place and in effect to prevent and detect unauthorized access to the MIS Office and file server room, we inspected physical access controls, such as appropriately locked entrance and exit doors, the presence of a receptionist in the administration building, intrusion detection, and whether visitor badges were being issued. We reviewed control procedures documented in Region III's "Northeast Region IT Business Continuity Plan," as of April 2008 regarding distribution of keys to staff authorized to access the MIS Office. We performed a detailed inspection of the MIS Office and file server room.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of fire detectors and alarms, fire control methods, and emergency power generators and lighting in the administration building. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of IT equipment. To evaluate temperature and humidity controls, we determined whether adequate air conditioning units were available for the file server room. We determined whether an uninterruptible power supply (UPS) had been installed to prevent loss of data through a controlled shutdown of power. Furthermore, we checked for the presence of an automated fire suppression system and water detection devices within the file server room, and whether the server and other computer equipment was on racks raised above floor levels to prevent water damage.

To assess the adequacy of business continuity planning, we determined whether corrective action had been taken regarding our recommendations documented in the prior audit report. In conjunction with our examination, we determined whether a written, tested business continuity plan was in place, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. During our initial audit work, conducted from December 15, 2005 to April 30, 2006, we reviewed a variety of documentation regarding business continuity planning provided by DMR Central Office, Northeast Residential Services, and the Northeast Region. This documentation included control procedures related to generating backup copies of magnetic media at Region III and on-site storage of the backup copies for the Northeast Region and five area offices. We determined whether there was an off-site storage location for Northeast Region for backup copies of magnetic media.

We reviewed the Continuity of Operation Plans (COOP) that was prepared by the DMR Central Office, as of October 14, 2005 and updated as of January 11, 2007, and the COOP prepared by Northeast Residential Services (NRS), as of June 2006. According to the Massachusetts Emergency Management Agency (MEMA), the COOPs should be prepared "in accordance with Department of Homeland Security Headquarters COOP Guidance Document, as of April 2004, that provides a structure for formulating a COOP plan; Presidential Decision-67, 'Ensuring Constitutional Government and Continuity of Operations,' and Commonwealth of Massachusetts Executive Order No. 144 that requires all Commonwealth agencies and local communities to prepare for emergencies and disasters, and to provide emergency liaisons to MEMA for coordinating resources, training, and operations."

In conjunction with our examination of business continuity planning, we interviewed DMR Central Office management, including the Commissioner, Deputy Commissioner, Chief Information Officer, and the Director of Facilities. We sought to determine the role of the Central Office regarding the development of business continuity planning at the DMR's regions and facilities and provisions for off-site storage. In addition, to determine the status of business continuity planning, we interviewed Region III managers, including the Budget Director, Regional Operations Manager, and MIS Director. In addition, we interviewed selected managers and staff at Region III's administrative and business offices, Northeast Residential Services, the North Shore Area Office located in Beverly, and the on-site pharmacy regarding their knowledge of the region's business continuity planning, their participation in the process, and their opinions regarding the business impact of a loss of automated systems over specific time periods.

To determine the adequacy of control practices regarding the backup of magnetic media at the Hogan Regional Center, we interviewed the MIS Director and Network Administrator responsible for generating backup copies and reviewed specific schedules for generating backup copies of magnetic media. We reviewed the procedures for the distribution to, and return of backup copies from, the off-site storage location at a different DMR Office. Because Region III processed data using application systems residing on the file server at the Central Office, we reviewed control procedures for generating backup copies of software residing on the Central Office's file servers. We did not review the Information Technology Division's (ITD) backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting System (MMARS), the Human Resources Compensation Management System (HR/CMS), or software applications, such as Meditech processed at the Massachusetts Information Technology Center (MITC). Our audit did not include an inspection of the on-site or off-site storage areas for backup copies of data files for MMARS, HR/CMS, or Meditech.

From March 24, 2008 to May 15, 2008, we reviewed the status of business continuity planning at the Northeast Region. We determined whether any new initiatives had been developed since our initial audit work. In that regard, we interviewed Region III managers, including the Budget Director, Regional Operations Manager, and MIS Director. We also interviewed DMR's Chief Information Officer (CIO) and IT Operations Manager regarding plans for the implementation of electronic vaulting of backup copies development of another alternate processing site. In addition, we reviewed additional documentation, such as the Northeast Region's COOP, as of April 2008 and the "Northeast Region IT Business Continuity Plan," as of April 2008. In addition, we reviewed the "DMR Regional Model Emergency Procedures and Plan, Northeast Regional Office," as of May 1, 2008 and the "DMR Site Evacuation Plan," as of April 2008.

Furthermore, we reviewed the Northeast Region's "Security Plan," as of April 2008, that was developed in conjunction with DMR Central Office. The "Security Plan" lists various IT-related components, including disaster recovery planning. The "Security Plan" documents a stated requirement for each element, such as implementation of a disaster recovery plan for each regional and area office, the status of the requirement, a plan to implement the requirement, and a completion date. We determined whether the additional documentation, including the Northeast Region COOP, as of April 2008 and the IT Business Continuity Plan, as of April 2008, included sufficient information to support the resumption of Region III's normal business operations in a timely manner.

To determine whether adequate controls were in place and in effect to properly account for computer equipment, we reviewed and evaluated the appropriateness of inventory control practices and procedures. Because the Executive Office of Human Services has managed inventory control for selected Executive Office agencies, such as the DMR since fiscal year 2006, we interviewed the Executive Office's Director of IT Infrastructure to determine the role of EOHHS regarding the accounting for IT resources, such as computer equipment. We also interviewed the DMR's Assistant Commissioner for System Integration.

We obtained and reviewed the inventory record for computer equipment, as of June 30, 2006. We reviewed the content of selected data fields, such as state identification number, serial number, cost and equipment location to determine whether sufficient information was available to perform audit tests, including confirmation of items listed on the record to the actual equipment. We also obtained and reviewed the inventory list of grounds equipment. We reviewed control procedures regarding the tagging of computer equipment purchased for the Hogan Regional Center and determined whether computer equipment was properly tagged with state identification numbers and that the tag numbers were accurately recorded on the inventory record. In addition, we determined whether the serial numbers attached to the computer equipment were accurately recorded on the hardware inventory record.

To determine whether the inventory record for computer equipment for the Hogan Regional Center, as of June 30, 2006, was current, accurate, and complete, we confirmed the inventory list provided by the auditee to the actual computer equipment on hand. We selected a statistical sample of 53 (11%) of 467 pieces of computer equipment located at the Hogan Regional Center for review. We compared the tag numbers, when available, and serial numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record. In addition, we selected a judgmental sample of 20 pieces of computer equipment installed at the Hogan Regional Center and compared serial numbers affixed to the items to the corresponding

items listed on the inventory record. Regarding inventory control practices over grounds equipment, such as a lawn mower, backhoe, and snow blower, we reviewed control procedures regarding grounds equipment with the Northeast Region's Budget Director and members of the Hogan Regional Center's maintenance staff. We reviewed Region III's list of six pieces of grounds equipment. We confirmed the six pieces of grounds equipment, such as the mower and sander recorded on Region III's list to the actual pieces of equipment located at the Hogan Regional Center. In addition, we reviewed surplus property records for computer equipment and grounds equipment, as of October 10, 2002, November 24, 2004, and June 6, 2005 provided to us as of September 2006.

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 computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on our audit of the Department of Mental Retardation's Northeast Region, we found that IT resources, including the file server and workstations installed at the Management Information Services Office and file server room were properly safeguarded, environmentally protected, and accounted for. We also determined that, with few exceptions, selected workstations installed throughout the Hogan Regional Center were properly accounted for. Our audit indicated, however, that inventory controls over grounds equipment maintained at the Center needed to be improved. Although we found that important controls were documented in a variety of business continuity related-documents, the Northeast Region needed to take additional corrective action to fully address the recommendations in our prior audit report in order to provide reasonable assurance that normal business operations could be resumed should automated systems become unavailable for an extended period. Moreover, we determined that on-site storage needed to be improved for backup copies of magnetic media at the Hogan Regional Center.

Our audit found that adequate physical security controls were in place over and within the administration building and the Management Information Office, housing the file server room to provide reasonable assurance that access to the file server would be restricted to only authorized persons and that the server and IT-related media would be safeguarded from damage or loss. We determined that telephone operators were on duty 24/7 in the administration building and that all visitors were required to sign-in and out. We found that appropriate key management practices were in place for the MIS Office; the Office was staffed continuously during normal business hours; and the door to the Office kept closed when staff was not present. The file server room was located in a non-public area, the room could not be accessed from outside the building, and access to the room was restricted to EOHHS and DMR IT staff.

We determined that adequate environmental protection controls, such as smoke detectors and fire alarms, and an emergency power supply were in place in the administration building to help prevent damage to, or loss of, IT resources. Our audit disclosed that the file server room was well organized, temperature and humidity levels within the room were appropriate, and an uninterruptible power supply (UPS) device was in place to permit a controlled shutdown and to prevent a sudden loss of data. A hand-held fire extinguisher was located within the server room. The server was placed on a rack above floor level to prevent water damage, was subject to air quality and temperature monitoring, and an alarm system was in place to detect changes in temperature. According to DMR management, regular inspection and maintenance programs were in place for fire alarms, emergency power supply, UPS, and heat and ventilation systems.

With respect to business continuity planning, we found that the Northeast Region was not covered by an approved, comprehensive, and tested business continuity plan. Our audit revealed that Region III had documented important control practices in four separate documents, the "Northeast Region Continuity of Operations (COOP)," as of April 2008, "Northeast Region IT Business Continuity Plan," as of April 2008, and two emergency/evacuation plans covering the Northeast Region's administrative and business offices and five area offices. Control practices, such as alternate processing sites, a listing of various disaster scenarios and associated instructions to follow, and emergency/evacuation plans were recorded in one or more of the four different documents. However, we determined that none of the individual documents or a combination of all four documents provided sufficient recovery strategies or resources to guide the Northeast Region to resume business operations in a timely manner.

To strengthen controls, we recommend that the Northeast Region, in conjunction with DMR Central Office, address the following control weaknesses: perform a criticality assessment and risk analysis; complete portions of the "Northeast Region IT Business Continuity Plan," such as the restoration of mission-critical systems; enhance certain control practices, such as the listing of disaster scenarios; and develop an emergency contact list, including IT personnel. Northeast Regional management needs to ensure that the COOP and the "Northeast Region IT Business Continuity Plan" document are consistent with each other. In addition, the Northeast Region should test the "Northeast Region IT Business Continuity Plan," document the test results, and take any corrective action if required. Regional management should integrate appropriate portions of the four business continuity-related documents and additional control practices into one comprehensive IT business continuity plan. We determined that on-site storage for backup copies of magnetic media at the Hogan Regional Center needed to be improved to ensure that appropriate temperature and humidity controls are provided.

Our audit revealed that, except for 11 pieces of computer equipment designated as surplus property, inventory tests of workstations recorded on the inventory record, as of June 30 2006, indicated that the computer equipment was safeguarded and properly accounted for. However, controls over grounds equipment, such as mowers and backhoes, needed to be improved. We recommend that the Northeast Region develop an inventory record, including state identification number, serial number, cost, location, and date of purchase. The Northeast Region should comply with the Office of the State Comptroller's regulations regarding fixed-asset management, including annual physical inventory and reconciliation.

AUDIT RESULTS

Business Continuity Planning

Our audit disclosed that although DMR's Northeast Region had developed a variety of documents that included important control practices regarding business continuity planning, none of the written documentation individually or collectively provided sufficient recovery strategies or resources to restore normal business operations in a timely manner should automated systems be unavailable for an extended period. We found that backup procedures for magnetic media processed on the file server installed at Hogan Regional Center were adequate. However, DMR needed to strengthen controls regarding the on-site storage location for the backup copies. This location was also used as the off-site storage site for backup copies from the five area offices situated in the Northeast Region.

Deficiencies pertaining to business continuity-related control practices included, but were not limited to DMR's Northeast Region's failure to:

- Perform a criticality assessment and risk analysis;
- Complete the portions of the "Northeast Region IT Business Continuity Plan," such as the listing of mission-critical systems;
- Ensure that information, such as listing of alternate processing sites and mission-critical systems are consistently stated in the COOP and the "Northeast Region IT Business Continuity Plan;
- Document all potential disaster scenarios and instructions to follow for each specific event;
- Develop a contact list, including IT personnel to be notified in the event of an emergency and include all communication information, such as landline telephone numbers, cell phone, and e-mail;
- Develop user area plans documenting procedures to follow for each business unit should automated systems be unavailable so that business activities can continue;
- Document detailed procedures regarding restoration of network services; and
- Develop schedules for testing the "IT Business Continuity Plan," document the tests performed, and any corrective action taken.

We determined that, at the close of our audit, Northeast Regional management had developed four documents that addressed various aspects of business continuity planning. These documents included the "Northeast Region COOP," as of April 2008, the "Northeast Region IT Business Continuity Plan," as of April 2008, the "Department of Mental Retardation Site Evacuation Plan,"

as of April 2008, and the "DMR Regional Model Emergency Procedures and Plan," Northeast Regional Office, as of May 1, 2008.

We found that Region III had documented important control practices required by the Continuity of Operations (COOP) Plan, as of April 2008. The purpose of the COOP was to "provide for the immediate continuity of essential functions of an organization at an alternate facility for up to 30 days in the event an emergency prevents occupancy of its primary facility." The COOP addressed important elements fundamental to business continuity planning, such as a listing of essential business functions, designation of the Northeast Region's mission-critical systems; general requirements for relocation to and use of the emergency relocation site in (hereinafter referred to as the alternate processing site), protection of vital records, orders of succession, and delegation of duties and responsibilities for continuity of operations to officials and selected manager.

Control practices documented in the COOP were insufficient to provide standards and guidelines for the resumption of normal business practices in a timely manner should automated systems be unavailable. For example, there was no requirement for a formal risk analysis and criticality assessment or procedures to restore network resources. Furthermore, we could find little evidence that a formal risk analysis and criticality assessment, that is integral to business continuity planning, had been performed. The DMR's "Security Plan," as of April 2008, stated that "no risk assessment process was in place at the Northeast Region."

We found that the Northeast Region also had a documented "Northeast Region IT Business Continuity Plan," as of April 2008. The IT business continuity plan was drafted to comply with COOP requirements that the basic COOP elements should "work in concert with business continuity and disaster recovery plans" to allow "for uninterrupted delivery of the Agency/Organization's essential functions." Our review of the plan indicated that many control practices needed to be clarified, developed, or enhanced. We found that Region III had designated an alternate processing site at the North Shore Area Office and several additional, tentative sites, such as State Police offices. However, COOP's Summary Information listed the North Shore Area Office and three additional sites not listed in the "Northeast Region IT Business Continuity Plan." All mission-critical and essential systems, such as MIS/IT and inventory control" listed in the COOP were not similarly listed in the "Northeast Region IT Business Continuity Plan." Restoration of critical functions stated in the "Northeast Region IT Business Continuity Plan." was not completed. Although the business continuity plan broadly described disruptions in network services or damage to equipment that would require relocation

to an alternate processing site, all potential disaster scenarios, such as natural disasters, major fires, threats, had not been addressed. Moreover, detailed instructions to follow should a catastrophic event occur were not documented. Procedures regarding loss of mission-critical systems, such as Meditech, residing on ITD mainframes and servers were not addressed, nor was there documentation of user area plans. Furthermore, the business continuity plan did not classify types of delays and disruptions in IT systems or describe recovery strategies and designated time frames for mission-critical and essential systems under various disaster scenarios.

We found that although the IT business continuity plan briefly referred to the DMR Central Office's role in replacing equipment, the plan did not include detailed procedures regarding the replacement of the file servers or workstations, copies of agreements for service and hardware replacement, or time frames for completion of these tasks. Although the plan described the monitoring of communication systems and problem resolution of loss of network resources, the plan did not include detailed procedures to restore network resources.

Our review of business continuity-related documents indicated that DMR had documented two separate emergency/evacuation plans. The Northeast Region had developed the "DMR Regional Model Emergency Procedures and Plan, Northeast Regional Office," as of May 1, 2008, "to prepare staff for emergencies and interruptions of operation." The plan included instructions to follow should an emergency or disruption of operations occur, such as contacting DMR Central Office and a contact list of important managers located at the Hogan Regional Center, and fire, police, and ambulance telephone numbers. Further, the plan included procedures to follow in the event of a fire or bio/chemical emergency, instructions for fire drills, medical emergencies, and personal responsibility regarding the protection of computer data. The Northeast Region had also documented "DMR Site Evacuation Plan," as of April 2008 for Northeast Regional offices located at the Hogan Regional Center and the five area offices under the purview of Region III. We were not provided with documentation that either plan was reviewed and approved or tested.

According to the COOP, the staff from the Northeast Region's MIS and the Central Office will develop a plan for the systematic testing of relevant systems, including a test of server backup procedures, a test of communication protocol and alternative communication systems, and the use of critical systems at one alternative site. At the date of our audit, Northeast Region did not provide us with a specific schedule of tests, test results, or any corrective action taken to address problems encountered during the tests. IT personnel stated that network recovery tests had been conducted at Region III. However, none of the test results was documented.

Failure to adequately test a comprehensive business continuity plan does not allow DMR to attain reasonable assurance that the recovery plan will effectively address various disaster scenarios. Moreover, the lack of tests of recovery strategies may impede the periodic review and modification of the plan. If the plan were not modified when needed, the Region may not be able to rely upon the plan's current viability due to factors, such as changes in the risks and threats to the IT environment, including application systems, network and communication changes, security requirements, electronic interfaces, personnel, logistics, and organizational changes. Without a comprehensive, formal, and tested recovery and business continuity plan, including required user area plans, critical client services, such as intake and eligibility determinations provided through Region III's administrative office, could be significantly impeded.

During our audit we interviewed selected managers and staff located at the Hogan Regional Center and a selected area office. Because much of the work performed by the managers and staff we interviewed was performed using hardcopy format, access to automated systems did not appear to be critical for a few days up to two weeks. However, according to DMR managers, the loss of Meditech, which is a mission-critical system, would immediately effect business operations. We found that the loss of mission-critical systems, processing requirements, and the use of manual procedures was not addressed in the plan. Should temporary manual procedures be included in the plan for mission-critical systems, such as Meditech, the procedures should be tested and staff trained in their use.

Our audit indicated that on-site storage of backup copies of magnetic media residing on the file server at the Hogan facility or stored at the facility by area offices needed to be improved. We found that at the Hogan facility backup media was stored in an open safe that lacked appropriate temperature and humidity controls and was cluttered with surplus computer equipment.

We acknowledge that all regional and area office file servers were backed up electronically on a daily basis and backup from the regional offices was sent weekly to a different DMR Office mitigating the potential loss of backup tapes stored at the Hogan facility. However, the loss of backup media at the Hogan facility could significantly hamper client services and the processing of administrative and financial transactions. Although the availability of backup is improved by daily electronic backup and weekly off-site storage, significant additional time would be required to reconstruct information from these sources compared to backup maintained in a secure on-site location.

The objective of business continuity planning is to help ensure the continuation 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 practices and industry standards for computer operations support the need for each entity to have an ongoing, business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available. Region III, in conjunction with the DMR Central Office, should perform a risk analysis of the systems and clearly understand the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage the systems, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence.

Recommendation:

We recommend that to strengthen business continuity planning, the Northeast Region should:

- Gain an understanding of generally accepted computer industry standards, such as Control Objectives for Information Technology (CobiT) regarding a business continuity-planning framework outlining business continuity, recovery and contingency objectives and procedures for mission-critical and essential business operations. The framework includes a criticality assessment and risk analysis, policies; procedures; defined responsibilities; documented management control practices; organizational controls, such as steering committee, recovery teams, and oversight functions; and assurance mechanisms. Assurance mechanisms would include internal reviews, testing, and independent examination and verification. The framework should also include senior management assignment of enterprise responsibility for additional recovery strategies and adequate provisions for on-site and off-site storage.
- Perform an enterprise-based risk analysis and criticality assessment to ensure that all functional areas and business processes are evaluated and updated, if necessary, the risk analysis results for IT operations. The risk analysis and criticality assessment should include all external partners, such as the federal government and outsourced services, such as ITD.

- Review the list of disaster scenarios to determine whether all potential scenarios have been identified, and update the list accordingly with respect to likelihood and impact at Region III's administrative office. Develop and update recovery and business continuity strategies for each of the disaster scenarios identified.
- Reconfirm Northeast Region's understanding of the relative importance of business functions and the potential impact of a loss IT processing support. Northeast Region should formally rank mission-critical, essential, and less essential business process functions and IT processes for development and update of disaster recovery, business continuity and contingency plans.
- Obtain an understanding and adequate level of assurance of disaster recovery and business continuity plans for required services and support from all mission-critical and essential business partners and third-party providers.
- Establish a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, Northeast Region should establish targets for acceptable time periods by which mission-critical IT operations need to be recovered.
- Ensure that appropriate resources are available at alternate processing sites, such as suitable hardware and communication equipment; supplies; adequate space in which to resume operations; backup copies of all required application programs, data files and system utilities; documented policies and procedures; and sufficient personnel.
- Develop and perform appropriate levels of testing to provide Northeast Region with sufficient assurance as to the viability of recovery and business continuity plans. Tests should be performed on control practices that can be reviewed and evaluated independently of the test of recovery strategies in conjunction with the implementation of the alternate processing site. Once tests are completed, test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.
- Review business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. We recommend that subsequent to testing the business continuity plan, the plan should be updated when needed to provide reasonable assurance that it is current, accurate, and complete. The completed plan should be distributed to all appropriate staff members, including Northeast Region officials, senior management, IT staff, and ITD administrators and staff.
- Train the Northeast Region staff in the execution of the business continuity plan under emergency conditions. Ensure that all key business process and IT management and staff have adequate skill and knowledge to carry out all tasks and activities outlined in recovery and business continuity plans.
- Aggressively pursue the implementation of electronic vaulting with DMR Central Office for backup of magnetic media stored at the Hogan Regional Center.
- Seek an on-site location for magnetic media stored at the Hogan Regional Center that provides appropriate temperature and humidity controls.

Auditee's Response:

Business Continuity Planning

Over the past 5 years, Department of Mental Retardation experienced numerous changes in management of IT operations, systems and equipment. Although the Region no longer has any direct or independent responsibility for IT operations, we realize that our staff, our providers and ultimately the people that we serve could potentially experience negative effects if information systems were not readily available. We also realize we cannot wait for direction from DMR Central Office or EOHHS. Our use of computer systems is reflective of the direct work we do with individuals and families, and although paper files at each area office and Hogan are our most comprehensive documents, we must have contingency plans to use if shared systems and communication are unavailable.

We are working to revise and expand our BCP plans to reflect these changes in DMR operations and to ensure that they are consistent with other emergency policies and procedures. We are currently developing independent and comprehensive plans for each of our 5 Area Offices, the Regional Office (including related field staff from DMR Central Office and UMass) and the Hogan Regional Center. Certain mission critical systems, such as Email, Meditech and HCSIS, are used by all divisions of DMR, but the impact on particular users and inter-dependencies must be analyzed and documented.

The replacement of the 6 servers and the rollout of the new desktop configuration to all DMR users will provide us with an opportunity to test our plans. These initiatives will be completed by mid 2009. We anticipate that our Business Continuity Plans will be fully drafted by then and reviewed by key managers and representative users. We will plan to test components of the plans and will update and revise as necessary. These plans will be reviewed and updated annually by the end of each calendar year.

On Site storage:

Magnetic media is backed up nightly with appropriate records maintained. Physical access security and environmental protection of storage is adequate and in place. The storage area is located within the locked area of the MIS space. The backup media are stored in a fire proof . . . safe. However, it appears that maybe appropriate temperature and humidity controls may not be up to standards. Other important MIS equipment was stored in the safe for security reasons. The Region will research alternative locations for media storage, if temperature and humidity controls cannot be put in place. DMR, Central Offices' new over the wire (tape less) back-up system is currently being used nightly, to back-up all user files on the server.

Auditor's Reply:

We agree with the Northeast Region's management decision to proceed with comprehensive, contingency planning for the Northeast Region, Hogan Regional Center, and the five area offices. Further, we concur with the decision to review, evaluate, and document the impact of the loss of mission-critical systems, such as e-mail and Meditech on the Region's work with individuals and families. We reiterate that a risk analysis and criticality assessment should be completed prior to the development of business continuity planning. We are pleased that the Northeast Region

plans to test components of the plan, revise the plan as needed, and review and update the plan annually. Further, we note that the Region has developed an emergency contact list of critical personnel, including IT staff and appropriate contact information.

We are pleased that Region management will research alternative locations for storing backup copies of magnetic media. We reiterate that the Northeast Region, working in conjunction with the DMR Central Office, would achieve the most effective business continuity planning. We will review the status of business continuity planning during out next IT audit.

Department of Mental Retardation
Physical Organization of Northeast Region
Administrative Offices, Residences, DMR Central Office, and Area Offices

North Shore Area Office	Merrimack Valley Area Office	Central Middlesex	Metro North Area Office	Lowell Area Office
(Beverly)	(Haverhill)	(Arlington)	(Wakefield)	(Lowell)

DMR Central Office
Boston

DMR Northeast Regional Office
450 Maple Street, Danvers

Administration Building
MIS Office/Network Room
Administrative and Clinical Staff
Meeting/Training Space

3 Hathorne Circle
Northeast Residential Services (NRS)
67 residential programs serving 287 clients

Recreation Building
Assistive Technology
Training/Conference Space
Recreational facilities for Hogan staff, residents, and community

5 Hathorne Circle
Intake and Eligibility
Regional Clinical Staff
Central Office Field Staff
University of Mass staff for revenue collections

1 Hathorne Circle	**2 Hathorne Circle**	**4 Hathorne Circle**	**6 Hathorne Circle**
Residence for 35 clients	Residence for 35 clients	Residence for 60 clients	Residence for 20 clients North Shore Enterprises Day Programs

Notes

All buildings beneath the line are located on the grounds of the Hogan Regional Center.

The patient residences (#1,2,4,and 6 Hathorne Circle) are physically connected to the Administration building

Central Office field staff assigned to Region III and located at #5 Hathorne Circle: (a) Investigations, (b) Legal, (c) Quality Enhancements, and (d) Human Rights

Summary of Internal Control Practices
Department of Mental Retardation
Northeast Region
as of May 15, 2008

Report Page Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
10	Physical Security: Hogan Regional Center, Administration Building, MIS Office, and File Server Room	Provide reasonable assurance that only authorized staff can access MIS Office and file server so that, loss or damage is prevented	Control over access to MIS Office and file server room through controls, such as designated facilities manager, operator's on duty 24/, locked doors, appropriate key management	In effect	Yes	Inadequate
10, 11	Environnemental Protection: Hogan Regional Center, Administration Building, MIS Office and File Server Room,	Provide reasonable assurance that the file server are adequately protected form loss or damage	Proper ventilation, fire alarms, fire extinguishers, temperature controls, water sprinklers, posted emergency procedures, equipment raised over floor level	In Effect	Yes	Inadequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place, but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Appendix II
Summary of Internal Control Practices
Department of Mental Retardation
Northeast Region
as of May 15, 2008

Report Page Ref	Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Documentation
11, 12	Business Continuity Planning	Provide reasonable assurance that Region III can restore essential and mission-critical functions should automated systems be rendered inoperable.	Current, formal, tested business continuity plan; periodic review and modification of plan; plan implemented, distributed, and staff trained in its use	Insufficient	Yes	Inadequate
10 - 12	On-site storage, Hogan Regional Center	Provide reasonable assurance that magnetic media is available should automated systems be rendered inoperable	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage adequate; storage area is in a separate on-site location	Insufficient	Yes	Adequate
11	Inventory Control over IT-related Resources	Provide reasonable assurance that IT resources are properly safeguarded, accounted for in the inventory record, and reported on, when appropriate, to oversight department	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	In Effect	Yes	Adequate
11	Inventory Control over Grounds Equipment	Provide reasonable assurance that grounds equipment is properly safeguarded, accounted for in the inventory record, and reported on, when appropriate, to oversight department	Maintenance of an up-to-date inventory record; equipment tagged with state ID tags; annual physical inventory and reconciliation performed	Insufficient	No	Inadequate

Additional Auditee Response

Additional Auditee Response regarding Audit Conclusion

Inventory Control over "Grounds Equipment":

The NE Region and Hogan have maintained an existing Inventory Control database based upon the procedures and policies in the "NE Regions Fixed Asset Management and Inventory Control Manual." As of June 2008, an updated and revised inventory control data base/file for Hogan Center has been in place, recording such information as, the cost, purchase date, location, serial number and DMR tag number. This has been specifically updated for grounds equipment, as all other inventory has complied with the Office of the State Comptrollers regulations. Existing procedures based on the "NE Regions Fixed Asset Management and Inventory Control Manual." has been put in place for grounds equipment inventory. This will be included in our "NE Regions Fixed Asset Management and Inventory Control Manual."

Physical Security:

The MIS office is located in a separate and discrete office space, off the main hallway of the Administration building. The office holds 3 staff, all of which have MIS roles and responsibilities. They each have work space away from the server room. The server has it's own designated area The hallway door to this large space, is divided into 4 separate rooms, has a key entry system that can be locked at all times. It does not house any equipment, storage or supplies, where staff, other than MIS would need access to the work area or the server room. An independent door, with locks, will be put on the server room to further increase the security of the room. All updates to the Physical Security of the MIS room will be included in our Disaster/Recovery Plan for the Region and Hogan Center.

The Region and Facility has Risk Analysis checklist that was completed in April 2008.

Environmental Protection:

The MIS server room is climate controlled, properly ventilated, with smoke detectors, fire extinguisher, equipment is raised over floor level, etc. Posted emergency procedures are located in a conspicuous place for easy recognition, review and access. All Environmental Protection s for the MIW server room will be included in our Disaster/Recovery Plan for the Region and Hogan Center. After the completion of construction in the administration building, all three (3) smoke detectors will be hardwired for improved fire protection of the server room.

Auditor's Reply:

We agree with the Northeast Region's management decision to implement a database that includes appropriate information, such as cost and DMR identification number for all property and equipment, including IT resources and grounds equipment. Development of an additional database regarding IT resources should be done in conjunction with the database maintained by EOHHS

responsible for the control and management of DMR's IT resources. We concur with the decision to include inventory control procedures regarding grounds equipment into the "Northeast Region's Fixed Asset Management and Inventory Control Manual." We will review the status of inventory control over grounds equipment at our next IT audit.

We are pleased that appropriate physical security and environmental protection controls were in place over and within the MIS Office and file server room that we reviewed during our audit. Moreover, we are pleased that the Northeast Region plans to further strengthen certain physical security and environmental protection controls and include these control practices in the Disaster Recovery Plan for the Northeast Region and Hogan Regional Center.