The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2007-1405-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY–RELATED CONTROLS AT DEPARTMENT OF MENTAL RETARDATION SOUTHEAST REGION

July 1, 2005 through February 9, 2007

OFFICIAL AUDIT REPORT

JUNE 29, 2007

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 (EOHHS). The DMR is comprised of 23 area offices located throughout the Commonwealth that operate within five regions: DMR Central, Central/West Region, Metro Region, Northeast Region, and Southeast Region. DMR's primary mission is to provide a variety of support services and care that include residential services, employment assistance, transportation, and treatment for the Commonwealth's mentally retarded citizens. Through various state-operated programs and contracts with private providers, DMR assists approximately 32,000 clients each day.

DMR's Southeast Region includes 78 cities and towns in Barnstable, Bristol, and Plymouth County. The Southeast Region is comprised of a Regional Office in Carver and seven area offices located in Fall River, New Bedford, Taunton-Attleboro, Cape Cod and the Islands, Plymouth, Brockton, and Weymouth as well as the Southeast Residential Services. At the time of our audit, 1,046 department staff were employed in the Southeast Region (SRS). The staff included 44 employees who work at the Southeast Regional Office, 209 who work in the area offices, and 793 who work in Southeast Residential Services that operate state-sponsored community homes. In addition, 38 staff from DMR's central office were located at the Southeast Regional Office working in areas such as Investigations, Legal, and Human Rights.

The DMR Southeast Regional Office's computer operations are supported through a local area network (LAN), consisting of one file server to which 88 workstations are connected throughout the facility. The LAN provides connectivity through telecommunication lines to two file servers at the DMR central office in Boston and the Commonwealth's wide area network (WAN).

The DMR central office's SQL server processes applications such as MediTech, which is the medical information application; Home and Community Services Information System (HCSIS), which allows service providers and DMR to file clinical information and reports on incidents, medication occurrences, restraints, and investigations; and Impact, which is an accounting application used in conjunction with the Massachusetts Management, Accounting and Reporting System (MMARS). These applications are supported through a cluster of file servers located at the Massachusetts Information Technology Center (MITC) in Chelsea. The applications receive technical support, including the backing up of all mission critical magnetic media, through DMR staff at MITC. The Southeast Region's file servers are connected through a WAN to the Information Technology Division's (ITD) mainframe, providing connectivity for access to the Human Resource Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System.

Our Office's examination focused on selected general controls, such as documented policies and procedures, physical security and environmental protection, system access security, inventory control over computer equipment, and business continuity planning.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an audit of information technology (IT) related general controls at the Department of Mental Retardation's (DMR) Southeast Region. The audit, which was conducted from August 23, 2006 through February 9, 2007, covered the period of July 1, 2005 through February 9, 2007. The scope of our audit included an evaluation of IT-related controls pertaining to IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and the on-site and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect within the Southeast Regional Office to support a properly controlled IT processing environment. In this regard, we sought to determine whether the Southeast Regional Office's IT-related internal control environment, including documented policies, procedures, and practices, provided reasonable assurance that IT control objectives would be achieved to support the Southeast Regional Office's mission.

We sought to determine whether adequate physical security controls were in place and in effect to restrict access to IT resources to authorized users only in order to prevent unauthorized use, damage to, or loss of IT-related equipment. We also determined whether sufficient environmental protection controls were in place to prevent and detect damage to, or loss of, computer equipment and data.

With regard to inventory control over computer equipment, we evaluated whether an annual physical inventory was conducted, computer equipment was accurately reflected and accounted for in the inventory record, and the system of record was properly maintained. Regarding system access security, we sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to the Southeast Regional Office's automated systems. We evaluated whether procedures were in place to prevent and detect unauthorized user access to automated systems and IT resources, through the local area network (LAN) file server and microcomputer workstations. In addition, we determined whether the Southeast Regional Office was actively monitoring password administration.

Regarding system availability, we sought to determine whether adequate business continuity and user plans were in effect to provide reasonable assurance that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render IT systems inoperable or inaccessible. Moreover, we determined whether adequate on-site and off-site storage was being provided for backup copies of magnetic computer media residing on Southeast Region's file server to assist in recovery efforts.

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 IT internal control environment, we reviewed the Southeast Region's organizational structure and primary business functions. We performed a high-level risk analysis, including areas of possible fraud and abuse, and assessed the strengths and weaknesses of the IT internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our examination of controls pertaining to IT policies and procedures, we interviewed senior management from both the DMR and the Southeast Region and obtained and reviewed existing IT-related policies, standards, and procedures. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also reviewed the degree of oversight provided by DMR and EOHHS to support Southeast Region's IT functions.

To determine whether computer equipment was adequately safeguarded from damage or loss, we reviewed physical security over computer equipment storage areas by interviewing senior management and security personnel and conducting walkthroughs. To determine the adequacy of physical access controls regarding computer equipment located throughout the Southeast Regional Office, we conducted site visits to the file server room, office areas, and to the on-site and off-site storage locations. Through observation and interviews, we confirmed the presence of physical security controls, such as locks and alarms, and determined whether access to the computer equipment storage areas was restricted to only authorized personnel.

To evaluate 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 suppression methods, such as sprinklers and hand-held extinguishers; power surge protectors; uninterrupted power supply (UPS); and emergency lighting in the administrative offices. We also reviewed general housekeeping procedures to determine whether only appropriate items were placed in the file server room or in the vicinity of computer equipment. To determine whether proper temperature

and humidity controls were in place, we reviewed for the presence of appropriate dedicated air-conditioning units in the file server room and the on-site and off-site storage locations. We also reviewed control procedures to prevent and detect water damage to automated systems and backup media for on-site and off-site storage of magnetic media.

To obtain an understanding of access security controls, we reviewed the Southeast Region's access security policies and procedures designed to prevent unauthorized access to the application systems and data files accessible through the Southeast Regional Office's workstations. Our test of system access security controls included a review of access privileges for employees who were authorized to access DMR's application systems and the Southeast Region server. To determine whether system access security was being properly maintained through the management of user IDs and passwords, we compared the LAN and the MediTech system user list provided by the Southeast Region to a roster of all Southeast Regional Office employees. We determined whether procedures were in place to ensure that the security administrator was promptly and properly notified of changes in personnel status (e.g., employment termination, job transfer, leave of absence) so that user IDs and passwords were being promptly deactivated from the system or access privileges were being appropriately modified. We compared a list of all 312 staff members assigned to the Southeast Region listed as authorized MediTech users and 624 LAN user accounts obtained from the security administrator to a list of all the Southeast Region current employees to verify that all of the authorized users were current employees. We also reviewed password administration controls, such as activation and deactivation, password length and composition, and the frequency of password changes.

To determine whether adequate controls were in place and in effect to properly account for the Southeast Region's computer equipment, we reviewed relevant inventory control procedures, obtained and tested the inventory record of computer equipment, and interviewed individuals responsible for inventory control. We reviewed the inventory record for the adequacy of data elements 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 serial numbers attached to the equipment were properly recorded on the selected hardware inventory listing. We also performed data analysis on the inventory and made note of any unusual distribution characteristics, duplicate records, or unusual or missing data elements. To determine whether the IT-related inventory record, dated November 8, 2006, was current, accurate, and valid, we tested a randomly selected sample of 139 out of 609 hardware items located through the Southeast Region's regional and area offices. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand. In addition, to verify the

relevance and completeness of the system of record for computer equipment, we judgmentally selected 56 additional items of computer equipment installed throughout the Southeast Region's offices and determined whether they were properly recorded on the inventory record.

We also confirmed the existence of the five laptops listed on the inventory record and in the custody of the Southeast Regional Office. To determine whether the Southeast Region complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting the Southeast Regional Office's performance of an annual physical inventory and reconciliation of IT equipment. We determined whether computer equipment had been purchased or leased during our audit period. Further, to determine whether the Southeast Region complied with Commonwealth of Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that the Southeast Region plans to request Commonwealth approval to dispose of as surplus. Finally, to determine whether the Southeast Region was in compliance with Chapter 647 of the Acts of 1989 regarding reporting requirements for missing or stolen assets, we reviewed incident reports for missing or stolen IT-related equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess the adequacy of business continuity planning, we evaluated the extent to which the Southeast Region had user area plans that could be activated, in conjunction with DMR's disaster recovery plans, to resume IT-supported operations should mission-critical and essential application systems be rendered inoperable or inaccessible. We interviewed the Southeast Region and DMR Central management to determine whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated. To determine whether controls were adequate to ensure that IT operational information on the Southeast Region's file servers would be available should the automated systems be rendered inoperable or inaccessible, we interviewed management responsible for creating backup copies of magnetic media at the Southeast Regional Office. We reviewed the adequacy of provisions for on-site and off-site storage for backup copies of critical media and conducted a site visit to the off-site storage location to assess the adequacy of physical security and environmental protection.

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

AUDIT CONCLUSION

Based on our audit, we found that information technology-related (IT) controls in place at the Department of Mental Retardation's Southeast Region provided reasonable assurance that objectives regarding documented IT-related policies and procedures, physical security, environmental protection, generation of on-site and off-site backup copies of computer media, and system access security would be met. However, our audit indicated that the Southeast Regional Office, in conjunction with the DMR, needed to strengthen their overall business continuity and user area plans and the procedures for storing on-site and off-site backup computer media to ensure timely restoration of business operations and on-going system availability. In addition, we determined that sufficient control practices were not in place to provide reasonable assurance that the computer equipment was properly accounted for in the DMR's inventory system of record.

Our examination of controls pertaining to IT-related policies and procedures revealed that DMR provided management oversight of IT-related functions at the Southeast Regional Office. Our review of the IT internal control environment indicated that the Southeast Region followed authorized and approved IT-related internal control policies and procedures that had been developed by DMR.

Our examination of physical security revealed that controls provided reasonable assurance that the Southeast Regional Office's IT resources were safeguarded from unauthorized access. Our review of the areas storing the file server revealed that the door is locked at all time when unattended, only upper-level management personnel were issued keys, and all visitors are escorted when in the file server room. Our review of areas storing workstations disclosed that the Operations Manager or a designated employee make a nightly round to verify that all the office doors are locked and that all areas are secure. Although physical security appeared to be adequate, written and approved policies and procedures would further ensure that assets would be protected from unauthorized access, use, damage, or theft.

We determined that adequate environmental protection controls were in place to ensure that IT operations were providing a proper environment to safeguard IT equipment located in Southeast Region's server room and areas storing workstations. We found that adequate environmental protection, such as fire prevention and detection controls, smoke detectors, alarms, and fire extinguishers, were in place in areas containing computer equipment. In addition, we found that an uninterruptible power supply was in place for the server to help prevent damage to, or loss of, the data should electrical power be abruptly lost. In addition, the Southeast Region had an emergency procedure plan in effect. Our audit also disclosed that the server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to the Southeast Region's microcomputers and data files and programs residing on DMR's file servers. We also determined that administrative password protection and changes to passwords were adequately controlled through DMR's IT networks. However, our review of user account management indicated that controls over administration of user IDs and passwords needed to be strengthened to provide reasonable assurance that access privileges would be deactivated or appropriately modified should Southeast Region employees terminate employment or incur a change in job requirements.

Our tests revealed that out of the 312 Meditech users as of August 8, 2006, 305 were current employees, five had resigned, and two were unknown users. In regards to the test of LAN users we found that out of the 624 LAN users, 621 were current employees and three had resigned. Our examination revealed that the user accounts had been deactivated for these former employees. We recommend that the Southeast Regional Office, in conjunction with DMR Central Office, reconcile the active user list to a current employee list on a routine basis to ensure timely deactivation of user privileges as outlined in the Southeast Region Logical Access Security policy statement. The auditee indicated as part of their response that corrective action would be taken to terminate user privileges in a timely manner for individuals no longer requiring access to the Southeast Region's application systems.

Regarding system availability, our review indicated that although the Southeast Region had identified an alternate processing site, controls pertaining to disaster recovery and business continuity planning needed to be strengthened. We found that the Southeast Regional Office, in conjunction with DMR, did not have comprehensive documented plans to address disaster recovery and business continuity for automated operations. Although we found through interviews with Southeast Region and DMR management that the Southeast Regional Office had certain procedures in place in the event of a disaster or emergency, the Southeast Regional Office, in conjunction with DMR Central Office, had not formally documented these procedures in a comprehensive user area plan and business continuity strategy that would address a loss of IT processing capabilities. Although the Southeast Regional Office indicated they would rely on DMR for instructions should systems become inoperable or inaccessible, the Southeast Regional Office did not have formally documented user area plans that would identify courses of action for Southeast Regional Office staff to follow under various disaster or emergency scenarios. In addition, although we determined that the Southeast Region had implemented procedures for the generation of weekly backup copies of their non-essential data, year-end copies of this data were stored in a fire-proof safe in the Operations Manager's office. We did determine that procedures regarding the generation of backup copies of magnetic media at a secure off-site location were adequate for mission-critical applications processed through DMR Central for the area offices.

With respect to inventory control of computer equipment, our audit indicated that controls needed to be strengthened to provide for the proper accounting of IT resources. Our audit revealed that the Southeast Region could not provide a comprehensive inventory listing of computer equipment on hand as required by the Internal Control Guide For Departments promulgated by the Office of the State Comptroller. The absence of a reliable inventory of computer equipment hinders the Southeast Region and its ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives. However, we did receive a list of computer equipment for the Southeast Region from DMR, dated November 2006. Our data analysis of the listing provided to us by DMR indicated that the Southeast Region had 609 IT hardware items.

The data analysis indicated that although there were data fields for end user, manufacturer, model, serial number, device and location, there were no fields of information with respect to associated value, historical cost, acquisition date, state tag numbers, and purchased dates. In addition, an annual physical inventory and reconciliation was not being performed by the Southeast Region to assist in verifying the accuracy and completeness of the inventory record. Since historical cost was not maintained for the computer equipment, the inventory system of record could not be used by the Southeast Regional Office to provide the value of IT resources under their control. In addition, our audit test revealed of the selected computer equipment of 139 items from the DMR Central Office's system of record indicated that 129 pieces of computer equipment were located in the correct location, and the remaining 10 items were located, but in different locations. Our test of 56 hardware items that were traced from multiple physical locations back to the inventory listing indicated that all 56 pieces of computer equipment were recorded correctly on the inventory record. Furthermore, an inventory test of the notebook computers indicated that all five notebooks were located at the Southeast Regional Office.

AUDIT RESULTS

1. Inventory Control over Computer Equipment

Our audit revealed inventory control over computer equipment must be strengthened to provide for the proper recording and accounting of computer assets. We found that the Southeast Region could not provide a comprehensive inventory system of record for computer equipment and was not performing an annual physical inventory and reconciliation of the system of record. Our audit revealed that procedures needed to be implemented or enhanced regarding the recording, maintenance, and reconciliation of the inventory system of record for computer equipment.

The Southeast Region's inventory listing provided to us by DMR Central Office included 609 items of IT-related equipment. Our analysis of DMR's inventory system of record indicated that although data fields, such as description, user name, serial number, and location, were present, the listing lacked data fields for state tag numbers, associated value, historical cost, equipment status, and acquisition date to properly account for IT-related computer equipment and support asset or IT configuration management. The inventory listing should include a data field for "condition of item" to support IT configuration management by noting the asset's status, such as being repaired, obsolete, or designated for surplus. The inclusion of this information will help support IT infrastructure decisions and ensure that DMR's IT-related computer equipment will be properly accounted for during the annual physical inventory.

Recording historical cost and acquisition date in inventory systems of record is required by Commonwealth of Massachusetts regulations for all departments to provide a comprehensive, auditable inventory record of fixed assets. By failing to record the historical cost of purchased computer hardware items and their purchase dates on the inventory system of record, DMR and the Southeast Region were not in compliance with the Office of the State Comptroller's fiscal year fixed-asset requirements and Office of the State Comptroller (OSC) Memorandum No. 313A. In addition, inventory valuation for computer equipment could not be analyzed and evaluated.

Based on a statistical sample of 139 pieces of computer equipment selected from the inventory record, we verified selected computer equipment by serial numbers and the recorded location of the computer equipment as listed on the DMR's inventory record. We found that 129 of the 139 items that were selected from the system of record were at the locations indicated on the inventory record. The remaining 10 items could be found in different locations than the location noted on the listing. Furthermore, to verify the integrity and completeness of the inventory system for computer equipment, we selected 56 additional items of computer equipment from floor locations within the Southeast Region and determined whether the equipment was properly recorded on the DMR's inventory system of record. We found that all 56 items selected were recorded correctly on the inventory record.

However, our audit indicated that the Southeast Region's monitoring of IT equipment needed to be strengthened. Specifically, Southeast Region senior management had not performed an annual physical inventory during our audit period and could not provide verification records for our audit period supporting any complete annual physical inventory or a reconciliation of IT-related equipment to DMR's inventory system of record. The absence of fully documented policies and procedures regarding inventory verification hinders the Southeast Region's ability to ensure the integrity of its inventory system of record as it pertained to IT-related assets.

We believe that the weaknesses in inventory control were the result of lack of adequate monitoring, management oversight, and proper assignment of asset control responsibilities. Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989 states, in part, that " ... the agency shall be responsible for maintaining accountability for the custody and use of resources and assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

Recommendation:

We recommend that the Southeast Region, in conjunction with DMR Central, enhance and implement internal control policies, procedures, and practices regarding inventory control of computer equipment in the areas of recording and inventory verification to help ensure that the Southeast Regional Office properly accounts for its computer equipment. The Southeast Regional Office should implement appropriate assurance methods, such as independent verification, physical inspection, reconciliation, and oversight, to ensure that inventory controls are in place and in effect. We recommend that procedures be established to ensure that the inventory record for computer equipment is maintained on a perpetual basis, allowing management to use the inventory for accounting and IT configuration management purposes.

We recommend that the Southeast Regional Office adapt its current control guidelines to comply with the Office of the State Comptroller's "Internal Control Guide for Departments" regarding asset management. We also recommend that the Southeast Regional Office benchmark its policies and procedures to generally accepted control practices for IT configuration management. Once DMR and Southeast Region senior management have approved the policies and procedures, the policies and procedures should be distributed and instructed to the appropriate staff.

With respect to IT configuration management, we recommend that the data fields in the IT inventory be expanded to include the purchase date, associated value, historical cost, state tag number, and the condition and status of the computer equipment. In addition, data fields may include information related to hardware or software maintenance. We recommend that all IT resources be included on the inventory to support IT configuration management objectives.

The Southeast Regional Office should implement these control procedures to help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that the Southeast Region can generate a complete record of all IT-related equipment on a perpetual basis. The Southeast Regional Office's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

The Southeast Regional Office should also perform an annual physical inventory and reconciliation of the inventory system of record. The perpetual inventory record of IT resources, including computer equipment and software, should be periodically verified through reconciliation to computer equipment acquisition, records of lost or stolen equipment, and disposal records.

Auditee's Response:

> *IT Operational services are provided to the Southeast Region by EOHHS. The Region has an on-site presence 2 days a week. We also have access by e-mail and phone if necessary. Regional staff will meet with this individual in order to address the issues identified in this audit result. We need to clarify the day-to-day responsibilities of the IT staff person and those of the regional staff. Also included in any discussions will be staff representatives from DMR's Central Office MIS. We will work within this group to establish a base inventory for the Region. Someone will be authorized to place, relocate, and/or remove MIS equipment as needs dictate. All staff will be notified of this process. In addition the Southeast Region will request that EOHHS expand the fields in the existing inventory report. The new fields will include those identified in the finding. Specifically these fields are: cost, condition, acquisition, installation date, and status of the resource. Once the fields are added to the inventory a decision will be made as to who updates the inventory.*

Auditor's Reply:

We are pleased that the Southeast Region is working in conjunction with DMR and EOHHS to improve inventory controls. We believe a single comprehensive inventory control system for all IT-related assets located throughout DMR facilities is an important component for the overall internal control structure. Identifying a single point of accountability for movement of computer equipment will assist in maintaining an accurate system of record for computer equipment. Strengthening inventory control procedures will improve the integrity of the system of record regarding computer equipment and assist the Southeast Region, DMR, and EOHHS in making IT infrastructure and configuration management

decisions. We believe that controls to ensure adequate accounting of computer equipment will be strengthened by adding the additional fields of information and by perpetually updating the inventory record when changes in status or location occur and then routinely reconciling the physical inventory to the system of record.

2. Business Continuity Planning

We determined that although procedures regarding the generation of weekly backup copies of magnetic media for non-essential systems were adequate, overall business continuity planning needed to be improved. We determined that the Southeast Region, in conjunction with the DMR Central and the EOHHS, had developed an Emergency Procedures and Plan document along with a Continuity of Operations Plan (COOP). The COOP plan addressed the criticality assessment of application systems. However, the plan was not specifically comprehensive to address the processing needs of the Southeast Region, since certain risks and exposures to computer operations and an alternate processing site had not been addressed. The COOP plan had also never been tested to ensure its viability.

An effective disaster recovery plan for DMR and individual Regional Offices should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring IT systems and activities either at the original site or a designated alternate-processing site. Furthermore, appropriate Southeast Region area plans should outline recovery or contingency steps with detailed steps to be followed to efficiently restore business operations in a timely manner. The Southeast Region area plans should be coordinated with overall enterprise-based business continuity or DMR business continuity plans. Without adequate disaster recovery and contingency planning, including required Southeast Region-user area plans, the Southeast Region was at risk of not being able to gain access to automated systems. A loss of processing capabilities could adversely affect business functions and result in unnecessary costs and significant processing delays. The lack of a detailed, tested plan to address the resumption of processing by the LAN and microcomputer systems might also render data files and software vulnerable or unusable should a disaster occur.

DMR and Southeast Region management should clearly identify responsibilities associated with Southeast Region area plans and the importance of developing these plans to address the loss of automated systems for an extended period of time. Although Southeast Region staff articulated the procedures that need to be prepared under various disaster scenarios to regain business functions, the procedures have not been formally documented. Southeast Region administrators should be responsible for: identifying and formally documenting key personnel alternate staff and emergency contact information; describing and documenting roles and responsibilities for a disaster recovery team at the

Southeast Region; formally assessing potential Southeast Region impact based on various disaster or emergency scenarios; and formally identifying Southeast Region-based files and records and detailing a strategy or process for the recovery of these records and files. The Southeast Region-based files and records would include hardcopy documents vital to the Southeast Region's daily processing activities. This Southeast Regional Office, in conjunction with DMR, needs to identify the nature and extent of the business activities that can be conducted in the absence of DMR-supported systems and/or damage to the Region's facility.

The objective of business continuity planning is to help ensure timely recovery of mission-critical and essential functions should a disaster cause significant disruption to computer or business operations. Business continuity planning for Southeast Region's information is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for DMR in conjunction with the Southeast Regional Office to have an ongoing business continuity planning process that assesses the relative criticality of business and IT systems and develops appropriate contingency and recovery plans. To that end, the Southeast Region 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.

Recommendation:

We recommend that Southeast Region management establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for the LAN. We recommend that senior management review the information technology environment and perform a criticality assessment and risk analysis of all automated systems used by the Southeast Regional Office. The Southeast Regional Office should also evaluate the frequency of its off-site backup copies of magnetic media for the non-essential business applications used by the office. Based on the results of the assessment, the Southeast Region in conjunction with DMR Central should proceed with the development of a written business continuity plan for their mission-critical and essential functions.

Once the plan has been developed, it should be periodically tested, then periodically reviewed and updated for any changing conditions. The Southeast Regional Office should specify the assigned responsibilities for maintaining the plan and for supervising the implementation of the tasks documented in the plan. Management should specify who should be trained in the implementation and execution of the plans under all emergency conditions and who will perform each required task to fully implement the plans. Further, copies of the completed business continuity and Southeast Region area plans should be

distributed to all appropriate staff members. A copy of the plan should also be kept in a secure, off-site location.

Auditee's Response:

The Southeast Region has taken the first step in developing a business continuity plan. We have sent a representative to a state-wide meeting where the task of the group is to complete a business impact analysis (BIA). The group is headed by a member of DMR's senior staff. The goal of the group is to identify all mission-critical operations and systems and then develop a complete task analysis applying timelines to each step. This will create an accurate description of the dependence of each staff position on the successful operation of all automated systems used by Southeast Regional staff including but not limited to : MEDITECH, HCSIS, IMPACT, and MMARS. Once the BIA is done the resulting plan will be distributed to the appropriate staff. The master copy will be stored off site to protect the document. The completed plan will be tested possibly on a state wide basis as each region is represented on the team. The plan will then be reviewed and updated as needed.

The Region has also instituted additional safeguards in the event of an MIS shut down in our offices. We have equipped each conference room in our offices with network accessibility. This will allow us to move staff off-site in order for them to complete their day to day responsibilities. We have also increased the number of staff with VPN access thus increasing our ability to respond to extended shut downs in any office.

In addition to the process identified for developing the business continuity plan there is an elaborate diagram available at our Central Office that details the current and future set up to address the need for disaster recovery. This plan identifies all current file servers in each of our offices and diagrams the links connecting each to our Central Office. In addition the diagram identifies the steps taken to create an appropriate back up system to aid in addressing the need for disaster recovery.

Auditor's Reply:

We are pleased that the Southeast Region, in conjunction with DMR, will perform the appropriate criticality assessments and develop a business continuity plan. The business continuity strategy should be sufficiently comprehensive to address various disaster and recovery scenarios and ensure system availability to mission-critical operations and IT processing at the facility. The diagram will assist in developing and continuously updating disaster recovery efforts to ensure a viable business continuity strategy to address changes to systems and technology.