AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

No. 2009-0251-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DR. JOHN C. CORRIGAN MENTAL HEALTH CENTER

February 24, 2006 through June 12, 2009

OFFICIAL AUDIT REPORT

NOVEMBER 17, 2009

TABLE OF CONTENTS

INTRODUCTION

The Dr. John C. Corrigan Mental Health Center (JCCMHC) is governed by Chapter 19, Section 7, of the Massachusetts General Laws and administered by the Department of Mental Health's (DMH) Southeastern Area Office under the purview of the Executive Office of Health and Human Services. The JCCMHC is located at 49 Hillside Street in Fall River. The facility provides and oversees 24-hour crisis and emergency services, outpatient medication clinics, acute in-patient hospitalization, partial hospitalization, child and adult case management, community-based flexible support services, program of assertive community training, respite services, children's support services, therapeutic after school programming, and clubhouse services. At the time of our audit, JCCMHC had been appropriated approximately $4,000,000 of state funds to support fiscal year 2010 operations and employed 158 full-time staff at the Center.

The goal of the Center is to provide and oversee mental health services to residents of the Fall River, Freetown, Somerset, Swansea, and Westport areas who have severe and long-standing problems of mental illness and related disruption in social role performance. The stated mission of the Center is to work in concert with DMH's mission, which is to assure and provide access to services and support mechanisms that meet the mental health needs of individuals of all ages, enabling them to live, work, and participate in their communities. These goals are accomplished by ensuring access to an integrated network of effective, efficient, and culturally competent mental health services that promote consumer rights, responsibilities, rehabilitation, and recovery.

The Center's computer operations are supported through a local area network (LAN), consisting of one file server to which 133 workstations are connected. The LAN is connected to the Commonwealth's wide area network (WAN) which supports the Information Technology Division's mainframe that provides the Center with access to the DMH's Mental Health Information System (MHIS), the Massachusetts Management Accounting and Reporting System (MMARS), the Human Resources Compensation Management System (HR/CMS), and other network services, including e-mail. In addition to the workstations available for JCCMHC personnel, the Center has three notebook computers available to senior managers. The JCCMHC receives technical support and guidance from DMH's Applied Information Technology (AIT) Division.

The primary application used by JCCMHC to support its mission-critical business functions is the Mental Health Information System developed by a private vendor, Meditech Incorporated. MHIS provides automated processing for a variety of important client-related services. The JCCMHC uses the MHIS application to analyze and review admissions, medical records management, coding diagnosis, billing and

accounts receivable, and accounts payable. MHIS is also used to monitor in-patient and out-patient medications. The MHIS application is supported through a cluster of file servers and application servers located at the Massachusetts Information Technology Center (MITC) in Chelsea. The JCCMHC also utilizes Microsoft Office to perform various administrative functions including the generation of statistical reports.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the JCCMHC's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws (MGL), we performed an Information Technology (IT) general controls examination of IT-related activities at the Dr. John C. Corrigan Mental Health Center (JCCMHC). The scope of the audit consisted of an evaluation of the status of prior audit results from our IT audit report, No. 2006-0251-4T, issued June 19, 2006, regarding business continuity planning and environmental controls over and within the areas containing computer equipment. In addition, we reviewed whether JCCMHC was in compliance with the security requirements associated with the protection of personally identifiable information (PII) and the requirements set forth through MGL Chapter 93H. The audit, which was conducted from February 2, 2009 through June 12, 2009, covered the period of February 24, 2006 through June 12, 2009.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results and to review whether JCCMHC was in compliance with requirements to protect personal information. We sought to determine whether sufficient environmental protection controls were in place to provide an appropriate IT processing environment and to prevent and detect damage to, or loss of, computer equipment and data residing on the systems. In addition, we sought to determine whether JCCMHC, in conjunction with the Department of Mental Health, had in place adequate disaster recovery and business continuity plans to provide reasonable assurance that computer operations would be regained within an acceptable period should a disaster render JCCMHC's computerized functions inoperable, or inaccessible.

We sought to determine whether JCCMHC had taken sufficient efforts to be in compliance with the security requirements that are associated with the protection of personally identifiable information, and the requirements set forth through MGL Chapter 93H.

Audit Methodology

To evaluate whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2006-0251-4T, we performed pre-audit work that included gaining an understanding of JCCMHC's mission and business objectives, current IT environment, and the degree of oversight provided by DMH regarding the Center's IT activities. We reviewed our prior recommendations and examined the extent to which JCCMHC had implemented corrective action regarding environmental protection controls and business continuity planning.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we conducted a walkthrough of the server room and the network communication closets and reviewed general housekeeping procedures for those areas. To evaluate provisions for temperature and humidity control for the server room, we determined whether there was an adequate air conditioning unit in the server room and whether temperature controls existed in the network communication closets. We determined whether an uninterruptible power supply (UPS) had been installed to prevent loss of data through a controlled shutdown of equipment following the loss of electrical power. Furthermore, we checked for the presence of fire suppression devices and water detection alarms within the server room and whether the server and other computer equipment located in the network closets were on racks and raised above floor levels to prevent water damage.

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

To assess whether JCCMHC was in compliance with the regulations that are associated with the governance of PII and the compliance requirements set forth through MGL Chapter 93H regarding the safeguarding of personal information, we reviewed whether documented policies and procedures were in place to protect personally identifiable information and whether related hardcopy files were safeguarded.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Our examination of the status of audit results from our prior audit report, (No. 2006-0251-4T) issued June 19, 2006, indicated that corrective action had been taken to address the control objective regarding environmental protection. Our current audit indicated that the Dr. John C. Corrigan Mental Health Center (JCCMHC) had implemented sufficient measures regarding the environmental protection controls over the server room and the network communication closets. However, the status of the prior audit finding regarding disaster recovery and business continuity planning had not been fully addressed.

Our examination of environmental protection over the server room and the network communication closets revealed that appropriate controls were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss resulting from environmental hazards. We found that there was one file/printer server at JCCMHC that was equipped with an uninterruptible power supply (UPS) and was connected to emergency power via a generator. There was a dedicated air conditioner in the server room for climate and humidity controls. Although the server room equipment was not located on a raised floor, there is a small battery operated water alarm located on the server room floor. In addition, JCCMHC installed a Sensaphone that helps the Center stay informed of vital environmental conditions and processes. If there were changes in particular environmental factors, such as heat, humidity, loud noises or water, the Sensaphone will notify the Campus Police and JCCMHC management. Moreover, the Campus Police inspect the server room and the network closets on a daily basis, and monitor and record the temperature of these areas.

We determined that JCCMHC did not have documented, Center-specific business continuity plans in place to regain all mission critical functions in the event of a sustained loss of IT capabilities. However, JCCMHC's administering agency, the Department of Mental Health, has developed an enterprise-wide business resumption plan, a draft Applied Information Technology (AIT) Division response and support plan and emergency contact list, a Meditech support plan with the Commonwealth's Information Technology Division, a draft IT Services Continuity Management Plan, a Client Server Data Recovery Plan, and an emergency preparedness plan. We also determined that JCCMHC did have certain contingency controls in place, such as a diesel generator dedicated to the facility, and UPS, and performed backups daily (remotely from Taunton). In addition, we determined that the Center had procedures in place such as user area plans. If a disaster were to occur, JCCMHC has downtime workflow processes and forms for its mission critical systems. In addition, we determined JCCMHC's verbal agreement with Taunton State Hospital to use their site as an alternate processing location should be formally documented.

Our review revealed that JCCMHC had documented policies and procedures regarding the security of personally identifiable information, an assigned security coordinator, and had security and compliance forms to verify that all staff members were fully aware of the security issues regarding accessing the network and protecting personal information in automated systems.

AUDIT RESULTS

1. Prior Audit Results Unresolved - Disaster Recovery and Business Continuity Planning

Our prior audit indicated that the Center did not have a comprehensive business continuity plan to provide reasonable assurance that business functions supported by technology could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. Although the Center had an informal disaster recovery plan in its MIS handbook and efforts were underway to develop business continuity plans for the Department of Mental Health (DMH) facilities through DMH Central, JCCMHC did not have an adequate strategy for continuous availability and recovery of automated systems.

Our current audit revealed that the Department of Mental Health had developed a business resumption plan, a draft applied information technology response and support plan, a Meditech support plan with the Information Technology Division, an Applied Information Technology (AIT) emergency contact list, a draft IT Services Continuity Management Plan, a client server data recovery plan, and an emergency preparedness plan. However, JCCMHC in conjunction with DMH, had not developed a comprehensive business continuity plan for recovering mission-critical business functions for the Center.

JCCMHC did have certain contingency controls in place, such as a diesel generator dedicated to the facility and an UPS, and performed remote backups daily from Taunton State Hospital. In addition, we determined that the Center had procedures in place for user area plans. If a disaster were to occur, JCCMHC has downtime workflow processes and forms for its mission critical systems. We determined JCCMHC did not have a written agreement with Taunton State Hospital to use their facility as an alternate processing site and that the verbal agreement was not referenced in any documented plan. A formal, comprehensive, and tested disaster recovery plan is not in place at JCCMHC to provide reasonable assurance that essential business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. The objective of a disaster recovery plan is to ensure that IT operations rendered inoperable can be restored within an acceptable period of time to support business functions.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption or loss of computer or network operations. Generally accepted industry practices and

standards for computer operations support the need 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.

Disaster recovery and business continuity planning should be viewed as a process to be incorporated within organizational functions rather than as a project that is completed upon the drafting of a written plan. Since the criticality of systems and underlying risks may change, a process should be in place to identify changes in criticality, risk, or other factors, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. Appropriate user area plans should outline recovery or contingency steps with detailed steps to be followed to efficiently restore business operations. The area plans should be coordinated with overall enterprise-based business continuity or business continuity plans.

Recommendation

We recommend JCCMHC, in conjunction with DMH, develop a comprehensive business continuity plan for recovering mission-critical business functions for the Center. We recommend that JCCMHC assess its automated processing environment from a risk management and business continuity perspective and further develop and test appropriate disaster recovery and business continuity and contingency plans. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to JCCMHC operations or the overall IT environment.

The business continuity plan should document JCCMHC recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The plan should ensure that the continuity framework documents minimum recovery requirements to maintain adequate business operations and service levels with diminished resources and establishes IT processing resumption procedures for workstations and notebook computers. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities, needed to effectively and efficiently recover network or IT operations within the required time frames. We recommend that business continuity be tested and periodically reviewed and updated, as needed, to ensure the viability of the plans. JCCMHC's completed plans should be distributed to all appropriate staff, which in

turn should be trained in the execution of the plans under emergency conditions. In addition, a complete copy of the plans should be stored in a secure off-site location.

JCCMHC's planning process should be considered as user area plans, and as such should be coordinated with the planning that has already been accomplished at an enterprise wide level by the Department of Mental Health.

Auditee's Response

DMH has focused its Business Continuity Planning under the Office of Emergency Preparedness. Coop Plans, Pandemic Planning, IT Service Continuity Management, Site Business Continuity Planning are all efforts that are under review and assessment. In support of those efforts, DMH AIT has undertaken the formation of an ITIL supported approach of emergency planning in the form of an Information Technology Service Continuity Management Plan. The plans for the implementation of that effort were shared with the Auditors. Since the audit began, progress has been made and a draft is under internal review. Further steps scheduled for the next few months are a complete criticality assessment for all business applications supported by DMH AIT and a comprehensive test plan. Once those tasks are complete, DMH AIT will present a draft plan for DMH Emergency Preparedness review and acceptance. Once we have passed that milestone, DMH will then share that draft with the Auditors for their further review and input if they would be willing to do so.

Auditor's Reply

We acknowledge that steps are underway to address disaster recovery and business continuity planning and that the Center is dependent on DMH and DMH's AIT. We note that recovery and contingency plans specific to the Center's operations need to be developed. These plans should be coordinated with the Information Technology Service Continuity Management Plan that is being drafted by DMH. Until appropriate disaster recovery and business continuity plans are completed, JCCMHC remains vulnerable.

2. Prior Audit Results Resolved - Environmental Protection Controls

Our prior audit, No. 2006-0251-4T, disclosed that although certain environmental protection controls were in place, adequate environmental protection was not in effect to provide reasonable assurance that the Center's IT-related assets located in JCCMHC's file server room, network communication closets, and off-site backup storage area would be adequately safeguarded from environmental damage. We found that there were certain environmental protection controls in place at the Center, such as an emergency evacuation plan for the entire building, dedicated air conditioning units for the file server room, smoke and fire detection devices throughout the Center, several fire extinguishers on each floor and in the file server room, and procedures for conducting fire drills. In addition, we found that all critical IT equipment in the file server room

and the network communication closets had uninterruptible power supplies (UPS) and were connected to an emergency power generator to help prevent damage to, or loss of, computer equipment. However, during our prior audit we observed that the network communication closets did not have adequate air circulation, the temperature was not monitored, and there were no heat detectors or a dedicated air conditioning system in three of the four network communication closets and the off-site back-up storage location. Generally, we found that the air temperatures appeared to be above normal temperature ranges for areas housing telecommunication equipment and file servers.

Our current audit found that appropriate controls for environmental protection over the server room and the network communication closets were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss resulting from environmental hazards. We found that there was one server at JCCMHC that was equipped with an UPS and was connected to emergency power via a generator. There was a dedicated air conditioner in the server room for climate and humidity controls. The server room contained a small battery operated water alarm and a Sensaphone that helps JCCMHC stay informed of vital environmental conditions and detect excess heat, loud noises, and water. If there are changes in these conditions, the Sensaphone will notify the Campus Police and JCCMHC management.