The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

NO. 2010-0270-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE WRENTHAM DEVELOPMENTAL CENTER

February 10, 2007 through January 27, 2010

OFFICIAL AUDIT REPORT
APRIL 14, 2010

TABLE OF CONTENTS

INTRODUCTION

The Wrentham Developmental Center (WDC), which began operations in 1907, is governed by Chapter 19B of the Massachusetts General Laws and is placed organizationally under the Department of Developmental Services (DDS). The Executive Office of Health and Human Services (EOHHS) provides additional oversight and guidance for WDC's operations. The WDC is an intermediate care facility that provides residential care for approximately 275 developmentally impaired adults. The WDC accommodates and medically assists clients in three units encompassing 17 residences and a 12-bed acute care medical center. At the time of our audit, the WDC was staffed by approximately 800 employees. The WDC received $47,449,477 of state funds for fiscal year 2007, $46,759,139 for fiscal year 2008, $47,330,073 for fiscal year 2009, and $46,204,149 for fiscal year 2010.

The WDC computer operations are configured in a local area network (LAN) that is supported by one file server to which 227 microcomputer workstations are connected throughout the campus. The WDC workstations are networked to a Dell PowerEdge 2400 file server that is connected by a dedicated leased line to DDS's file servers located in Boston. The WDC file server, which is located in the administration building, connects through DDS's file servers 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), Massachusetts Management Accounting and Reporting System (MMARS), and to other mission-critical applications, including the Medical Health Information System (MHIS) and the Home and Community Services Information System (HCSIS) that are installed at MITC. The EOHHS and DDS are responsible for the management of network operations and computer equipment located at the WDC and have assigned a site manager to be responsible for monitoring all IT-related functions at the facility.

The MHIS and HCSIS applications are used to process a variety of administrative and medical information pertaining to patient admissions and discharges, client records, and investigations. The MHIS is a statewide application that was developed by a vendor, Meditech Inc. The MHIS application processes automated information for admissions, medical records, coding diagnosis, therapeutic information, patient care, billing, and accounts receivable. The HCSIS is a DDS web-based application that provides incident collection and reporting of information pertaining to client activities and/or incidents.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) audit at the Wrentham Developmental Center (WDC). The audit, which was conducted from October 13, 2009 through January 27, 2010, covered the period of February 10, 2007 through January 27, 2010. The scope of the audit consisted of an evaluation of the status of prior audit results in our audit report, No. 2007-0270-4T, issued June 25, 2007, regarding internal control documentation for IT-related policies and procedures, physical security, system access security, inventory control over computer equipment, and disaster recovery and business continuity planning. In addition, we determined whether the WDC had appropriate policies in place regarding the protection of personally identifiable information.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit results. Our audit objective regarding internal control documentation for IT-related policies and procedures was to determine whether the WDC's IT-related internal control environment, including policies, procedures, and practices, provided reasonable assurance that IT-related control objectives were in place to support business functions. We sought to determine whether adequate physical security controls were in place to protect residents and staff, and to safeguard computer equipment. The areas reviewed were the WDC's administrative offices, residential units, and the file server room. Regarding system access security, we sought to determine whether adequate controls were in place to ensure that only authorized personnel had access to WDC's automated systems and whether password administration controls were being monitored.

We sought to determine whether inventory controls over computer equipment had been addressed and whether adequate controls were in place to provide reasonable assurance that IT-related assets were properly recorded and accounted for, and were safeguarded against unauthorized use, theft, or damage.

We determined whether WDC, in conjunction with DDS and EOHHS, 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 WDC's computerized functions inoperable, or inaccessible. Regarding the security and confidentiality of personal information, we sought to determine the extent to which the WDC was meeting the requirements of Executive Order 504.

Audit Methodology

To evaluate whether corrective action was taken on our recommendations presented in our prior audit report, No. 2007-0270-4T, we performed pre-audit work that included a review of prior audit work papers and gaining an understanding of WDC's current IT environment. To obtain an understanding of the internal control environment, we reviewed the WDC's organizational structure, primary business functions, and relevant policies and procedures and conducted formal interviews with WDC and DDS management.

Regarding our review of documented IT-related policies and procedures, we interviewed senior management at WDC and reviewed, analyzed, and assessed relevant IT-related internal control documentation obtained from EOHHS. We determined whether IT- related policies and procedures were in place and in effect and communicated to appropriate staff.

To evaluate physical security, we interviewed management and conducted walk-throughs of areas housing IT equipment, such as resident units, the file server room, and administrative offices. Through observation and tests, we evaluated the adequacy of physical security controls over areas housing IT equipment. We examined the existence of controls, such as office door locks and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current WDC or DDS employees and that the areas were restricted to only authorized personnel. Furthermore, we reviewed procedures for physical key management and the documentation and resolution of security violations and/or incidents, and requested a list of key holders to areas housing computer equipment.

To determine whether adequate controls were in place and in effect to properly safeguard and account for computer equipment, we initially reviewed inventory control policies and procedures and obtained an inventory list of computer equipment. We conducted an inventory test applying ACL audit software to select and analyze a sample of 72 out of 592 items listed on the DDS system of record for IT-related fixed assets that are located at the WDC. Additionally, we selected 54 items observed during our walk-through of the Center and traced the items from the floor to the inventory listing. We examined the inventory record for key data fields, such as identification tag numbers, location, condition, description, and historical cost.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to the local area network and the mission-critical MHIS and HCSIS web-based applications utilized by the WDC. We reviewed control practices regarding logon ID and password administration and password composition by evaluating the appropriateness of documented policies and

guidance provided to personnel. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes. In order to verify that all users of the WDC network were either current employees or authorized contract employees, we obtained a system-generated user list containing 357 user accounts to the WDC network as of November 6, 2009. We compared this list to a WDC employee and contractor listing, dated November 30, 2009. We also performed a test of the MHIS application by comparing a list of 316 MHIS user accounts to the employee roster, dated November 30, 2009. Our audit did not include an examination of controls over network security.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and the procedures to be followed to resume computer operations in the event that computing system capabilities become inoperable or inaccessible. We interviewed DDS and WDC management to determine whether the criticality of application systems had been assessed; whether an IT risk analysis for computer operations had been performed; and whether a Continuity of Operations Plan (COOP), disaster recovery plan (DRP), and business continuity plan (BCP) were in place and, if so, whether they had been adequately tested. To assess the business impact on WDC's operations should a disaster render the mission critical applications inoperable, we conducted a series of five interviews among a cross section of users. In addition, we reviewed the status of management's efforts to designate an alternate processing site to be used in case of an extended disruption of computing system availability.

To determine the status of the WDC's compliance with respect to the handling of personally identifiable information (PII), we reviewed Executive Order 504 to identify agency responsibilities regarding protection of personal information and notification for confidentiality breaches. We interviewed senior management and completed an assessment regarding the protection of personal information of WDC's clients and staff.

Our audit was conducted in accordance with generally accepted government auditing standards 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 version 4.1) issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Based on our audit at the Wrentham Developmental Center (WDC), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to documented policies and procedures, physical security, and system access security would be met. However, our audit found that controls pertaining to inventory control over computer equipment and business continuity planning needed to be strengthened.

Our examination of internal control documentation revealed that WDC, in conjunction with DDS, had developed and implemented IT-related policies and procedures regarding physical security, inventory control over computer equipment, and system access security. We found that DDS had an Internal Control Plan in place to assist in the management of IT operations at the Wrentham Developmental Center.

We found that physical security controls provided reasonable assurance that IT resources located in the WDC's administrative offices, file server room, and resident areas were adequately protected against unauthorized physical access. The combination of preventive and detective controls, including management control practices, provided reasonable assurance that IT equipment would be protected against unauthorized access, damage, or theft. We found that security personnel were present to monitor activities throughout the WDC campus on a 24-hour basis. We also found that management had policies and procedures in place and in effect to monitor the issuance and return of keys distributed to employees.

Regarding system access security, we found that controls for DDS's application systems used by WDC provided reasonable assurance that only authorized users had access to the application programs. We found that users were properly authorized and that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated, or appropriately modified, should personnel terminate employment or incur a change in job requirements. Our audit tests confirmed that for all but one user account, current users were either authorized WDC or EOHHS employees, or authorized contractors. The one exception was for an account that had not been deactivated for a former employee who had terminated employment at WDC in February 2009. We determined that this account did not have access to the mission-critical applications and a subsequent audit test confirmed that the user account was immediately deactivated by WDC management when brought to their attention. Regarding password security, all users are required to change their password within a pre-defined time period, and passwords have a defined length of alpha/numeric characters as recommended by the Commonwealth's Information Technology Department. During the course of our audit, nothing further came to our attention to indicate that there were weaknesses in the WDC's access security controls.

With respect to inventory control of computer equipment, our prior audit report, Number 2007-0270-4T, indicated that WDC management could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon, since a complete annual physical inventory and reconciliation was not being performed. Our current audit disclosed that sufficient corrective action had not been taken by WDC, in conjunction with DDS, to ensure that annual reconciliations are performed as required by the Office of the State Comptroller. Furthermore, our examination of the inventory system of record revealed that key data fields, such as acquisition date, purchase order number, cost, condition, and specific location of the equipment, were not present. Our audit confirmed that 126 computer-related items tested out of the population of 592 items were properly accounted for and tagged.

Our review of business continuity planning indicated that although WDC did not have a comprehensive business continuity strategy, we determined that the agency had in place a Continuity of Operations Plan (COOP) dated February 2009 and other documented control practices requiring an alternate relocation site for clients and emergency notification plans. With respect to disaster recovery planning for computer operations, we found that DDS has responsibility for IT equipment and applications installed at WDC. Our audit disclosed that DDS did not have an approved, comprehensive, and tested disaster recovery plan (DRP) to restore computer operations at WDC in the event of a disaster. We found that existing plans did not provide sufficient disaster recovery strategies to regain computer operations in a timely manner should a catastrophic event render IT systems inoperable. To strengthen controls, a detailed risk analysis and business impact analysis needs to be performed to provide input for completing comprehensive and tested disaster recovery and user area plans that operate in conjunction with WDC's COOP. Regarding our analysis of the business impact on WDC operations should mission-critical applications become inaccessible, our audit revealed that four out of the five users we interviewed would experience minimal impact in their daily responsibilities. We found that only the Assistant Facility Director would be adversely impacted in performing critical functions such as reviewing daily reports in a timely manner, analyzing daily patient activity, and monitoring facility operations on a daily basis.

Regarding our review of controls over personally identifiable information, we found that the WDC had policies and security controls in place to help protect sensitive and personal information against unauthorized access or disclosure. We verified that a Security Officer was assigned by DDS to oversee the implementation of Executive Order 504 at WDC and confirmed that all employees had been trained and were required to acknowledge by signature that they had attended the training on Executive Order 504.

AUDIT RESULTS

1. Prior Audit Results Resolved

a. Documentation of IT-related Policies and Procedures

Our prior audit found that WDC's documented IT policies and procedures had only limited formal documentation that was not sufficiently comprehensive to address WDC's IT operations.

Our current audit indicated that WDC, in conjunction with DDS and EOHHS, had developed documented IT policies and procedures to provide guidance and to strengthen WDC's processing environment.

b. Physical Security

Our prior audit revealed that WDC management did not maintain a list of key holders for areas housing both computer equipment and residents throughout the facility and, therefore, could not be assured that access would only be limited to authorized staff.

Our current audit found that management had implemented policies and procedures in place to monitor the issuance and return of keys distributed to employees to ensure that only authorized personnel have access to areas housing both computer equipment and residents. We found that physical security controls were in place and in effect to provide reasonable assurance that IT resources would be protected and were operating in a controlled environment. We found that authorized access to the server room was limited to three senior management employees and we observed that security personnel were present to monitor activities throughout the WDC campus on a 24-hour basis.

c. System Access Security

Our prior audit revealed that system access security controls over WDC's mission-critical application systems, the Home and Community Services Information System (HCSIS), and the MediTech (MHIS) application needed to be strengthened to ensure that only authorized users have access to these systems. DDS had established written policies and procedures in place for the removal of access privileges for terminated employees; however, we found that these procedures were not always being followed. The audit revealed that management staff was not always providing written notification of changes in employee status, such as terminations and leaves of absences, to the DDS Southeast Region's Human Resource Department.

Our current audit revealed that controls provided reasonable assurance that only authorized users had access to data files and web-based applications accessed through WDC's file server and microcomputer workstations. We determined that out of a total of 804 full-time employees and 14 contract employees, 357 were granted access privileges to the WDC network. Of the three user accounts that could not be reconciled to the employee and contractor lists, we confirmed that one account did not reflect a name

change by marriage, one account was for an authorized EOHHS employee, and the remaining account was for an individual who had terminated employment in February 2009. We verified that the user account had not been used since the individual had left the employment of WDC, that the level of access privileges was relatively low, and that the account was deactivated as soon as the agency was notified. Regarding MHIS access, we were able to reconcile all user accounts to the employee roster for WDC for access to MHIS. Our audit tests of user account management controls revealed that users were properly authorized, and that, except for the one instance noted above, administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated, or appropriately modified, should personnel terminate employment or incur a change in job requirements.

2. Prior Audit Results Unresolved

a. Inventory Control over Computer Equipment

Our audit disclosed that inventory control practices over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the inventory system of record. Although our tests confirmed that for data recorded for computer equipment information was correctly and completely recorded, the inventory record lacked important information to properly track equipment assets. In addition, since a complete annual physical inventory and reconciliation was not being performed to assist in verifying the relevance and reliability of the inventory record, WDC, in conjunction with DDS and EOHHS, could not provide reasonable assurance that the inventory system of record for computer equipment could be relied upon.

The WDC's computer equipment inventory listing provided to us by DDS included 592 items located throughout the WDC campus. Based on a sample of 72 IT items generated by ACL software, we found that all of the items in the sample could be located throughout the WDC and that each item was properly recorded on the inventory record. In addition, we selected an additional 54 items from various locations and confirmed that all these items were recorded in the system of record.

Our analysis of the inventory record indicated that although data fields, such as model, description, tag identification number, and serial number, were present, the listing lacked critical data fields for historical cost, acquisition date, condition, and location. The absence of a sufficiently reliable inventory of computer equipment hinders the WDC's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives. Furthermore, by failing to record the historical cost of purchased computer equipment and their purchase dates on the inventory system of record, WDC and DDS were not in compliance with the requirements of the Office of the State Comptroller's Fixed Assets-Acquisition Policy, dated November 1, 2006. In addition, by not

performing an annual reconciliation of the inventory system of record, WDC and DDS were not in compliance with the Office of the State Comptroller's Accounting and Management Policy, dated November 1, 2006. This policy states, "There shall be a reconciliation of the fixed asset inventory against the books and records maintained by the Department. . . . .This reconciliation is to be done, at a minimum, on an annual basis. This reconciliation shall be available for audit either by the department's internal auditors, the State Auditors Office or the Commonwealth's external auditors."

Our audit revealed that weaknesses in inventory control were the result of an inadequate assignment of asset control responsibilities and insufficient monitoring and management oversight. 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 1989 states, in part, "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 WDC, in conjunction with DDS, perform an annual physical inventory and reconciliation of the inventory system as required by the Accounting and Management Policy of the Office of the State Comptroller, dated November 1, 2006. The purpose of performing an annual reconciliation is to ensure that the inventory system of record is maintained on a perpetual basis in an accurate, complete, and valid manner.

We further recommend that DDS's system of record for IT inventory be expanded to include data fields containing information relative to cost, location, condition, acquisition installation date, and status of the IT resource. The recommended control procedures should provide increased assurance that all IT-related equipment is properly recorded and accounted for and enable the development of a complete record, maintained on a perpetual basis, of all IT-related equipment at the WDC.

Auditee's Response

> *The Executive Office of Health and Human Services currently maintains a web based inventory system that functions as the system of record. Included in this database are data fields for the item, the serial number, the manufacturer, the model number, the location, the assignment, the status of the equipment, the acquisition date, the installation date, and the cost of the equipment. The EOHHS IT employee assigned to*

WDC is responsible for maintaining and updating the information and he is the sole person at WDC with access to this system. We will work with EOHHS to assure that any new equipment placed at WDC contains the cost and acquisition date information so that it may be included in the database.

On an annual basis, a physical inventory of all IT equipment assigned to WDC will be taken and reconciliation made between the inventory of record and the physical inventory in compliance.

Auditor's Reply

We acknowledge that the referenced system of record contains the data fields noted above. Information needs to be entered in the data fields for the equipment records contained in the inventory system of record. The data will help ensure that IT resources are properly accounted for and will assist WDC in addressing IT configuration management objectives. We are pleased that an annual physical inventory will be conducted at WDC and that a reconciliation between the system of record and the equipment on hand will be performed, as required by the Office of the State Comptroller. The reconciliation should also include reference to documentation on IT acquisitions and changes in IT equipment.

b. Business Continuity Planning

We determined that DDS has responsibility for the support of all equipment and applications installed at WDC. Although certain objectives for contingency planning existed, our audit found that DDS did not have a sufficiently comprehensive disaster recovery plan (DRP) in place to provide for the timely restoration of business and IT capabilities should application systems be rendered inoperable or inaccessible. We found that WDC had a Continuity of Operations Plan (COOP), dated February 2009, that provided detailed procedures to be performed to sustain key business functions during and after a disruption of computer operations. However, we determined that DDS did not have a formal DRP and user area plans that work in conjunction with WDC's COOP to address a catastrophic event that would deny access to WDC's facility for an extended period of time.

A business continuity plan should document the WDC's recovery strategies with respect to various disaster scenarios. Without adequate disaster recovery and contingency planning, including required user-area plans, WDC is at risk of not being able to gain access to automated systems. Furthermore, the absence of a comprehensive and tested disaster recovery plan could 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 should a disaster occur.

We found that DDS was sufficiently aware of the need for comprehensive disaster recovery and business continuity plans and had taken steps to begin to develop recovery strategies and had implemented on-site

and off-site storage of backup copies of programs and data files. The absence of a sufficiently comprehensive and tested disaster recovery plan and designated alternate processing site places at risk DDS' ability to recover systems within an acceptable period of time.

Although DDS understands that IT systems may need to be recovered under disaster scenarios, an appropriate risk analysis methodology was not conducted to identify the relevant threats that could render IT systems inoperable or inaccessible, the likelihood of the threat, and expected frequency of occurrence for each disaster scenario. As a result, if a disaster were to occur rendering IT inoperable or inaccessible, DDS would be unable to provide the foundation and structural framework for managing computer capabilities associated with emergency response and continuity of responsibilities supporting WDC's mission within an acceptable time period.

Generally accepted business practices and industry standards for computer operations support the need for the WDC in conjunction with DDS to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, WDC, in conjunction with DDS, 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 sufficiently detailed disaster recovery and business continuity plans be developed that are based on criticality and business impact assessments, risk management, and recovery plan testing. To help ensure that the Center responds optimally in the event of a disaster, the recovery and business continuity plans should be developed to work in conjunction with WDC's COOP detailing current mission-critical operations, applications, supporting IT infrastructure, and a risk analysis assessment of various disaster scenarios. The business continuity plan should address all key business processes including procedures for sustaining the business functions during and after a disruption of services. The disaster recovery plan should also address IT recovery under circumstances when access to WDC's facility is denied for an extended period of time. The disaster recovery plan should be an IT-focused plan designed to restore information systems operability at an alternate processing site.

The agency's contingency plans should assign specific staff with roles and responsibilities and present detailed steps for them to follow in recovering mission-critical and essential IT systems and operations. The BCP and DRP should also address the telecommunications and security issues that would arise if the agency had to conduct off-site computer operations. In addition, the plans should document vendor protocol for the emergency use of computers suitable for operating WDC's mission-critical applications. The plans should be adequately tested to provide reasonable assurance of their viability, periodic training

should be conducted for IT and operational staff, and hardcopy and electronic copies of the disaster recovery, business continuity, and agency-specific user area plans should be stored in a secure off-site location.

Auditee's Response

The DDS Disaster recovery plan is currently a work in progress. Although we have not tested all of our applications, the DDS Meditech application was successfully tested and ITD confirmation documentation has been forwarded to the Auditors. This audit does not illustrate that a backup network has been built with a server room, air conditioning, dedicated emergency power with a generator access and dual feed electrical service. Servers have been installed on site with new telecomm circuits also in place. A new active directory network has recently been implemented, and we have not yet fully tested the disaster recover aspects of this network. This new network has given us a more secure network with centralized backups which are major enhancements to our overall plan. We are working with the EOHHS engineers to document the Disaster recovery process with these new enhancements. Once that is completed, a copy of the new plan will be tested and forwarded to all appropriate parties. Please note that some of our applications reside at ITD and are, therefore, reliant on plans submitted by ITD.

There are also new plans being developed by EOHHS in conjunction with ITD to re-locate multiple agencies under one roof in a new location. The new EOHHS consolidation plans will change how disaster recovery will be done in the near future.

Auditor's Reply

We acknowledge DDS's action in having appropriate back-up procedures to aid recovery efforts at the WDC. We encourage DDS to continue to work in conjunction with EOHHS in formulating, testing, and communicating a comprehensive business continuity and contingency strategy to ensure the timely recovery of mission-critical and essential business functions and systems.