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. 2010-1405-7T

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

July 1, 2007 through December 11, 2009

OFFICIAL AUDIT REPORT

MARCH 11, 2010

TABLE OF CONTENTS

INTRODUCTION

The Department of Developmental Services (DDS) 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 DDS is comprised of 23 area offices located throughout the Commonwealth that operate within five regions: DDS Central, Central/West Region, Metro Region, Northeast Region, and Southeast Region. DDS's mission is dedicated to creating, in partnership with others, innovative and genuine opportunities for individuals with intellectual disabilities to participate fully and meaningfully in, and contribute to, their communities as valued members. Through various state-operated programs and contracts with private providers, DDS assists approximately 33,000 clients.

DDS'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, Plymouth, Brockton, Weymouth, and Cape Cod and the Islands. At the time of our audit, 975 department staff were employed by the Southeast Region, including 39 employees who work at the Southeast Regional Office, 200 who work in the area offices, and 736 who work in Southeast Residential Services that operate state-sponsored community homes. An additional 38 DDS Central Office staff were located at the Southeast Regional Office working in Investigations, Legal, and Human Rights.

The Southeast Region's computer operations were configured in a local area network (LAN) consisting of one file server and 88 desktop workstations. The Southeast Region's workstations were connected to a Dell PowerEdge file server that is connected by a dedicated leased line to DDS's file servers located in Boston. The Southeast Region's file server connects through DDS's file servers to the Commonwealth's wide area network (WAN) providing access to computer systems installed at the Massachusetts Information Technology Center (MITC) in Chelsea. The WAN provides DDS Southeast Region access to the Human Resource Compensation Management System (HR/CMS), the Massachusetts Management Accounting and Reporting System (MMARS), and to other mission-critical applications, including Meditech and the Home and Community Services Information System (HCSIS) that are installed at MITC.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws (MGL), we performed a follow-up audit of certain information technology (IT) general controls. Our audit, which was conducted from September 14, 2009 through December 11, 2009, covered the period of July 1, 2007 through December 11, 2009. The scope of the audit consisted of an evaluation of the status of prior audit results in our prior audit report, No. 2007-1405-4T, issued June 29, 2007, regarding inventory control over computer equipment and disaster recovery and business continuity planning. In addition, we determined whether the Southeast Region 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. We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded and accounted for in the inventory system of record and safeguarded against unauthorized use, theft, or damage. In addition, we determined whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647 reporting requirements.

We sought to determine whether DDS Southeast Region, in conjunction with the Executive Office of Health and Human Services (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 the Southeast Region's computerized functions inoperable or inaccessible. A further objective was to determine whether DDS Southeast Region was in compliance with the regulations that are associated with the protection of personally identifiable information and the compliance requirements set forth in Chapter 93H of the Massachusetts General Laws and Executive Order 504.

Audit Methodology

To determine whether corrective action had been taken to address the recommendations presented in our prior audit report, No. 2007-1405-4T, we performed pre-audit work that included gaining an understanding of the Southeast Region's mission and business objectives and reviewing prior audit workpapers, the current IT environment, and the degree of oversight provided by EOHHS regarding IT

activities. We reviewed the extent to which the Southeast Region had implemented corrective action on our prior recommendations regarding inventory controls over computer equipment and business continuity planning.

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 to determine whether appropriate data fields were included 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 identification numbers and equipment serial numbers for selected items were accurately recorded on the computer equipment inventory listing. We also performed data analysis on the inventory records, noting any unusual distribution characteristics, duplicate records, or unusual or missing data elements.

To determine whether the IT-related inventory record, dated September 21, 2009, was current, accurate, and valid, we randomly selected a sample of 69 out of 345 hardware items located at the Southeast Regional Office and the three area offices selected for review. To evaluate whether the system of record accurately and completely reflected the computer equipment, we verified the location, description, and serial numbers of hardware items listed on the inventory system of record and traced them to the actual equipment's physical location. In addition, we randomly selected 32 additional items of computer equipment installed throughout the Southeast Region and determined whether the items were properly recorded on the inventory record. We also identified the ten laptops in the custody of the Southeast Region.

To determine whether the Southeast Region complied with Commonwealth of Massachusetts Regulations for fixed-asset accounting, we reviewed supporting evidence that the Southeast Regional Office performed an annual physical inventory and reconciliation of IT equipment. We determined whether computer equipment had been purchased or leased during our audit period. 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 also reported to the Office of the State Auditor.

To assess the adequacy of business continuity planning, we determined whether the Southeast Region had performed any formal planning in conjunction with EOHHS to resume IT operations should the network application systems be rendered inoperable or inaccessible. In addition, we determined whether risks and

exposures to computer operations had been evaluated. We conducted interviews with management and supporting staff from the Southeast Regional Office to determine whether the criticality of application systems had been assessed and whether a continuity of operations plan (COOP) and business continuity plan (BCP) were in place and, if so, whether the plans had been adequately reviewed and tested. In addition, we reviewed the status of management's efforts to designate an alternate processing site to be used in case of an extended loss of the current operational facility and disruption of computing system availability.

To assess whether DDS Southeast Region was in compliance with the regulations that are associated with the protection of personally identifiable information and the compliance requirements set forth through Chapter 93H of the Massachusetts General Laws and Executive Order 504, we determined whether documented policies and procedures were in place regarding the protection of sensitive data, hardcopy files were safeguarded, and appropriate controls were in place regarding logical access to the Meditech system by DDS Southeast Region personnel.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT 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. 2007-1405-4T, issued June 29, 2007, indicated that corrective action had been taken to address control objectives regarding disaster recovery and business continuity planning. However, our audit tests revealed that inventory controls over computer equipment still needed to be strengthened.

We determined that the DDS Southeast Region's control practices were in place to provide reasonable assurance that normal business operations could be resumed within the Southeast Region in a timely manner should the LAN file server and workstations become unavailable for an extended period. Our audit disclosed that DDS Southeast Region had developed an emergency procedures plan along with a continuity of operations plan (COOP) for its business functions. In addition, all the area offices under the Southeast Region have a specific emergency procedures plan. We found that additional guidance was provided by Security Standards and Procedures Plan developed by the Executive Office of Health and Human Services (EOHHS).

With respect to inventory control of computer equipment, our audit indicated that controls needed to be strengthened to provide reasonable assurance that IT resources would be properly accounted for in the inventory system of record. Our audit revealed that the DDS Southeast Region and EOHHS could not provide a comprehensive inventory listing of computer equipment on hand as required by the Office of the State Comptroller's "Internal Control Guide for Departments." We found that reconciliations were not being performed to assist in verifying the accuracy and completeness of the inventory record. Furthermore, we found that the inventory system lacked data fields for information regarding tag numbers, purchase dates, historical cost, or equipment condition. Our audit test of the EOHHS inventory record disclosed that all 69 IT assets randomly selected from the EOHHS system of record could be located. However, our test of 32 items from physical locations to the system of record revealed that only 17, or 53%, of the selected items were recorded on the inventory record. In addition, none of the 104 newly purchased IT items was recorded on the EOHHS system of record. The absence of a reliable inventory of computer equipment hinders the ability of DDS Southeast Region and EOHHS to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

We found that the Southeast Region in conjunction with EOHHS had developed policies and procedures to protect personal information.

AUDIT RESULTS

1. Prior Audit Results Unresolved – Controls 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 for property and equipment. We found that the DDS Southeast Region, in conjunction with EOHHS, could not provide a comprehensive inventory system of record for computer equipment and that an annual physical inventory and reconciliation of the system of record was not being performed. Our audit revealed that procedures needed to be strengthened 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 EOHHS included 750 items of IT-related equipment located at the Regional Office and all seven area offices. Based on a statistical sample of 69 IT items randomly selected from the inventory listing of 345 hardware items located at the Southeast Regional Office and three selected area offices, we found that all 69 items were located throughout the Southeast Region and were properly recorded on the inventory record. Although the equipment was located, we observed that, in general, equipment was not tagged with state identification numbers. However, our test of 32 items selected from physical locations and compared to the system of record revealed that 15 items, or 47%, of the selected items were not recorded on the inventory system of record. For the 17 items found, we confirmed that information was correctly recorded for item description and serial number. In addition, although there were 104 newly purchased IT items, none of them was recorded on the inventory system of record.

Our analysis of the inventory record indicated that although data fields, such as origin, model, serial number, and location were present, the listing lacked critical data fields for historical cost, state tag numbers, and acquisition date. The absence of a sufficiently reliable inventory of computer equipment hinders the Southeast Region's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

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, DDS Southeast Region and EOHHS were not in compliance with the Office of the State Comptroller's fiscal year fixed-asset requirements and Office of the State Comptroller's Memorandum No. 313A. In addition, inventory valuation for computer equipment could not be analyzed and evaluated.

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 the DDS Southeast Region, in conjunction with EOHHS, enhance and implement internal control policies, procedures, and practices regarding inventory control of computer equipment in the areas of recording and inventory verification to provide reasonable assurance that computer equipment allocated to the DDS Southeast Region is properly accounted for. We recommend that appropriate assurance methods, such as independent verification, physical inspection, reconciliation, and oversight, be implemented to ensure that inventory controls are in place and in effect. We further 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 Region amend 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 Region model its policies and procedures in accordance with generally accepted control practices for IT configuration management. Once approved by EOHHS and Southeast Region senior management, the internal control-related 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 of the computer equipment. In addition, we recommend that data fields related to the status of hardware maintenance be considered. We recommend that an effort be made to ensure that all IT resources are properly recorded on the inventory system of record to support IT configuration management objectives.

The recommended control procedures should help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner enabling the Southeast Region, or DDS, to generate a complete record of all IT-related equipment on a perpetual basis. The procedures should identify requirements to update the inventory records on a perpetual basis to reflect any changes to computer equipment, including location, assignment, or status for deployed equipment and items held in storage.

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

Auditee's Response

The Southeast Region recognizes the need to strengthen our IT inventory system. We will work closely with our IT representative and IT staff from our Central Office to develop a stronger and more robust inventory document. Discussion has begun within the Region to appoint a manager from the business office to be the point person with our EOHHS IT representative. The job description of this person will be redesigned to add the responsibility of coordinating information about each piece of IT equipment currently in use throughout the Region. This will include working with the IT representative in designing a more accurate flow of information from the Region and its area offices through the business office and subsequently to EOHHS for inclusion in the master inventory being maintained by that agency. In addition to the assignment of a Regional staff person as the IT inventory point person staff in each of our Area Offices will be identified to work with that person to inventory all IT equipment in our Area Offices. Our decision to assign a staff person to this role will provide us with a new resource to work with our IT Central Office staff and EOHHS IT staff to expand the fields of information in the current IT inventory spreadsheet to encompass the areas of concern identified in the IT audit recommendations. Our feeling is that by making the IT inventory a focus of an individual's job responsibilities we will be better able to address the deficiencies sited in the audit. We also feel that better information concerning the IT equipment throughout our Region will enable us to identify our IT needs and provide substantial information to advocate for additional resources in this area. In conclusion, we feel that the renewed dedication of staff time to address the audit issues will provide the region with a stronger inventory system.

Auditor's Reply

We commend the actions initiated by the Southeast Region to improve fixed-asset inventory controls. Ensuring that equipment is properly tagged, assigned to individuals or functional units, and recorded on a perpetual inventory system of record helps to ensure that the Commonwealth's assets are identified and safeguarded. We believe that the efforts to improve the exchange of information from the Region and the area offices to the EOHHS will strengthen inventory control procedures and improve the integrity of the inventory system of record. The enhanced controls should assist the Southeast Region and EOHHS

management in making IT infrastructure and configuration management decisions and identifying future technology needs.

2. Prior Audit Results Resolved - Business Continuity and Contingency Planning

Our prior audit indicated that there was limited evidence that formal planning had been performed to restore DDS-based business operations in the event that automated systems were damaged or no longer accessible.

Our follow-up review disclosed that the DDS-Southeast Region control practices were in place to provide reasonable assurance that normal business operations could be resumed at the region in a timely manner should the LAN file servers and workstations be unavailable for an extended period. Our audit disclosed that DDS-Southeast Region had an emergency procedures plan along with a continuity of operations plan and they are covered under EOHHS' Security Standards and Procedures. In addition, all the area offices under the Southeast Region have a tailored emergency procedures plan and electronic media is backed up off site in real time at their Central Office in Boston.