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. 2008-1308-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON THE EXAMINATION OF INFORMATION TECHNOLOGY RELATED CONTROLS
AT THE MASSACHUSETTS OFFICE ON DISABILITY

December 1, 2003 through October 19, 2007

OFFICIAL AUDIT REPORT

DECEMBER 7, 2007

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Office on Disability (MOD), which was established in 1981, is organized under Chapter 6, Section 185, of the Massachusetts General Laws (MGL) and operates within the purview of the Executive Office for Administration and Finance in accordance with Chapter 7, Section 4G, of the MGL. MOD is comprised of a Director, who is appointed by the Governor, and 14 staff members, who include three assistant directors and a local area network coordinator. The Director is responsible for the administration of MOD's programs and services. MOD, which is located at One Ashburton Place in Boston, received a state appropriation of $716,762 and a federal grant of $214,451 for fiscal year 2007.

According to its mission statement, MOD's primary purpose is "to bring about full and equal participation of people with disabilities in all aspects of life by working to assure the advancement of legal rights and for the promotion of maximum opportunities, supportive services, accommodations and accessibility in a manner which fosters dignity and self determination." By providing information, referral, and advocacy, MOD assists people in obtaining services, such as vocational rehabilitation, accessible housing, and employment. Since the passage of the Americans with Disabilities Act (ADA) in 1990, MOD has acted as the Commonwealth's coordinating agency to ensure compliance with the law.

According to information on its website, MOD responds to the needs of over 18,000 individuals yearly through three major programs: Community Services, Client Services, and Government Services. The Community Services Program assists individuals in learning about their rights and responsibilities as people with disabilities. Through training and technical assistance, MOD helps to ensure that state and local governmental entities, as well as places of public accommodation, meet their non-discrimination responsibilities.

Responding to over 10,000 requests a year, the Client Services Program assists several hundred people each month to learn about legal rights and services available to people with disabilities. The program also provides disability-related services to federal, state, and local officials, businesses and other interested parties. The Government Services program works to ensure that Massachusetts' policies and practices are consistent with state and federal laws. MOD also provides mediation and representation services to clients of the Massachusetts Rehabilitation Commission, Massachusetts Commission for the Blind, and independent living centers under a grant from the Rehabilitation Services Administration.

At the time of our audit, MOD's information technology (IT) operations were maintained by one IT staff member, who was the local area network (LAN) coordinator. At that time, MOD's IT operations were supported by three file servers, 16 networked desktop computer workstations, and five notebook computers. The file servers and desktop computers were configured in a local area network located in MOD's 13th floor office space. MOD's designated file servers were connected to the Commonwealth's wide area network (WAN) providing access to the Commonwealth's Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

The primary computer applications used by MOD to support its business processes were two commercial database applications. The Omega database application, operating on a file server, was used by the Client Services Program to capture client information, monitor and track cases, and produce an annual report required by the terms of MOD's federal grant. The Community Services Program maintained information regarding physical access for the disabled in city and town facilities using Call Tracking**,** a database application operating on MOD's microcomputer workstations. In addition, MOD used the Microsoft Office 2003 software suite for correspondence, spreadsheet and database analysis, and documentation.

The Office of the State Auditor's examination focused on an evaluation and review of certain IT-related general controls.

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) general controls examination of IT-related activities at the Massachusetts Office on Disability (MOD) for the period of December 1, 2003 through October 19, 2007. The audit was conducted from September 5, 2007 through October 23, 2007. Our audit scope included an examination of IT-related general controls pertaining to documented IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and 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 to support MOD's IT processing environment. In this regard, we sought to determine whether MOD's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support business functions.

Our audit objective regarding IT-related policies and procedures was to determine whether IT-related policies and procedures adequately addressed the areas under review and were sufficiently documented and in place. We determined whether adequate physical security controls were in place and in effect to ensure that only authorized users had access to IT resources in order to prevent unauthorized use, damage, or loss. We also determined whether sufficient environmental protection controls were in place to provide a controlled operating environment and to prevent and detect damage to computer equipment and data.

Our objective regarding system access security was to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to MOD's application systems and data files. We evaluated whether procedures were in place to prevent unauthorized user access to automated systems and IT resources through workstations and file servers connected to the local area network (LAN). In addition, we determined whether LAN data was sufficiently protected against unauthorized disclosure, modification or deletion, and whether MOD was actively monitoring user account administration.

With regard to inventory control over computer equipment, including notebook computers, we reviewed and evaluated control policies and practices regarding accounting for computer equipment. In addition, we determined whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647, the Internal Control Act, reporting requirements for missing or stolen assets.

With respect to the availability of automated processing capabilities and access to IT resources and data, we determined whether business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup procedures were being performed and whether backup copies of magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding MOD's overall mission and IT environment. Regarding our review of IT policies and procedures, we interviewed senior management and staff, completed questionnaires and obtained, reviewed, and analyzed existing IT-related policies and procedures. We obtained and reviewed the internal control plan to determine whether IT internal controls were adequately documented and whether the internal control plan included, or referenced, IT control policies and practices. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also interviewed MOD staff regarding the extent to which IT policies and procedures were documented and identified, or cross-referenced, in the internal control plan.

To determine whether computer equipment and backup copies of magnetic media stored on-site and off-site were adequately safeguarded from damage or loss, we reviewed physical security over the IT resources through observations and interviews with senior management. We conducted walk-throughs, observed and identified security devices, and reviewed procedures to document and address security violations and/or incidents. We determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to the file server room and the central office. We reviewed control procedures for physical access, such as the authorization of staff to access the file server room, and key management regarding door locks to the central office and other areas housing IT equipment. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms.

With respect to environmental protection, our objective was to determine whether controls were adequate to prevent and detect damage to, or loss of computer equipment and media. To determine the adequacy of environmental controls, we conducted walkthroughs of the file server room and office areas housing IT equipment at MOD's main office. Our examination included a review of general housekeeping; fire prevention, detection and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and review of pertinent documentation.

We reviewed MOD's system access security policies and procedures designed to prevent unauthorized access to application software and data files residing on the LAN. We discussed the security policies and procedures with the LAN administrator, who was responsible for controlling access to MOD's LAN and computers. Our examination of system access security included a review of the staff's access privileges to applications residing on the LAN and the desktop computers. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition, length, and frequency of password changes. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed procedures for authorizing access to MOD's IT resources. We then determined whether individuals granted access to the Omega application system were currently employed by MOD by comparing an automated list of individuals authorized to access the system with an official listing of current employees.

To assess the adequacy of business continuity planning, we evaluated the extent to which MOD had plans that could be activated to resume IT-supported operations should the network and servers be rendered inoperable or inaccessible. We interviewed senior management to determine whether MOD had formally documented procedures for the development and maintenance of appropriate business continuity plans. We also determined the extent to which the MOD had performed a risk analysis with regard to the loss of IT-enabled business operations under different disaster scenarios. As part of our examination of business continuity planning, we assessed the adequacy of generation and storage of backup copies of magnetic media, and physical security and environmental protection controls for on-site and off-site storage. In that regard, we interviewed IT staff responsible for creating and storing backup copies of computer-related media. Since backup copies of computer-related media were stored off-site in an electronic vault located with a third party, we visited the vendor's data center and reviewed physical, environmental, and encryption security procedures associated with backup storage. We further sought to determine whether MOD's IT personnel were aware of, and trained in, all procedures required to restore systems via backup media that would be required under disaster or emergency circumstances.

With regard to inventory control over computer equipment, we evaluated whether an annual physical inventory was conducted, whether computer equipment was accurately reflected in the inventory of property and equipment, and whether the inventory system of record was properly maintained for computer equipment. To determine whether adequate controls were in place and in effect to properly account for MOD's computer equipment, we reviewed inventory control policies and procedures and requested and obtained MOD's inventory listing of computer equipment. We reviewed the inventory listing to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of IT-related computer equipment. We also performed data analysis on the inventory to identify any duplicate records, unusual data elements, or missing values. To determine whether MOD's purchased computer equipment was recorded on the inventory listing, we selected 20 items, or 100% of MOD's purchased computer equipment items from invoices during the audit period. To determine whether computer equipment items on the inventory listing were locatable at MOD's office areas, we selected a judgmental sample of 47 items (67%) out of a total population of 70 items and verified their locations. To determine whether computer equipment data found on the inventory listing was recorded accurately, we inspected the 47 items and compared serial numbers found on the equipment and other related information to the data recorded on the inventory record. In addition, we verified actual locations, assigned users, serial numbers, and other related information for the five notebook computers recorded on the inventory list. Further, to assess the integrity and completeness of MOD's inventory listing, we selected 10 additional IT-related items in adjacent locations while conducting our visual inspection of the 47 items of computer equipment items and determined whether they had been properly assigned asset numbers, tagged, and recorded on the inventory record.

To determine whether MOD complied with Commonwealth of Massachusetts regulations for accounting for assets, we reviewed evidence supporting MOD's performance of an annual physical inventory of IT assets. Further, to determine whether MOD had complied with Commonwealth regulations for disposal of surplus property, we reviewed records and supporting documentation for computer equipment disposed of during the audit period. Finally, to determine whether MOD's staff were aware of and in compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen assets, we reviewed documented inventory control policies and procedures, interviewed senior management to determine whether MOD had experienced any incidences of missing or stolen IT-related equipment during the audit period, and verified whether any incidents were reported to the Office of the State Auditor.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) 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), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at the Massachusetts Office on Disability, we found that internal controls in place provided reasonable assurance that IT-related control objectives would be met with respect to physical security, environmental protection, system access security, and on-site and off-site storage of backup media. However, we found that MOD needed to strengthen and formalize IT policies and procedures regarding inventory control over computer equipment, and enhance its overall disaster recovery and business continuity planning to provide reasonable assurance that IT systems can be restored and that business operations can be regained within an acceptable period of time.

Although we determined that certain IT policies and procedures were in place, the level of formal documentation needed to be enhanced for inventory control over computer equipment, environmental protection, disaster recovery and business continuity planning, and system access security. The absence of sufficiently documented controls increases the risk that desired control practices would not be adequately communicated, administered, or enforced.

We found that physical security controls provided reasonable assurance that MOD's IT resources were safeguarded from unauthorized access. We found that the file server room was locked, but a list was not maintained of individuals who had access. Although we found no intrusion alarms, the building housing MOD's office space has full-time police protection on duty 24 hours per day, seven days per week. Our examination also disclosed that MOD's two office areas have restricted physical key access to only approved individuals and are kept locked after business hours. In addition, visitors are escorted when accessing the file server room to minimize the risk of damage or theft of computer equipment.

Adequate environmental protection, such as sprinkler systems and a dedicated air conditioner were found to be in place in MOD's file server room to help prevent damage to, or loss of, IT-related resources. We observed that the file server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. We also observed that the file server room has a UPS connected to the servers to allow safe system shutdown without data loss, and a hand-held fire extinguisher located adjacent to the file server room. However, we found that the file server room lacked a monitoring system for temperature and humidity in the event of a failure of the dedicated air conditioner. In addition, we observed that evacuation and emergency procedures were not posted within MOD's office areas.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to MOD's programs and data files residing on MOD's file servers and microcomputer workstations. We determined that system access privileges granted to individuals were appropriate for their job responsibilities and functions. We found that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should MOD employees terminate employment or incur a change in job requirements. Our tests confirmed that all current system users were MOD employees. However, through observations and interviews, we determined that administrative password composition and the frequency of password changes were not adequately controlled for access through MOD's IT network. Specifically, we found that MOD's password composition policy needed to be strengthened. During our audit, the LAN coordinator developed and circulated to MOD staff a memorandum regarding a revised password composition policy, to be effective October 30, 2007, requiring that all passwords be subject to more stringent requirements. We recommend that MOD formalize the revised password policy and monitor compliance with it.

Our audit disclosed that MOD did not have a formal, tested, disaster recovery plan to provide reasonable assurance that the Omega database application system and essential data processing operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable. At the time of our audit, MOD had an informal disaster recovery plan and had begun to formulate a business continuity strategy. Our audit indicated that the level of disaster recovery and business continuity planning needed to be strengthened to provide detailed documented plans to address recovery strategies to provide continuity of business operations. Although a potential alternate processing site had been identified, a formal agreement was not in place, and a user area plan had not been established to document procedures to be followed by non-IT staff to support business continuity objectives in the event of a loss of IT operations.

We found that adequate procedures were in place regarding the generation of daily backup copies that were electronically transferred on a daily basis to a secure off-site location. We determined through our visit to the off-site location that appropriate physical security and environmental protection controls were in place and that encryption controls appeared to be adequate.

With respect to inventory control over computer equipment, we found that MOD was not in compliance with fixed assets policies and procedures promulgated by the Office of the State Comptroller (OSC) and had not conducted an annual physical inventory and reconciliation. In addition, we found that MOD was not maintaining an up-to-date perpetual inventory system of record that included all required asset information. Our examination of computer equipment purchases confirmed that all purchases had been recorded on MOD’s inventory listing. Our inspection of computer equipment items at MOD disclosed that, although all items were locatable, they had not been assigned and tagged with asset numbers.

We found that although MOD had a limited number of notebook computers, the Office lacked a formal policy to control the assignment and use of notebooks. We determined that MOD had assigned notebook computers to employees without requiring signed acceptance of the responsibility for security and authorized use. The lack of a formal policy to control notebook computers could hinder MOD's ability to safeguard and properly account for available computer equipment.

We found that MOD had complied with the Operational Services Division’s (OSD) policies and procedures regarding surplus Commonwealth fixed assets and had properly obtained surplus status for the computer equipment items that it disposed of during the audit period. Finally, our review for compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that MOD staff responsible for inventory were aware of the requirements and that MOD did not have any occurrences of missing or stolen computer equipment during the audit period.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

Our audit revealed that although the Massachusetts Office on Disability had a documented business continuity plan, MOD had not developed a sufficiently-detailed disaster recovery strategy. We found that MOD had taken steps to address business continuity planning by implementing off-site storage of backup media and initiating steps to identify a viable alternate processing site. However, further effort is needed to develop and subsequently test a detailed recovery strategy 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. In addition, although MOD understood that a loss of IT capabilities would adversely impact operations, the relative criticality of automated systems needed to be assessed and the extent of potential risk and exposure to business operations needed to be documented.

At the time of our audit, MOD's senior management had determined that funding did not allow for maintaining a permanent alternate processing site. Consequently, MOD was considering an alternate processing site at another state agency that could be used to support off-site IT recovery efforts. Regarding IT resources, MOD uses Microsoft Office 2003 software for internal correspondence, spreadsheet and database analysis, and other documentation, and data files are maintained on the Office's LAN. Access to MOD's application software, data, and on-line documentation would be jeopardized if IT processing capabilities were unavailable. MOD's off-site data storage potentially provides a means of recovery for lost information on the LAN.

The objective of business continuity planning is to help ensure the continuation of essential functions enabled by technology should a disaster cause significant disruption to computer 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.

Contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality or other factors, such as risk, 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.

Recommendation:

We recommend that MOD assess its automated processing environment from a risk management and business continuity perspective and further develop and test appropriate 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 MOD's operations or the overall IT environment.

The business continuity plan should document MOD's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. 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 needed time frames. We recommend that business continuity be tested and periodically reviewed and updated, as needed, to ensure the viability of the plans. MOD's completed plans should be distributed to all appropriate staff, who 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.

Auditee's Response:

> *We accept the draft as an accurate representation of conditions at MOD during the audit period. Please be aware that we are already taking steps to implement the Auditor's recommendations.*

Auditor's Reply:

We commend MOD for initiating corrective action and will review the status of business continuity planning and disaster recovery in the future.

2. Inventory Control over Computer Equipment

Our audit revealed that although the Massachusetts Office on Disability had adequate documented internal controls regarding ordering, purchasing, and disposing of fixed assets, and its computer equipment items were locatable, MOD was not performing annual physical inventories and reconciliations of fixed assets. In addition, we found that MOD did not maintain an updated perpetual inventory system of record containing asset information that is required by the Office of the State Comptroller (OSC). We also found that MOD lacked a formal policy to control the assignment and use of notebook computers. As a result, MOD could not provide reasonable assurance of the integrity of the inventory listing and that it could be relied upon to assist in the accounting for and verification of computer equipment. Further, the absence of a reliable inventory system of record for computer equipment hindered MOD's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Our audit disclosed that MOD's documented inventory control procedures and practices regarding computer equipment needed to be strengthened and formalized to ensure that IT resources would be properly accounted for in a complete and updated system of record. We found that MOD was not performing annual physical inventories and reconciliations of fixed assets that are required by the Office of the State Comptroller, as well as MOD's Internal Control Manual. We determined that MOD lacked adequate control procedures and practices to ensure the maintenance of a current, accurate, and complete perpetual inventory record of computer equipment. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is purchased, relocated, or disposed. As a result, MOD could not provide reasonable assurance of the integrity of the inventory system of record and its reliability as a tool for accounting for and monitoring computer equipment. The absence of a sufficiently reliable inventory of computer equipment hindered MOD's ability to properly account for and monitor IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Our audit also determined that MOD had not developed adequate procedures and control practices regarding maintenance and reconciliation of a system of record for IT resources. Although fixed assets regulations promulgated by the Office of the State Comptroller, as well as policies found in MOD's internal control manual, as updated in April of 2006, required the performance of an annual physical inventory of fixed assets, MOD senior management acknowledged to us that they had not performed a physical inventory for at least two years.

With respect to inventory recordkeeping, MOD senior management stated, at the beginning of our audit, that the Office was in the process of creating and enhancing a system of record for computer equipment. We initially examined MOD's September 12, 2007 inventory listing and found that, although the record contained certain fields of information including location, description, and serial number, it lacked other data fields needed to properly account for computer equipment, such as assigned asset numbers, original costs, status or condition, and acquisition dates. Data regarding asset costs, assigned numbers, and dates of acquisition are required by fixed assets regulations promulgated by the Office of the State Comptroller.

Information regarding the status of an item is useful information for supporting IT configuration management by noting the asset's status, such as being repaired, obsolete, or designated for surplus.

During the audit, we provided guidance to MOD in creating an inventory listing that will serve as its official system of record for IT resources. Subsequently, we examined the inventory listing of computer equipment that MOD provided on September 27, 2007. This revised listing contained 70 computer equipment items with a total stated value of $53,414; however, the listing still lacked columns of information for MOD-assigned asset numbers and acquisition dates.

Regarding inventory verification, we found that MOD's monitoring of computer equipment items needed to be strengthened. Specifically, MOD senior management stated that they had not performed a required annual physical inventory of fixed assets and reconciliation of computer equipment items. The absence of fully documented policies and procedures regarding inventory verification hindered MOD's ability to ensure the integrity of its inventory system of record as it pertained to IT-related assets.

Our audit also determined that MOD lacked a formal policy to control the assignment and use of notebook computers. We determined that MOD had assigned five notebook computers to employees without requiring signed acceptance of the responsibility for security and authorized use. The lack of a formal policy and procedures to control notebook computers could hinder MOD's ability to properly account for available computer equipment.

Recommendation:

To ensure that inventory control over IT resources is adequately maintained, we recommend that MOD strengthen documented inventory control procedures and practices to ensure compliance with policies and procedures promulgated in the Office of the State Comptroller's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation. Specifically, MOD should perform an annual physical inventory and reconciliation of computer equipment to ensure that an accurate, complete, valid, and current inventory record of IT resources is in place. We recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical inventory, acquisition, and disposal records. Also, MOD should include on its inventory system of record additional data fields for asset numbers and acquisition dates to be in compliance with OSC guidelines.

With respect to MOD's monitoring of its IT-related equipment, MOD should improve documentation supporting the annual physical inventory, including a reconciliation of the physical inventory to MOD's inventory records. This improved documentation will help ensure the integrity of MOD's perpetual inventory system of record for IT-related assets and provide reasonable assurance that MOD's inventory records can be effectively used to support IT configuration management and help safeguard its computer equipment. Further, once MOD has completed an annual physical inventory of computer equipment, we recommend that MOD maintain supporting documentation of the physical inventory performed and its reconciliation to the perpetual inventory system of record.

Finally, with respect to notebook computers, we recommend that MOD develop a formal policy requiring that users who are assigned notebook computers must sign a responsibility and acceptable usage form. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment.

Auditee's Response:

> *We accept the draft as an accurate representation of conditions at MOD during the audit period. Please be aware that we are already taking steps to implement the Auditor's recommendations.*

Auditor's Reply:

We commend MOD for initiating corrective action regarding inventory control over IT resources. We will review the status of inventory control over IT resources in the future. Compliance with the Office of the State Comptroller's "MMARS Fixed Asset Subsystem Policy Manual and User Guide" will also ensure that other equipment is properly accounted for and that appropriate controls are in place to maintain the integrity of the inventory system of record.