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. 2002-1308-4T

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

JULY 1, 2000 to SEPTEMBER 2, 2003

OFFICIAL AUDIT REPORT

DECEMBER 31, 2003

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Office on Disability (hereinafter referred to as MOD) was created in 1981 and is organized under Chapter 6, Section 185 of the Massachusetts General Law (MGL) and operates within the purview of the Executive Office for Administration and Finance under Chapter 7, Section 4G of the MGL. At the time of our audit, MOD was comprised of a Director and 13 staff, including two assistant directors and a local area network (LAN) coordinator. For the fiscal year 2003, MOD's appropriation was $585,000. MOD also received an annual Client Assistance Program grant of $227,000 from the United States Department of Education, Rehabilitation Services Administration. MOD's administrative office is located in Boston.

The MOD's primary mission 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 MOD's website, the agency has responded to the needs of over 15,000 individuals yearly through three major programs: Community Services, Client Services, and Government Services. The Community Services Program assisted approximately 10,000 individuals a year to learn about their rights and responsibilities as people with disabilities. Through training and technical assistance, MOD helped to ensure that state and local governmental entities, as well as places of public accommodation, comply with their non-discrimination responsibilities. In conjunction with the Community Services Program, MOD implemented the Community Access Monitor (CAM) program to train citizens regarding state access laws, the ADA, and other state and federal laws regarding the disabled. As a result, over 1,000 certified volunteer monitors, trained by MOD, worked within communities to promote physical and communication access for people with disabilities. The Client Services Program assisted several hundred people each month to learn about legal rights and services available to people with disabilities. The program also provided disability-related services to federal, state, and local officials, businesses and other interested parties. The Government Services Program evaluates and monitors the activities of governmental entities to ensure that the needs of the disabled are addressed. In addition, MOD has overseen the activities of the Governor's Special Advisory Commission on Disability Policy and the Inter-Agency Disability Services Coordinating Council, created in 1994, by Executive Orders 351 and 352, respectively. Both bodies work to improve accessibility and delivery of services to the disabled, and to enable people with disabilities to provide input and advice to the Governor regarding the development of public policy. 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 computer operations were supported by two file servers and 26 microcomputer workstations configured in a local area network. The file servers were connected through a wide area network (WAN) to the Information Technology Division (ITD) mainframe, which provides connectivity for access to the Web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system. The primary computer applications used by MOD to support its business processes were two commercial database applications. The Alpha 4 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 for federal reporting requirements. The Community Services Program maintained information regarding physical access for the disabled in city and town facilities in Access, a database application operating on microcomputer workstations. In addition, MOD performed its administrative functions using business-related applications, such as word processing.

Our Office's examination focused on selected general controls, such as physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From April 1, 2002 to May 31, 2002 and from August 19, 2003 to September 2, 2003, we performed an audit of selected information technology (IT) related controls at the Massachusetts Office on Disability (MOD) for the period of July 1, 2000 through September 2, 2003. The scope of our audit included an examination of control practices, procedures, and devices regarding physical security and environmental protection over and within the administrative office and the room housing the file servers at MOD. We reviewed MOD's awareness of and compliance with the Executive Office for Administration and Finance's Information Technology Division's (ITD) "Enterprise Information Security Policy." We reviewed and evaluated system access security to MOD's automated systems, including file servers and microcomputer workstations. In addition, we examined inventory control practices for computer equipment and software.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the automated systems. With respect to the normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning, including the provisions for on-site and off-site storage of backup copies magnetic media. We reviewed procedures for generating and transferring backup copies of critical magnetic media to an off-site storage location. We evaluated physical security and environmental protection controls over backup media stored off-site.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT-related resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion. In addition, we sought to determine whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to the file server-based database application for client information and office business applications residing on the microcomputer workstations and the network on which the applications reside, and that procedures were in place to prevent and detect unauthorized access to automated systems. In addition, we sought to determine whether MOD was aware of ITD's "Enterprise Information Security Policy," as of November 2001 and had complied with its provisions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of IT resources.

We sought to determine whether adequate business continuity planning had been performed and whether plans were in place to restore mission-critical and essential business operations in a timely manner should the automated system be unavailable for an extended period. Further, we determined whether adequate control procedures were in place regarding on-site and off-site storage of computer-related media. Another objective was to review and evaluate control practices regarding accounting for IT-related resources, including computer equipment and software.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of MOD's mission and business objectives. Through pre-audit interviews with the managers and staff and reviews of the website and selected documents, such as MOD's Progress Report covering the 1995 through 1999 fiscal years, business operations and statutory authority, we gained an understanding of the primary business functions supported by the automated systems. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential.

As part of our audit work, we reviewed and evaluated the organization and management of IT operations at the administrative office. In that regard, we reviewed relevant policies and procedures, reporting lines, and a job description. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives, such as ITD's "Enterprise Information Security Policy," as of November 2001.

We interviewed MOD management to discuss internal controls regarding physical security and environmental protection over and within the administrative offices housing the microcomputer workstations, file server room, and the on-site and off-site storage areas. We inspected the administrative office, including the file server room, and reviewed relevant documents, such as the internal control plan, and performed selected preliminary audit tests.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the administrative office. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with MOD management and staff. To determine whether adequate controls were in effect to prevent and detect unauthorized access to the offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, the presence of a receptionist at the entrance point, and whether visitors were required to sign in/out. We reviewed access control procedures, such as the list of staff authorized to access the file server room, and key management regarding door locks to the administrative office's entrance, the file sever room, a separate work office and storage area for client records, and other restricted areas within the office.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS), surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server room or in the vicinity of computer-related equipment. To evaluate temperature and humidity control, we determined whether appropriate dedicated air conditioning units were present in the file server room. Further, we reviewed control procedures to prevent water damage to automated systems, client records, and on-site storage for computer-related backup media.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer workstations. To determine whether MOD's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the assistant director and evaluated selected access controls to the network and applications residing on automated systems. In addition, through interviews with the assistant director and general counsel/assistant director, physical observations, and reviews of documentation, we determined whether MOD was aware of ITD's "Enterprise Information Security Policy," and whether stated control practices were in place and in compliance with the policy. We determined whether MOD's internal control documentation included control practices, such as a risk assessment, an acceptable use policy for IT resources, and security awareness training required by ITD's "Enterprise Information Security Policy."

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the assistant director responsible for access to the automated systems on which the Office's application systems operate. In addition, we reviewed control practices used to assign MOD staff access to the application programs and data files. 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 and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. To determine whether all users with active privileges were current employees, we obtained the list of individuals granted access privileges to the Alpha 4 database and other business-related applications and compared all users with active access privileges, as of April 2002 and August 2003, to MOD's personnel roster of current employees. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so required, we reviewed the frequency of the changes.

Regarding inventory control over IT-related resources, we first reviewed formal policies and procedures promulgated by the Massachusetts Office of the State Comptroller (OSC) regarding inventory control. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed the role of the assistant director regarding the accounting for computer equipment and software, reviewed the inventory control procedures for computer equipment and software, and performed selected tests.

During our audit period, we obtained the hardware inventory records as of April 5, 2002 and as of August 21, 2003, respectively. To determine whether the IT-related inventory record, as of April 5, 2002 and August 21, 2003, were current, accurate, and complete, we attempted to confirm all pieces of equipment recorded on the inventory list, including file servers, microcomputer workstations, and printers to the actual computer equipment installed at the office. We determined whether computer equipment installed at the administrative office was tagged with state identification numbers and whether the tag numbers were accurately listed on the inventory record. We compared the tag numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record. Further, we determined whether serial numbers were accurately recorded on the inventory record. We reviewed the inventory record to determine whether appropriate "data fields," such as state identification number, manufacturer's model number, serial number, location, and cost were included in the record.

We then traced 100% of computer equipment installed at the office to the items listed on the inventory record. To determine whether equipment purchased during the 2002 and 2003 fiscal years were listed on the inventory record and located at MOD offices, we traced four microcomputer workstations and three printers with a listed value of $10,859 purchased during the 2002 fiscal year and a scanner with a listed value of $276 purchased during the 2003 fiscal year to the inventory record as of August 21, 2003 and to the actual equipment on hand. Further, we reviewed software inventory control practices.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and the microcomputer workstations be unavailable for an extended period. We interviewed the assistant director to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. In addition, we interviewed the general counsel/assistant director of the Client Services Program to determine the impact on program operations should the automated systems be unavailable for an extended period. Further, we reviewed and evaluated procedures in place to resume normal business functions should the file servers or the microcomputer workstations be rendered inoperable.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated system be rendered inoperable, we interviewed the assistant director and LAN coordinator responsible for generating backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of backup copies of mission-critical and essential magnetic media at the administrative office. We did not visit the off-site storage location. We did not review ITD backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS).

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on our audit at the Massachusetts Office on Disability (MOD), we found that adequate physical security and environmental protection controls were in place and in effect to provide reasonable assurance that automated systems were properly safeguarded and protected from damage and loss. Our audit indicated that, although important control practices were in place to provide reasonable assurance that IT-related resources were properly accounted for in MOD records, certain controls needed to be improved. With respect to system access security, we determined that all users with active access privileges to automated systems were current employees. Our audit disclosed, however, that control practices regarding logon ID and password administration needed to be strengthened and internal control documentation needed to be enhanced.

Regarding availability of systems, our audit disclosed that certain control practices needed to be strengthened to provide reasonable assurance that normal business operations could be resumed at MOD in a timely manner should the file servers or the microcomputer workstations be unavailable for an extended period. Although we found that, by the close of our audit, control practices regarding on-site and off-site storage of backup copies of magnetic media for administrative and programmatic activities processed at MOD were adequate, further effort was warranted to meet business continuity planning requirements.

Our review of internal controls indicated that management was aware of the need for internal controls, had a defined organizational structure for the Office, an established chain of command, clearly delineated reporting responsibilities, and a documented job description for information technology staff. Our audit revealed that MOD's internal control plan, as of March 19, 2002, included certain control procedures regarding inventory control over property and equipment, system access security, on-site and off-site backup of magnetic media, and physical security and environmental protection over the file server room. MOD should further develop its policies and procedures regarding physical security, environmental protection, and logon ID and password administration. In addition, MOD should ensure that documented control practices, such as an IT-related risk assessment, security awareness program, and acceptable use of IT resources be in compliance with the Executive Office for Administration and Finance's Information Technology Division's "Enterprise Information Security Policy." (See Summary of Internal Control Practices, page 15.)

Our audit revealed that appropriate physical security controls had been implemented over and within the state office building housing the MOD. These controls included on-duty State Police officers, security devices, such as stand-alone and hand-held metal detectors used to screen persons and personal items, and restricted access to the building after normal business hours. With respect to the MOD administrative office, we determined that there was one entrance/exit to the office, a receptionist was located at the front entrance, and keys to the front door and business offices were assigned to appropriate staff. Our audit disclosed that the file server room was located in a non-public area that could not be accessed from outside the building, the door to the room was locked at all times, and access to the room was restricted to three staff. Further, appropriate physical security controls were found to be in place at an adjacent business office housing a work area and file cabinets for storage of client records. According to MOD management, entrance doors to both offices were locked after normal business hours. With respect to confidential client information in hardcopy form, we determined that sufficient controls were in place to protect records from unauthorized access. To strengthen physical security controls, we recommend that MOD management enhance documented policies and procedures in the internal control plan regarding physical access to the business offices, including the file server room and to require that doors to individual business offices within the administrative office be locked after normal business hours.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply were in place in the building housing MOD's administrative office to help prevent damage to, or loss of, IT resources. We confirmed that, under the aegis of the Bureau of State Buildings, a vendor tested fire alarms on a regular basis and fire drills were conducted periodically. Our audit indicated that the file server room was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. During our audit a dedicated air-conditioning unit was installed in the file server room. We found that two uninterruptible power supply devices were in place to permit a controlled shutdown and to prevent a sudden loss of data. To improve environmental protection controls, we recommend that hand-held extinguishers be located within the file server room.

Our tests of access security to the file servers and microcomputer workstations indicated that, although important control practices were in place, other controls needed to be improved to provide reasonable assurance that access to systems, data, and programs would be restricted to only authorized users and that information would be safeguarded against unauthorized use, disclosure, or modification. We found that management was aware of the Executive Office for Administration and Finance's Information Technology Division's (ITD) "Enterprise Information Security Policy," as November 2001. Duties and responsibilities regarding information security had been assigned to the assistant director. We determined that MOD management had implemented informal procedures regarding security awareness for staff, including security over confidential client information. According to MOD management, the agency planned to document policies and procedures regarding acceptable use of information technology and security awareness training for staff.

We determined that, although the Office had developed appropriate procedures regarding authorization and recording of access privileges to automated systems and activation of logon IDs and passwords, these control practices had not been documented. We found that informal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. Audit tests of access security indicated that all users were current employees. We conducted two tests in this regard covering users as of April 2002 and August 2003, comparing system-generated user lists of 16 (100%) and 14 (100%) users who had access privileges to the Office's personnel roster of current employees at those times.

Regarding logon ID and password administration, we determined that passwords were not being changed periodically. Further, MOD had not developed control documentation regarding password formation and use, length of passwords, and frequency of password changes. At the close of our audit, management stated that a schedule for password changes was being developed.

To strengthen system access controls, we recommend that MOD develop formal policies and procedures that address requirements of the "Enterprise Information Security Policy," such as an acceptable use policy for IT resources and a security awareness plan. Further, we recommend that MOD document the process of granting authorization to access automated systems. Because MOD's staff is comprised of only 14 users and all users are authorized to access the systems, we recommend that the agency maintain a list of users, the dates they were granted access privileges, and the level of privileges. With respect to logon ID and password administration, we recommend that MOD determine an appropriate schedule for required password changes. We recommend that MOD document the Office's requirements and procedures regarding the formation, length, and use of passwords, and the frequency of password changes. Documented policies and procedures regarding access security should be included in the MOD's internal control plan. In addition, we recommend that to reinforce user responsibilities regarding access privileges, MOD should require all users to sign a formal security statement acknowledging their responsibilities to protect their password from unauthorized use and/or disclosure.

Our audit disclosed that appropriate control practices were in place to properly account for IT-related resources. We determined that MOD had complied with important control practices required by the Internal Control Act, Chapter 647 of the Acts of 1989 and associated requirements regarding fixed-asset management promulgated by the Office of the State Comptroller (OSC) as of the 2003 fiscal year. However, we determined that MOD's hardware inventory record, as of August 2003, needed to be updated. Although we had found that the inventory record, as of April 2002 with a listed value of $63,675 was current, accurate, and complete, the inventory record as of August 2003 was understated by $11,135 and still reflected the April 2002 total value. We found that five microcomputer workstations and a scanner purchased during the 2002 and 2003 fiscal years had not been entered into the inventory record. According to MOD management, a physical inventory and reconciliation had not been performed since the 2002 fiscal year. We determined that the IT-related inventory record included appropriate fields, such as state identification number, location, and cost. IT-related equipment installed in the administrative office, adjacent work office, and the file server room had been properly tagged with state identification numbers. Our audit indicated that MOD was aware of Operational Services Division requirements regarding surplus property. In addition, software licenses for the business-related applications were appropriately on file at the administrative office.

To strengthen inventory control over IT-related resources, we recommend that MOD maintain a perpetual inventory record. Purchases of equipment should be entered into the inventory record within seven days of acquisition as required by the Office of the State Comptroller and surplus equipment should be removed from the inventory record and recorded on a surplus inventory in a timely manner when the asset is no longer in service, but is still in the custody of the agency. The item should be fully removed from the inventory and surplus list when it is no longer under the custody of the agency. In addition, physical inventory and reconciliation should be conducted at least annually, as required by the OSC. Further, to enhance the level of information in the inventory system of record and support configuration management, we recommend that MOD include the data fields for serial number and date of acquisition in the inventory record.

Our audit disclosed that MOD had developed a business continuity plan as of July 2001 that outlined a strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. The plan included important control practices, such as a contact list, instructions for staff to follow in the event of a disaster, a list of IT-related resources, and a description of telephone and voice mail. Although the plan noted the need for an alternate processing site, at the time of our audit, no alternate processing site had been designated nor had the documented procedures been tested. We acknowledge that MOD had ready access to on-site and off-site backup tapes and could, for a limited time, manually collect information from citizens seeking information or services. However, given MOD's mandate to assist people with disabilities, we recommend that the Office designate an alternate processing site to ensure that business operations could be resumed in a timely manner.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site backup of magnetic media. We determined that MOD had implemented procedures and schedules for generating backup copies of magnetic media, and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies. We also found that physical security and environmental protection over the on-site storage location was adequate. We did not visit the storage facility housing off-site backup copies of magnetic media.

Auditee's Response:

Thank you for this opportunity to respond to the draft audit report transmitted to MOD via your letter of October 23, 2003.

With one exception, we accept the draft as an accurate representation of conditions at MOD during the audit period.

We . . . request clarification and question one recommendation. In the last sentence of the paragraph beginning at the top of page 10, it is recommended that the "doors to the individual business offices are kept locked after normal business hours." Earlier in the paragraph, the report acknowledges that the office entrance doors are locked after hours. We respectfully suggest that the report is unclear as to which additional offices should be locked. Specifically, there are three management offices in all: the fiscal office, the director's office and the general counsel's office. Clarification of this recommendation would be appreciated. It should be noted that we also question the advisability of this measure for two reasons. First, all manager's offices contain locked cabinets in which sensitive files are housed, rendering the business files at least as secure as the client file storage mechanisms that the Auditor found to be acceptable. Because of the layout of MOD's space, should those three offices be locked, virtually all access to heat and air conditioning to the rest of the space would be lost. This would jeopardize the climate control environment for the bulk of MOD's computers, increasing the likelihood that they would be damaged by extremes of heat or cold.

> *Thank you for the Auditor's thoughtful review and recommendations. Please be aware that we are already taking steps to implement the Auditor's recommendations.*

Auditor's Reply:

We are pleased that MOD management is addressing our recommendations regarding environmental protection, inventory control over IT-related resources, password administration, and business continuity planning. We reiterate that physical security over the administrative office and adjacent office housing a work area and storage for client records was adequate. With respect to security over individual business offices located within the administrative office, we acknowledge that certain environmental issues should be addressed with the Bureau of State Office Buildings so that inner office doors can be locked after normal business offices. We reiterate that this procedure will result in an additional control over physical security. In the event that the individual office doors have to be left open for environmental factors, we recommend that MOD continue to rely upon locked cabinets to protect documents.

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
10	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, file server room, microcomputer workstations, and client records in hardcopy form to prevent unauthorized use, loss or damage	Control over access to offices, computer rooms, file servers, and microcomputer workstations; designated facilities manager; intrusion detection devices; locked doors, foot patrols	In Effect	No, except for file server room	Inadequate
10	Environmental Protection	Provide reasonable assurance that IT-related resources operate in an appropriate environment and are adequately protected from loss or damage	Proper ventilation, temperature control, fire alarms, fire suppression mechanisms, water sprinklers, posted emergency procedures	In Effect	Yes	Adequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Pg. ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation.
10,11	System Access Security	Provide reasonable assurance that only authorized users are granted access to the automated systems	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	In Effect, except for password changes	Yes	Inadequate
12	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed	Insufficient, due to lack of data integrity	Yes	Adequate
13	Business Continuity Planning	Provide reasonable assurance that MOD can restore mission-critical and essential functions in a timely manner should file servers and microcomputer workstations be rendered inoperable or be inaccessible.	Current, formal, tested business continuity plan; alternate processing site; periodic review and modification of plan; plan implemented and distributed; and staff trained in its use	In Effect, except for designated alternate processing site	Yes	Inadequate

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
13	On-site storage	Provide reasonable assurance that backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location	In Effect	Yes	Adequate
13	Off-site storage	Provide reasonable assurance that critical and important backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Same as above. Storage area in a separate off-premises location	In Effect	Yes	Aadequate