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. 2002-0512-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE DEPARTMENT OF YOUTH SERVICES

JULY 1, 2001 THROUGH AUGUST 16, 2002

OFFICIAL AUDIT REPORT
JULY 9, 2003

TABLE OF CONTENTS

INTRODUCTION

The Commonwealth of Massachusetts created the nation's first juvenile correctional system in 1846 when it opened the first reformatory school, based on the premise that juveniles were more likely to be rehabilitated than adults. This juvenile correctional system eventually became known as the Division of Youth Services, an independent unit within the Department of Education. In 1969, the Division of Youth Services was abolished, and the Department of Youth Services was established in 1971 under Massachusetts General Laws, Chapter 18A, Section 2 as a separate agency operating under the Executive Office of Health and Human Services.

The Department of Youth Services (DYS) provides a comprehensive and coordinated program of youth delinquency prevention and services to delinquent children and youth referred to or placed in custody with the Department by the courts throughout the state. At the time of our audit, the DYS had a "continuum" model of services and supervision, consisting of 102 programs. The services were divided among 38 programs that serve youth living in the community and 64 residential programs, ranging from staff secure group homes to secure locked units. The DYS is divided into four regional areas: western, central, southeastern (including Cape Cod and the Islands), and metropolitan Boston. At the time of the audit, the DYS tracked an average daily population of 3,278 juveniles, approximately 200 of whom were in the pre-trial stage. The remaining youth cases were adjudicated by the court and placed in the custody of the Department.

During our audit, the information technology (IT) facilities of the DYS central office were networked into 13 separate locations throughout the state, including the central Boston office, area offices, and administration buildings to support ten DYS business activities. The central office is connected to the Massachusetts Executive Office for Administration and Finance's Information Technology Division's (ITD) mainframe for access to the Commonwealth's centralized accounting information system, known as the Massachusetts Management and Accounting and Reporting System (MMARS), and the Human Resources Compensation Management System (HR/CMS). The IT infrastructure at the central office in Boston consisted of ten central network file servers with approximately 95 microcomputer workstations and at the regional offices consisted of eight distributed network file servers connected to approximately 325 microcomputer workstations located throughout 42 Day Reporting Centers (DRC) and 15 program locations, which clients used for educational purposes.

The primary software application used by DYS is the Youth Services Information System (YSIS), which is a Windows-based program that accesses the Department's intranet and operates in Visual Basic on an Oracle database. The YSIS client data consists of client histories, work histories, living conditions, parents' or guardians' income, and educational, medical and psychological information. At the time of the audit, DYS was in the process of testing a new tracking system called the Massachusetts Juvenile Justice Information Connection (MAJJIC). According to the DYS, the vendor-developed MAJJIC will enhance the Department's ability to carry out their mission and business objectives. In addition, DYS in 2001 implemented MassMail, which is an e-mail system utilizing Windows 2000 and Microsoft Outlook.

In 2001, DYS implemented a computer salvage and recycling initiative with its Windows 2000 MassMail rollout. As a result, the Department was able to extend their operating budget by over $150,000 for under-funded educational and operating projects. During the rollout of MassMail, DYS standardized their operations on Microsoft's Windows 2000 operating system and Office 2000 product suite and migrated from Banyan to Microsoft's Exchange and Outlook e-mail services. As a result of this upgrade, many of DYS computers, which were older Pentium 133 MHz systems, had to be replaced to support the new services and application requirements. Of the installed computers, 95 were decommissioned and scheduled for salvage. The DYS' MIS Department took on the responsibility of recycling the 133 MHz computers, consolidating memory and re-imaging the recycled "educational machines" from the decommissioned hardware. The hardware was then made available for use to clients in January 2002. According to DYS, the program was well-received and more requests were submitted than could be fulfilled.

In February 2002, the DYS staff requested that the Operational Services Division (OSD) and ITD's MassMail agencies notify DYS of any IT hardware that was becoming available through surplus from other agencies. The original intention was to acquire some monitors in the hope of extending the DYS IT budget and allowing DYS to reduce the cost of acquiring new desktops. The DYS request, which had been broadcast throughout other state agencies, yielded IT donations from ITD's service partners and from many of the state colleges. As a result of the IT equipment donations, DYS was able to recycle over 140 computer monitors, reconstruct 50 "educational machines," acquire 80 machines for use by DYS employees, distribute eight high-speed laser printers, and install and extend their network with the use of their cable plant through deployment of donated Ethernet Hubs and switches. The impact of this recycling effort has allowed DYS to gain at least one year on their IT needs and deployment. A list of agencies that supported this program is listed in the Appendix.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From February 21, 2002 through August 16, 2002, we performed a follow-up audit of certain financial and IT-related controls at the Department of Youth Services (DYS) for the period covering July 1, 2001 through August 16, 2002. Our follow-up audit included a review of the status of audit results noted in our prior financial and IT-related audit report (No. 1999-0512-4C, issued March 24, 2000). The prior audit results included control deficiencies in the areas of Monitoring and Evaluation of Provider Service Contracts, Hardware and Software Inventory Controls, and MIS Department Organization and Management. We also reviewed access security controls over the Department's client tracking system, known as the Youth Services Information System (YSIS). Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security, environmental protection, hardware and software inventory, business continuity planning, on-site and off-site backup media storage, and system access security.

Audit Objectives

The primary objective of our audit was to determine whether adequate controls were in place and in effect for selected IT-related areas and whether corrective action had been taken with regard to prior audit results and recommendations. We sought to determine whether the Department provided adequate organization and management for the IT environment with respect to documentation of polices and procedures, tasks and activities, monitoring, evaluation of operations, and oversight. We further sought to determine whether adequate physical security controls were in place to provide reasonable assurance that access to the file server room and the on-site and off-site media storage areas was limited to only authorized personnel. Moreover, we sought to determine whether sufficient environmental protection was being provided to prevent and detect damage or loss of IT-related equipment and media.

We evaluated whether an effective disaster recovery and business continuity plan had been implemented to provide reasonable assurance that IT operations could be regained within an acceptable period should a disaster render computer systems inoperable or inaccessible. We also sought to determine whether adequate controls were in place to ensure that backup copies of all critical and essential magnetic media were being generated on a scheduled basis, properly labeled, accounted for, and stored in secure on-site and off-site locations.

We sought to determine whether adequate system access security controls were in place to provide reasonable assurance that only authorized users would have access to the DYS' automated systems. We evaluated whether adequate controls were in place to prevent unauthorized access to systems and data and whether appropriate controls were in place to ensure timely deactivation of user privileges when access is no longer authorized or needed as a result of changes in employment or job status.

With regard to fixed-asset management, we evaluated whether policies and procedures were being followed, specifically whether hardware and software were safeguarded from unauthorized use and theft and were accurately reflected in the fixed-asset inventory and accounting records. We also determined whether an annual physical inventory was conducted. We sought to determine whether copies of software licenses were on file for microcomputer and LAN-based software.

Audit Methodology

To determine the areas to be examined, we met with DYS senior management to gain an updated understanding of IT-related and financial operations. We reviewed prior audit results and recommendations and reviewed the extent of progress in implementing recommendations brought forward in our prior report. To determine our audit scope and objectives in addition to our follow-up work, we reviewed documentation regarding the mission, organization, and management of DYS and conducted a pre-audit survey.

Regarding our review of organization and management, we interviewed senior management, reviewed and analyzed documentation provided, and reviewed IT-related management practices. To assess physical security and environmental protection, we interviewed management and inspected the file server room, on-site storage of backup magnetic media, and the office area.

To assess the adequacy of disaster recovery and business continuity planning, we interviewed management and determined whether formal, written, and tested business continuity and contingency plans had been developed to resume computer operations should the Department's LAN and microcomputer systems be damaged or destroyed. We also sought to determine that backup files were being generated and stored offsite. We observed selected operations, reviewed relevant documents, and performed selected tests. We also determined whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated.

To determine whether system access security controls were in place to provide reasonable assurance that only authorized users would have access to systems and data files, we sought to obtain system access security policies and procedures and to conduct selected tests. To determine whether only authorized access privileges existed on the system, we reviewed procedures for granting system access. To determine whether user IDs and password security were being properly maintained, we interviewed the security administrator and assessed the level of access security being provided. In addition, we compared and verified the system-generated list of staff authorized to access the automated systems to a list of then current DYS employees and vendors.

To evaluate whether the Department's hardware and software inventories were properly accounted for and controlled, we reviewed documented inventory control policies and procedures, obtained a copy of the inventory record, and reviewed the record layout for the appropriateness and comprehensiveness of required information. We assessed the adequacy of inventory controls by testing the integrity of the inventory record, determining whether equipment was properly tagged with DYS identification numbers, and determining whether annual inventory reconciliation had been performed. To determine whether inventory records were current, accurate, complete, and valid, we sampled items listed on the master inventory record and compared them to their physical locations. In addition, we traced items from their physical locations to the master inventory record. We also obtained an inventory of software licenses for microcomputer and LAN-based software. In addition, we reviewed DYS procedures for the reporting of lost or stolen property.

With regard to our review of prior audit results, we reviewed internal control policies and procedures for monitoring and evaluation of provider service contracts, hardware and software inventory controls, and MIS department organization and management.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted auditing practices. Audit criteria used in the audit included management control practices 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 upon our examination of internal controls at the Department of Youth Services, we found that although IT-related controls were in place for physical security and environmental protection, controls needed to be strengthened for hardware and software inventory, logical access security, and business continuity planning. We also found that the Department had not sufficiently addressed prior audit recommendations regarding hardware and software inventory control and the development of IT-related policies and procedures. However, DYS had implemented formal procedures to more adequately monitor and evaluate contracted service providers. The recommendations had been provided in our prior Audit Report No. 1999-0512-4C, issued on March 24, 2000.

We found that internal controls in place provided reasonable assurance for physical security and environmental protection for the DYS file servers and workstations in the central Boston office. We found the file servers at the central office were located within a file server room that was locked, well-maintained, clean, and temperature controlled. Our review revealed that system access security over the DYS local area network (LAN) needed to be strengthened to ensure that only authorized users have access to the system. We found that control practices needed to be strengthened to ensure that user accounts would be deactivated from the LAN in a timely manner for users no longer authorized or requiring access. However, during the course of our audit DYS put into place formal policies for mandatory timely reporting, verification, and deactivation of unauthorized users.

With respect to hardware and software inventory control, we found although policies were in place requiring a hardware inventory, the inventory system of record included detailed information only on IT resources located at the central office. Although a current inventory of software was not available, we found that DYS had the capability to determine what software products were installed on file servers and workstations. We found that the hardware inventory for the central office was complete and that it accurately reflected equipment on hand. It is our understanding that the Department was planning on developing a full inventory of all IT resources, including the 12 area offices and administration buildings.

We determined that the Department did not have a documented and tested disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems processed through the DYS's LAN be rendered inoperable.

AUDIT RESULTS

1. System Access Security

Our audit disclosed that although certain system access security controls were in place, other control procedures needed to be strengthened to provide reasonable assurance that only authorized users would have access to application systems and data files at DYS.

At the time of our audit, there were 947 employees and 526 user accounts, 417 of which were assigned to current employees. The remaining 109 user accounts were for 78 active contract personnel, eight project names, three IT-related consultants, and 20 individuals who had not been employed by DYS for over a year. Our audit determined that adequate procedures were not in place to ensure that access privileges would be deactivated in a timely manner for users no longer authorized or needing access to the automated systems and that authentication mechanisms would be reconciled on a periodic basis to current authorizations. Our system access security test of 526 user accounts revealed that logon IDs and passwords were left active for 20 system users who were no longer employed by DYS as employees or contract personnel. Based on interviews with the system administrator and requests for documentation, we determined that there was no written policy to deactivate user accounts from the LAN in a timely manner for employees and contract personnel whose authorization status had changed. Because there were no formal procedures in place to notify the MIS Department of individuals who no longer required or would be authorized access to DYS systems, MIS was unable to ensure that logon IDs and passwords would be deactivated in a timely manner.

The failure to deactivate user accounts that are no longer required decreases the overall effectiveness of logon ID and password security and increases the risk of unauthorized access to automated systems. Under such circumstances, user accounts that should have been deactivated may allow a prior employee or someone else unauthorized access to confidential or sensitive information. The access privileges of staff who have terminated or have had their job responsibilities changed would continue to be inappropriately available for use by anyone having access to the logon ID and password. Changes in employment status that would impact whether system access privileges should continue to be authorized would be termination of employment, change of position or job responsibilities, and extended leaves of absence where access is no longer required. In addition, the assignment of project-based logon capabilities to more than one person inhibits one from identifying actions taken by individual users who have been granted access privileges extending beyond read-only access. The latter makes it more difficult to hold individual users accountable for actions taken.

Generally accepted control practices and industry standards for IT operations support the need for formal, documented policies and procedures to assure that only authorized users have access to programs and data. The policies and procedures to deactivate logon IDs and passwords when an employee's employment status changes should specify mandatory reporting by departments to the IT Department as well as mandatory checks by the IT Department of current users and deletion of unauthorized user accounts. Failure to implement adequate controls regarding system access security could result in unauthorized system access that could result in unauthorized disclosure or use of confidential information or alteration of data.

During the course of our audit, the DYS removed the 20 invalid user IDs and by the end of the audit, DYS had begun to establish formal policies for mandatory timely reporting, validating, and deactivating user accounts for individuals no longer requiring or authorized access. We also found during the audit that documented evidence that users had been authorized to access IT systems was not available for all users. We note that efforts were made to strengthen the authorization process when DYS became a MassMail client.

Recommendation:

We recommend that the DYS strengthen their IT policies and procedures to more adequately address authentication integrity and deactivation of user access privileges for users no longer authorized or requiring access. The latter should include timely modification of access privileges for circumstances when employee responsibilities are changed. We recommend that DYS enhance their efforts to monitor and evaluate access security controls and to establish assurance mechanisms to ensure that related control objectives are met. Management should reassess on an annual basis the adequacy of procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.

Updated IT policies and procedures for access security should clearly identify related control objectives and management control practices. The updated policies and procedures should be cross-referenced to the Department’s internal control plan and include control practices to address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts. We suggest that access security policies and procedures include a formal approval procedure for granting the access privileges by data or system owners.

Active user accounts should be verified on a regular basis to employee payroll listings and authorized contract personnel listings, if any. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes). Formal reconciliation of authentication mechanisms (example, electronic lists of authorized users) should be performed at least twice a year or more frequently as access risks, or employee or contract personnel turnover warrants. The purpose of the procedures is to help ensure the integrity of the authentication mechanisms and to review and confirm access rights. We suggest that DYS confirm the appropriateness of access privileges for authorized users. In addition, periodic comparison of IT resources with recorded accountability should be made to help reduce the risk of errors, misuse or unauthorized access or alteration.

Since logical access to and use of IT resources should be restricted through adequate identification, authentication and authorization mechanisms, and the linking of users and resources with access rules, we recommend that efforts be made to eliminate or minimize the need for using multiple logons. In addition, to support the Department's access security framework, we also recommend that DYS ensure that all data are classified in terms of ownership and sensitivity (security categories) according to a data classification scheme.

To strengthen authorization, we recommend that documented evidence be maintained indicating the nature and extent of authorized access for each user.

Auditee's Response:

> "That the DYS strengthen their IT policies and procedures to more adequately address authentication integrity and deactivation of user access privileges for users no longer authorized or requiring access, and that DYS enhance their efforts to monitor and evaluate access security controls and to establish assurance mechanisms to ensure that related controls objectives are met."
>
> *DYS has begun implementing procedures to improve the monitoring and access to their systems. We will enhance our documentation and prepare detailed policies that mirror the procedures adopted. This process will be an ongoing function as software is upgraded and technological communication is improved. Currently, procedures are being addressed to prevent unauthorized people from accessing the DYS technology. Formal policies are being researched to improve the implementation and reduce redundancy.*
>
> *Security procedures are currently in place; they include a forced change of a user access password occurs every 42 days. Application access is limited to need and provided after employees receive application training to YSIS, MMARS, HR/CMS and soon to be MAJJIC.*
>
> *Procedures and policies will be reviewed yearly and adjusted as required.*
>
> "That access to security policies and procedures include a formal approval procedure for granting the access privileges by data or system owners."

The procedure surrounding this suggestion has been implemented but the policy has not been documented. This will be done. Currently we review the DYS user accounts bi-monthly. We send a quarterly listing by area of users with active accounts for their review of accounts on both DYS and non-DYS employees.

With the advent of MAJJIC additional controls and policies are being investigated and will be implemented, including stricter enforcement of non-DYS accounts. These are areas where we've asked the Area IT support team to become more actively involved.

"that DYS confirm the appropriateness of access privileges for authorized users."

User accounts are validated with Human Resources on a bi-monthly basis. In the field, all user accounts are reviewed with local IT personnel. We understand the importance and believe it is critical that former employees are removed from MMARS and HR/CMS, therefore, H/R has taken an active role in assuring terminated employees are removed from state comptroller systems. Involvement of Area IT personnel has been implemented with requests that Area field personnel monitor non-DYS employee's access and security levels.

Currently we validate on a quarterly basis all user accounts to the Magnet network, VPN certificates, dial-in access accounts, MMARS and HR/CMS accounts. Additional cross checking is done against the ITD recharge report for MassMail exchange accounts.

We recognize the importance of documenting the procedures and publish a policy to reflect these issues. The IT unit will develop policies and procedures.

"That efforts be made to eliminate or minimize the need for using multiple logons, that DYS ensure that all data are classified in terms of ownership and sensitivity (security categories) according to a data classification scheme, and that documented evidence be maintained indicating the nature and extent of authorized access for each user"

DYS agrees to this recommendation and seeks to fully address this recommendation when ITD approves the implementation of a single sign-on. Currently our users have upwards of five user id and passwords to remember. HR/CMS and MMARS each have their own passwords. VPN certificates, local login with exchange and YSIS each require user id and passwords. DYS has direct control over the YSIS (MAJJIC) implementation.

With the advent of the roll out of the new software, MAJJIC, we will adopt and implement new policies and procedures to control access to existing ownership and assure timely restriction and control to sensitive client data.

We will enhance and improve our documentation relative to user access and security levels. This will be an on-going process which will be incorporated with our user account review.

We will examine the use of an electronic method to log and maintain when new employees are assigned usernames and passwords. Currently we do not

> *maintain this detailed information; however we do have paper copies of MMARS and HR/CMS permission requests.*

Auditor's Reply:

DYS appears to be addressing the issue of access security. As procedures are implemented they need to be documented in the Department's internal control manual.

2. Business Continuity Planning

We determined that the Department did not have a documented and tested disaster recovery and business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems processed through DYS's LAN be rendered inoperable or inaccessible. The only document relating to business continuity planning that was available was a Y2K rollover plan that had not been updated since December 1999. Although DYS had procedures for testing the recovery of their database to resume operations in the event that ITD goes off line, there was no policy regarding recovery testing.

Although DYS was performing a nightly backup to tape of its ten file servers, we found that the Department did not store any backup copies of magnetic media in a secure off-site location. In addition, we found that added physical security should be applied to the on-site storage of backup copies located in the file server room. By not having backup copies stored off site, DYS incurred the risk that in the event of a disaster affecting the file server room, the on-site backup tapes in the file server room could also be destroyed along with data and programs residing on the file servers.

At the time of the audit, DYS had designated a DYS training room in Westborough as the Department's alternate processing site. However, no recovery tests had been performed from this site and its viability as an alternate site had not been validated. Since the level of equipment at this site was limited, further assessment is warranted. The absence of a tested business continuity plan, including recovery tests at an alternate processing site, does not provide the Department with sufficient assurance that mission-critical and essential data processing operations can be regained within an acceptable time period.

Because IT operations supports the Department and its area offices, the business continuity plan should take into account recovery strategies to address various scenarios, including the loss of IT components for each of the DYS offices. Without a formal, comprehensive recovery and contingency plan that includes required user area plans and network communication components, which has been sufficiently tested, the Department could be inhibited from processing information for YSIS or other applications residing on DYS' LAN, or from accessing information or processing transactions related to MMARS or HR/CMS residing on the ITD mainframe. As a result, DYS would be hindered from obtaining information needed to continue critical business operations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted control practices and industry standards for IT operations support the need for DYS 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. To that end, DYS should assess the extent to which they are dependent upon the continued availability of information systems for all required processing or operational needs and develop recovery plans based on the critical requirements of their information systems.

The assessment of impact should identify the extent to which departmental business objectives and functions are affected from loss of processing capabilities over various time frames. The assessment of criticality and impact of loss of processing should assist the Department in triaging its business continuity planning and recovery efforts.

The DYS, in conjunction with ITD, should perform a risk analysis of their IT systems to more clearly identify the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage or preclude the use of the systems and the likelihood and potential frequency of each threat. The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative critical character and importance of systems, and that adequate resources are available. The recovery strategies should address potential scenarios of loss of IT operations and should be based upon the results of risk analysis and an assessment of processing requirements. Without a formal, tested recovery plan, critical and essential information related to the Department’s clients and programs might be unavailable should the automated systems be rendered inoperable.

Sound management practices, as well as industry and government standards, advocate the need for comprehensive and effective backup and disaster recovery and business continuity planning to ensure that mission-critical and essential operations can be regained. Disaster recovery and business continuity planning should be viewed as a process to be incorporated within the functions of the organization, rather than as a project that would be considered as completed upon the drafting of a written recovery plan. Since the criticality of systems, importance of business objectives, or the risks and threats associated with IT operations may change, a process should be in place to identify the change in criticality, business requirements, or risks, and management should amend recovery and contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans. Business continuity and contingency planning has taken on added importance given that potential processing disruptions could be caused by man-made events.

Recommendation:

We recommend that DYS ensure that adequate off-site storage is in effect for backup copies of electronic media. The off-site location(s) should be accessible by only authorized personnel and should incorporate appropriate physical and environmental controls to protect the backup copies of magnetic media. We also recommend that a copy of the business continuity plan be stored in the off-site location along with any other required resources.

The DYS should establish a business continuity planning framework that incorporates critical and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of the Department’s systems is evaluated on an annual basis, or upon major changes to user requirements. The DYS should also conduct a formal risk analysis of its IT-related components, including outsourced services provided by ITD, on an annual basis, or upon major changes to the relevant IT infrastructure or to business operations or priorities. Based on the results of the risk analysis and criticality assessment, DYS should confirm its understanding of business continuity requirements and, if necessary, amend recovery plans to address mission-critical and essential IT-supported business functions.

The DYS should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical and essential operations within the needed time frames. In addition, the DYS should ensure that appropriate user area plans are in place and are sufficiently understood by administrative and operational management, as well as staff, to enable business areas to continue their operations should automated processing be lost for an extended period of time. The user area plans should take into account unavailable processing due to a loss of mainframe, LAN, or microcomputer-based system operations.

We recommend that DYS determine whether the Westborough alternate site is viable. If the site does not meet the Department's requirements, we recommend that another alternate processing site be identified and tested. We recommend that the business continuity plan identify the alternate site(s) that have been approved for business operations and data processing.

We further recommend that the business continuity plan be tested and formally reviewed and approved. The plan should be periodically reviewed and updated when necessary to ensure that it remains appropriate to recovery needs. The DYS should ensure that management and staff are adequately trained in the execution of the plan. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location. Since recovery actions may need to be made in concert with ITD or other third parties, we recommend that recovery tests be coordinated with ITD and any other required third parties and that a copy of the plan be available to appropriate ITD and third-party personnel. Moreover, the plan should provide for off-site storage of backup media and additional environmental protection of on-site storage of backup media.

Auditee's Response:

> "That DYS ensure that adequate off-site storage is in effect for backup copies of electronic media."
>
> "That a copy of the business continuity plan be stored in the off-site location along with any other required resources."
>
> *Remote site backup tapes are being sent to the Wormwood Street office on a weekly basis. Wormwood backup tapes are being stored off-site at a secure location. Every Wednesday each print and file server in our agency is checked to insure backups are being run correctly.*
>
> *The backup tapes along with software installation media are maintained in a fire-proof safe in the Wormwood computer room.*
>
> *The procedure and policies documenting this effort will be formalized and published.*
>
> *Our business continuity plan must be reviewed with the advent of the Majjic rollout. This recommendation will be addressed as part of the acceptance plan within Majjic as the business continuity plan continues to be a priority for the IT department.*

“[DYS] should establish a business continuity planning framework that incorporates critical and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training and communication.”

Addressing this suggestion is planned for the upcoming year with the implementation of MAJJIC as part of the rollout plan.

“[DYS] should conduct a formal risk analysis of its IT-related components, including outsourced services provided by ITD, on an annual basis, or upon major changes to the relevant IT infrastructure or to business operations or priorities.”

We have informally assessed our needs and have made the necessary adjustments. We will continue assessing our needs and improve on the documentation needed as part of our planning for the upcoming year.

“[DYS] should confirm its understanding of business continuity requirements and, if necessary, amend recovery plans to address mission-critical and essential IT-supported business functions.”

This suggestion is planned for the upcoming year.

“[DYS] should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios.”

This suggestion had been implemented over the past, and will be tested again once the roll out of the software and computers is completed. Our procedures are solid but the documentation is lacking. DYS will address this suggestion with the MAJJIC rollout, including documentation of tested failover tasks and procedures.

“[DYS] should ensure that appropriate user plans are in place and sufficiently understood by administrative and operational management, as well as staff, to enable business areas to continue their operations should automated processing be lost for an extended length of time.”

This suggestion will be addressed once the new software has been distributed, tested, and is in production mode for all agencies.

“That DYS determine whether the Westborough alternate site is viable.”

The DYS HADLEY Building was appropriate as a secondary fail over site, however the site may be closing. We are reviewing new procedures with an eye to utilizing the Westboro campus as our secondary alternative site. Wormwood remains our primary backup for the client application continuity site. Current implementation includes DB replication twice a week from ITD Chelsea data center and quarterly testing of failover procedures. Once the new location is determined, the site will become a business continuity location and will be fully tested. Documentation and procedures will be written to direct and instruct how the agency would continue operations during a major outage.

> "That the business continuity plans identify the alternative site(s) that have been approved for business operations and data processing."
>
> *Once the new site has been identified and the technology is place, successful testing will lead to the approval of the new alternative site.*
>
> "That the business continuity plan be tested and formally reviewed and approved."
>
> *The business continuity plan will be tested and formally reviewed and approved once the technology is in place. The current failover from ITD to Wormwood is tested regularly.*

Auditor's Reply:

DYS appears to be taking the necessary steps to address the objectives of business continuity planning. It is hoped the MAJJIC rollout can be incorporated within the business continuity plan. Since some parts of the plan appear to be scheduled for next year, the Department may be vulnerable until the plan is fully integrated and completed. Accordingly as the systems change, business continuity testing of the new configurations should be ongoing.

PRIOR AUDIT RESULTS

Status of Prior Audit Results
from the Office of the State Auditor's Report:
Audit Report No. 1999-0512-4C, issued March 24, 2000

Control Issue	Status
1. Monitoring and Evaluation of Service Provider Contracts	Partially resolved as of August 16, 2002 Resolved as of January, 2003
2. Hardware and Software Inventory Controls	Unresolved
3. MIS Department Organization and Management	Unresolved

1. Monitoring and Evaluation of Service Provider Contracts

Our prior audit had determined that DYS did not conduct sufficient monitoring and evaluation of contracted service providers. We had found that DYS had not established standardized written internal control policies or procedures for use throughout the Department to monitor contract performance or quality of services rendered to clients. Furthermore, because the DYS had no standard procedures in place to identify or assess potential internal control risks that might exist, there was no assurance that service providers were complying with contract terms or that clients were receiving quality service. Although monitoring and evaluation of service providers was accomplished to a limited degree under the direction of the area directors, and that periodic reviews were conducted by senior management, we had found that more stringent internal control procedures were needed to help ensure that the Commonwealth was receiving the goods and services for which it contracted. At that time, we had concluded that although DYS had been monitoring service providers, the evaluation process was informal and inconsistently exercised.

Our prior audit recommendation states that the Department of Youth Services "should establish written and standardized internal control policies and procedures for provider service contract monitoring and evaluation for use at all agency locations. Management should develop written policies and procedures that will ensure that all contract payments are reported in a timely and accurate manner and are supported with proper documentation."

Although our prior Audit Report No. 1999-0512-4C had been issued on March 24, 2000, adequate monitoring had not been initiated until January 2002. Because of this delay in implementing controls for monitoring and evaluating service provider contracts, adequate mechanisms were not in place to provide assurance that service providers were complying with contract terms or that clients were receiving quality service. The Operational Services Division's "Procurement Policies and Procedures Handbook," Chapter 5 states: "The Commonwealth has a responsibility to conduct monitoring and evaluation of the commodities and services purchased. These activities can assist in identifying and reducing fiscal and programmatic risk as early as possible, thus protecting both public funds and clients being served." Chapter 5 also provides several monitoring procedures including requirements to: "review and require progress reports to verify if contractor is meeting targeted performance deadlines." Because of the late start by DYS, there have been no annual progress reports. Furthermore, because DYS had not been following adequate monitoring and evaluation policies and procedures for timely payments to service providers, the Department may have been placed at risk of not being provided quality services.

At the beginning of our current audit, DYS had developed policies and procedures for monitoring and evaluating service providers. The agency had established a six-step monitoring process consisting of the following:

(1) Personnel Visit, this section deals with training,

(2) Programming Visit, this section deals with clients rights,

(3) Safety and Security Visit, this section deals with safety,

(4) File Visit, this section deals with building maintenance,

(5) Client Visit, this section deals with the intake and discharge of clients,

(6) This section is for wrap-up visits wherein previous visits and issues are reviewed, including a review of areas that might have been missed in previous sections.

DYS had also hired two staff members in October 2001 to monitor and evaluate service providers and, in January 2002, was in the process of implementing their six-step monitoring process. At the close of our audit, DYS had completed three of the steps of the monitoring process for all service providers. Subsequent to the audit, DYS had continued to make progress in monitoring and evaluating contracted service providers. Although at the beginning of our audit the prior audit result remained unresolved, efforts to enhance and implement a formal monitoring process had been addressed subsequent to the completion of our audit engagement.

Importantly, DYS needs to ensure that appropriate mechanisms are in place to verify that acceptable services are provided by contractors and vendors, and that approved payments are made to service providers in a timely manner, inasmuch as service provider contracts at DYS totaled $65 million in fiscal year 2001 and $68 million in fiscal year 2002.

Recommendation:

We recommend that DYS continue the process of monitoring and evaluating contracted service providers to assure that quality services are delivered and that payments are made to service providers in a timely manner.

Auditee's Response:

No response received.

2. Hardware and Software Inventory Controls

Our audit revealed that although the Department of Youth Services did maintain policies and procedures for maintaining an inventory of IT-related hardware, the inventory system of record included equipment for only the central office. Although DYS had totals of pieces of equipment located at field locations, no detailed information was available in the system of record. Based on our review of hardware and software fixed assets for fiscal year 2002 and related accounting and control practices in place, the DYS needed to strengthen its inventory practices to ensure that records regarding hardware inventories were current, accurate, complete, and valid.

With respect to maintaining inventory information on software, the DYS through the use of the automated auditing tool "AuditWizard" did maintain an inventory of software licenses; however, there were no formal, written policies in place for this. DYS did not comply with our recommendation from prior audit No. 1999-0512-4C, which stated "We recommend that DYS management develop and implement formal written standards, policies, and procedures regarding the authorization, installation, use, and recording of hardware and file servers and microcomputer-based software. We believe that controls should be strengthened to ensure that fixed assets are adequately accounted for and that inventory records are comprehensive, timely, and accurate." Furthermore, DYS failed to follow certain state regulations. Chapter 7, Section 4A, of the Massachusetts General Laws requires that each state agency maintain an automated asset management system reflecting all minor fixed assets. Without a complete inventory record of hardware and software, the DYS may be unable to detect theft or loss. During the course of our audit, the DYS created a complete hardware inventory for the central Boston office and is working toward a complete hardware inventory for the entire department.

With respect to policies for software inventory, during the course of our audit, DYS did create a policy that only authorized copies of software be installed and used by employees; however, the DYS should establish formal, written policies for software inventory control which require periodic review and reconciliation of the software inventory and reporting of lost or stolen software. Control measures should be in place to ensure that staff is aware of the guidelines for authorized use and the prevention and detection of unauthorized copies of software. Additional controls should be in place to monitor compliance with Departmental policies and procedures. The process of inventory control and maintaining a reliable record of software inventory must be appropriately assigned and managed to ensure that there is a reliable record maintained and that there is accountability in the process.

Undetected copyright infringements regarding software could place DYS at risk of legal action. The Commonwealth has specified strictures in Executive Order No. 286, regarding the illegal copying of software onto state-owned computers. Furthermore, Title 17 of the United States Code states, "*It is illegal to make or distribute copies of copyrighted material without authorization.*" Civil penalties include a maximum fine of up to $100,000 per infringement. Criminal penalties are imposed for 10 or more copies with a value greater than $2,500 and may include fines of up to $250,000 and incarceration of up to five years.

Generally accepted control practices and industry standards for IT operations support the need for agencies to have a complete hardware and software inventory.

Recommendation:

We recommend that DYS continue completing their hardware inventory for the entire department and immediately develop written, formal policies for software inventory control, as well as manage, develop, and implement formal written standards, policies, and procedures regarding the authorization, installation, use, and recording of hardware and file servers and microcomputer-based software. We believe that controls should be strengthened to ensure that fixed assets are adequately accounted for and that inventory records are comprehensive, timely, and accurate.

Procedures should be developed to ensure that only authorized software packages reside on Department systems. In addition, we suggest that the DYS establish a list of software deemed as "authorized" for use. We recommend that the DYS review all software currently in use to ensure that it is authorized and properly purchased. Moreover, we recommend that the DYS periodically review software residing on microcomputers hard drives to ensure that only authorized and legal copies are being used. Any unauthorized or illegal software copies should be immediately removed and, if necessary, replaced with purchased copies.

The Department of Youth Services should establish procedures for maintaining a perpetual inventory of software for the LAN and stand-alone systems connected to a LAN or workstation. Software inventory records should include all pertinent information such as origin of the software, cost, version, and number of copies purchased. As DYS upgrades or changes its software, the inventory should reflect the changes in a timely manner. Responsibility for maintaining the perpetual software inventory should be assigned to a staff member having sufficient independence from those who acquire or purchase software products.

Auditee's Response:

> "That DYS continue completing their hardware inventory for the entire department and immediately develop written, formal policies for software inventory control, as well as manage, develop and implement formal written standards, policies and procedures regarding the authorization, installation, use, and recording of hardware and file servers and microcomputer-based software."
>
> *This recommendation is valid and DYS will make a very serious effort to address these shortfalls. It will become an ongoing function. Due to our rapid expansion to address the agency's technological changes, our policies and procedures have not been maintained in a formal and organized manor. Formal procedures and polices will be improved and the documentation will reflect the changes.*
>
> "That DYS review all software currently in use to ensure that it is authorized and properly purchased."
>
> *A formal review has been made of all software licensing and we are in the process of validating these findings as part of the MAJJIC rollout. With the implementation of Windows 2000 and Auditwizard we have gained greater control over software that is loaded on our machines. We have manually reviewed the licensing needs of the agency and believe we are in full compliance for licenses on each machine and are at current supported revision levels.*
>
> "That DYS periodically review software residing on microcomputers' hard drives to ensure that only authorized and legal copies are being used."
>
> *The Director of Network Operations has determined that the Department of Youth Services has licenses for all software that has been distributed by the IT staff. This is an on-going requirement and will be reviewed on an annual basis.*
>
> "DYS should establish procedures for maintaining a perpetual inventory of software for the LAN and stand-alone systems connected to the LAN or workstation."
>
> *All software to date has been identified: AuditWizard and Spybot Search and Destroy software have been purchased and installed to help in identifying illegal software. Formal procedures will be developed and implemented.*

Auditor's Reply:

We are pleased that the Department is going to address this issue. Understandably, once an up-to-date, accurate and complete inventory is in place, it will be less of a challenge to maintain should appropriate inventory control practices be exercised. We will review their progress at the next scheduled audit.

3. MIS Department Organization and Management

Our audit revealed that although the Department of Youth Services did maintain policies and procedures for the MIS Department's organization and management, they are not complete. There are no policies for physical security or for environmental protection. Regarding System Access Security, at the start of our audit, there were policies and procedures for access to the LAN, but no policies to access Youth Services Information System (YSIS). During the course of our audit, DYS approved policies and procedures for all network access including YSIS. Implementation of procedures for hardware inventory and record keeping are incomplete. During the course of the audit, the DYS began to rectify this problem by developing a complete hardware inventory for the central Boston office and is working toward a complete hardware inventory for the entire department which includes 13 separate facilities. There are no policies for software inventory. At the start of our audit, there were no policies for monitoring and control of authorized software. During the course of our audit, DYS approved policies that only authorized copies of software can be installed and used by employees; however, the DYS should establish formal, written policies for software inventory control which require periodic review and reconciliation of the software inventory and reporting of lost or stolen software. There were no policies for on-site and off-site generation and storage of backup copies of magnetic media. Although there are policies and procedures for monitoring and evaluation of provider service contracts, DYS did not take action until January 2002, though our prior audit recommendation was published March 24, 2000. Due to the delay in implementing the prior audit recommendation only one of a six section process has been completed, and there have been no progress reports published. Also, although there are policies for monitoring and control of payments to service provider contracts, current written policies are not being observed. The DYS is planning on amending these policies to ensure that they are being followed.

The DYS had not adequately addressed our recommendation from prior audit No. 1999-0512-4C which stated, "We recommend that the Department of Youth Services administrators document their IT-related policies and procedures in order to provide sufficient guidance to IT operations. The development of documented policies and procedures should be focused on providing a control structure for managing IT processes and activities throughout the department. Given the pervasive nature of information technology, not all IT-related activities are performed by or are under the aegis of the MIS Department. The policies and procedures for all IT-related processes should be geared to those areas over and above the detailed procedures required by the infrastructure or specific systems. We further recommend that DYS administrators develop and document procedures to ensure adequate monitoring and evaluation of adequacy of documented internal controls systems."

Such documented policies and procedures would provide reasonable assurance that control and business objectives would be achieved. Formal documentation of IT-related policies and procedures provides a good basis for ensuring that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff, serve as a good basis for evaluation, and increase communication among personnel to improve operating efficiency and effectiveness. Clearly, well-trained personnel develop a better understanding of their duties and improve their levels of competence when documented procedures are followed. The absence of formal standards and policies leads employees to rely on their individual interpretations of what is required to be performed or properly control IT-related systems. In such circumstances, management may not be adequately assured that desired actions will be taken.

Failure to provide documentation of policies and procedures, to provide a statement of internal controls, and to require audit and management trails seriously undermines the capability of auditing the system. In addition to being a generally accepted control practice, Chapter 647 of the Acts and Resolves of 1989 requires that all state agencies have documented and approved internal control procedures.

Recommendation:

As noted in our prior audit report, issued March 24, 2000, we recommend that the Department of Youth Services document their IT-related policies and procedures in order to provide sufficient guidance to IT operations. The development of documented policies and procedures should be focused on providing a control structure for managing IT processes and activities throughout the department. Given the pervasive nature of information technology, not all IT-related activities are performed by or are under the aegis of the MIS Department. The policies and procedures for all IT-related processes should be geared to those areas over and above the detailed procedures required by the infrastructure or specific systems. We further recommend that DYS administrators develop and document procedures to ensure adequate monitoring and evaluation of adequacy of documented internal control systems.

<u>Auditee's Response:</u>

> "That DYS document their IT-related policies and procedures in order to provide sufficient guidance to IT operations."
>
> *DYS recognizes we are deficient in this area and will make efforts to address this gap. This recommendation will be addressed over the next several months.*
>
> "That DYS administrators develop and document procedures to ensure adequate monitoring and evaluation of adequacy of documented internal control systems."
>
> *This recommendation will become integrated within our rollout of MAJJIC and will be addressed over the next several months. The DYS Systems group will address this oversight on an on-going basis.*

<u>Auditor's Reply:</u>

We suggest that DYS use a recognized control model, such as CobiT, to use as a framework for developing and implementing IT-related control policies and procedures. By benchmarking against CobiT, DYS will be able to jumpstart the process of developing IT-related policies and procedures. Understandably, certain policies and procedures will need to address the requirements of specific IT platforms, systems, regulations, requirements, and management objectives.

APPENDIX

Agencies that provided surplus IT equipment donations to DYS

Criminal History Systems Board
Executive Office of Health and Human Services
Fiscal Affairs Division
Greenfield Community College
Information Technology Division
Massachusetts Commission Against Discrimination
Massachusetts Commission for Deaf and Hard of Hearing
Massachusetts Department of Transitional Assistance
Metropolitan District Commission
Office of Victim Assistance
Operational Services Division
Massachusetts State Police
Westfield State College