

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819

BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

A. JOSEPH DeNUCCI

AUDITOR

No. 2008-0512-4T

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

July 1, 2006 through August 31, 2008

**OFFICIAL AUDIT
REPORT
NOVEMBER 10, 2008**

TABLE OF CONTENTS

INTRODUCTION	1
---------------------	----------

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	3
---	----------

AUDIT CONCLUSION	7
-------------------------	----------

AUDIT RESULTS	11
----------------------	-----------

1. Youth Services Information System	11
2. User Account Management and Password Administration	14
3. Noncompliance with Chapter 647 Reporting Requirements	16
4. Inventory Control over Computer Equipment	18
5. Business Continuity Planning and Off-Site Storage	22

Appendix

Full Text of Auditee's Response	24
--	-----------

INTRODUCTION

The Department of Youth Services (DYS) was established by the Massachusetts Legislature under Chapter 838 of the Acts of 1969, amending Chapter 18A Massachusetts General Laws. DYS, which serves as the juvenile justice agency of the Commonwealth, receives administrative oversight from the Executive Office of Health and Human Services. The Department emanated from the nation’s first juvenile correctional system that began operations in the Commonwealth in 1846 on the premise that juveniles were more likely to be rehabilitated than adults. The DHS mission is to protect the public and prevent crime by promoting constructive changes in the lives of youth in their custody. DYS works in conjunction with communities, families, other state and federal agencies and private human service providers to accomplish its goals. The Department operates from a central office in Boston and five regional areas: northeastern, western, central, southeastern (including Cape Cod and the Islands), and metropolitan Boston. The Department received an appropriation of \$160.5 million in state funds for fiscal year 2008 and an appropriation of \$163.1 million in state funds for fiscal year 2009. At the time of our audit, the DHS had 892 employees.

DYS serves approximately 7,000 at-risk youth in the Commonwealth on an annual basis by providing a comprehensive and coordinated program of youth delinquency prevention and services to youth referred to, or placed in custody with, the DHS by the juvenile courts throughout the state. DYS operates a variety of residential programs ranging from highly secure facilities to community-based group homes and re-entry centers for youth. At the time of the audit, there were 2,091 youths committed by the Court to the custody of DHS. Of these youths, 1,867 were adjudicated as delinquent and were committed until their 18th birthday, whereas the remaining 224 were committed as youthful offenders until their 21st birthday. DYS is also responsible for approximately 300 youths being held on a daily basis by the Court at pre-trial detention programs.

The DHS Systems Unit is responsible for managing the Department’s information technology requirements. DYS’s mission is supported through the use of ten central network servers connected to 95 microcomputer workstations located at the central office in Boston. In addition, the DHS regional offices utilize 12 file servers connected to 650 microcomputer workstations located throughout 42 Community Reporting Centers (CRC) and 15 program locations. DYS also uses 65 Blackberry mobile data systems providing access to mission-critical applications. The Department relies on the Commonwealth’s Information Technology Division’s (ITD) mainframe for access to the Massachusetts Management and Accounting and Reporting System (MMARS) and the Human Resources Compensation

Management System (HR/CMS). In addition, DYS utilizes MassMail and Microsoft Outlook for email applications.

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 application was installed in 1998 to provide a data entry system to process mission-critical information. The YSIS data modules contain information relative to client histories, committed offenses, admissions, and discharges and warrant information.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the DYS information technology environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Department of Youth Services (DYS) during the period January 17, 2008 through August 31, 2008. The audit covered the period July 1, 2006 through August 31, 2008. The scope of our audit included an evaluation of IT-related controls pertaining to organization and management of IT activities and operations, physical security, environmental protection, system access security, inventory control for computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. Our audit also included a general review of the operation of the Youth Services Information System (YSIS). The review of YSIS consisted of an assessment of the application system for obtaining and processing mission-critical information in a timely manner, utilization of data modules, and management and staff user satisfaction.

Audit Objectives

Our primary audit objective was to determine whether the DYS IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives were in place and in effect to support business functions. Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and IT-related policies and procedures adequately addressed the areas under review. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets at the central office location as well as at selected regional sites. Our objective regarding system access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized personnel had access into the automated systems. Furthermore, we sought to determine whether DYS management was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. In addition, we determined whether an effective business continuity

plan was in place that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. We also sought to determine whether adequate procedures for on-site and off-site storage of backup media to support system and data recovery operations were in place.

We sought to determine whether the YSIS was supporting the Department's current business requirements and whether the application system's data was complete and timely.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of DYS's relevant operations and information technology environment. To obtain an understanding of the internal control environment, we reviewed the DYS organizational structure, primary business functions, and relevant policies and procedures. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of documented IT-related policies and procedures, we interviewed senior management and reviewed and assessed relevant IT-related internal control documentation. We also reviewed the organizational structure and reporting lines of DYS. For the areas under our review, we determined whether policies and procedures were in place, in effect, and communicated to appropriate staff. To determine whether IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of the personnel employed at DYS, including their duties and job descriptions, and compared the staff list to the organizational chart and each employee's stated day-to-day IT-related responsibilities.

To evaluate physical security, we interviewed senior management and security personnel, conducted physical inspections, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as office door locks, locked entrance and exit doors, the presence of personnel at entry points, whether sign-in/sign-out logs were required for visitors, and whether the facility was equipped with an intrusion alarm. We reviewed management policies and procedures regarding the distribution and usage of access codes to obtain entry to DYS facilities.

To determine whether adequate environmental controls were in place to properly safeguard areas housing computer equipment from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in place, we inspected the file server room to confirm the presence of appropriate dedicated air conditioning units and/or heating, ventilation and cooling systems (HVAC). In addition, we reviewed environmental protection controls related to general housekeeping procedures in the file server room, as well as selected areas housing computer equipment. Audit evidence was obtained through interviews, observation, and review of relevant documentation

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to the YSIS application. The application system, which resides on DYS's file servers, is accessed through workstations that are located at the DYS central administrative office and individual office facilities. We reviewed control policies regarding logon ID and password administration and password composition, evaluated the appropriateness of documented policies and guidance provided to DYS personnel and interviewed employees from the Systems Unit responsible for system access security. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted to only authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. We determined whether all individuals authorized to access system applications were required to change their passwords periodically and, if so, the frequency of the changes. In addition, we reviewed selected access user privileges, access logs, and evidence that passwords were required to be changed on a pre-determined basis. To verify that all users of the YSIS application system were current DYS employees, we compared a system-generated user account list for YSIS, dated April 2, 2008, that contained 720 user accounts to a DYS employee list, dated March 2008. We determined whether there were any changes in employment status between February 1, 2008 and March 31, 2008. We developed an exception list of those individuals no longer requiring access privileges to the YSIS application.

To assess the adequacy of inventory control procedures for computer equipment, we conducted an examination of DYS's inventory to determine whether controls were in place and in effect to properly account for and safeguard IT resources. We examined policies and procedures regarding the fixed-asset inventory to determine whether DYS was in compliance with the Office of the State Comptroller's regulations regarding fixed asset control. To confirm the existence and assess the proper recording of computer equipment, we randomly selected a sample of 101 out of 1,579 IT-related items listed on the DYS inventory, dated March 6, 2008, to locate the equipment and compare information for identification

tag numbers, location, description, and historical cost to what was recorded. In addition, we selected 121 items of computer equipment from their locations and determined whether the items were properly recorded on the inventory.

To assess the adequacy of business continuity planning, we determined whether any formal recovery or contingency planning had been performed for resuming computer operations should the network or application systems be rendered inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated. To determine whether backup copies of application systems and data files would be available for the recovery of IT operations, we determined whether backup copies were generated on a scheduled basis and stored at secure on-site and off-site locations.

To determine whether the YSIS application system was supporting the mission of DYS, we reviewed the use of the system to assess whether the system was meeting user needs and if application changes were required. We reviewed existing application modules within YSIS and compared those modules to the required hardcopy forms being maintained. We also conducted interviews with a cross section of DYS employees to gain and record an understanding of the difficulties and deficiencies with the current application system as it relates to their particular responsibilities.

We conducted our audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association.

AUDIT CONCLUSION

Our audit of the Department of Youth Services (DYS) determined that adequate internal control practices were in place and in effect to provide reasonable assurance that control objectives would be met in the areas of IT organization and management, physical security and environmental protection controls. However, our examination found that controls needed to be strengthened for system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and off-site storage of backup media. Our performance review of the Youth Service Information System (YSIS) revealed serious flaws in the functionality and security of the application system.

Regarding our review of the YSIS application, we found that the system was not capturing critical information, such as client location, medical consent and treatment information, educational assessments, and facility vacancies. Our audit evidence revealed that the YSIS application is used primarily for data entry processing throughout the central office and DYS regional facilities. We found that staff must revert to calling, faxing, and mailing to receive and give information on clients because of system inadequacies and limitations. We also found the YSIS application impedes management in analyzing data which is critical to evaluating the effectiveness of programs and that, as a result, committed youths may not be deriving the optimum benefits of remedial programs. These inefficiencies obstruct management's ability to properly monitor and deploy DYS staff. DYS management has been hindered in its efforts to standardize operations and improve efficiencies at each of its facilities because the system does not provide timely and relevant data to make key management decisions. We found that the application system also has serious security flaws, as it does not provide management with an audit trail of changes to records being made in the system. We found that the system does not function as a "real time" enterprise-based system and cannot be upgraded to meet the current business requirements of the DYS.

Our examination of IT-related organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties, and clear points of accountability regarding IT functions. We found that management and staff were well aware of their responsibilities and that documented job descriptions defined those responsibilities for IT positions. Our review of internal controls found that DYS, in conjunction with EOHHS, had developed and documented policies and procedures for certain IT-related functions. With respect to appropriate use of information technology, we determined that DYS had promulgated adequate written policies and procedures regarding e-mail and Internet use.

Our audit revealed that physical security controls at both the central office and at regional facilities selected for examination were in place and in effect to provide reasonable assurance that computer equipment would be protected from unauthorized access and would be operating in a controlled environment. We found that employees were required to wear identification badges and were assigned access security codes to gain entry to office areas. We also found that the file server rooms at the locations were locked and that access was limited to authorized staff members.

Our examination of environmental protection over the central office areas and the file server room revealed that appropriate control mechanisms were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss resulting from environmental hazards. Specifically, we found control objectives related to general housekeeping, air conditioning, fire prevention and detection, and emergency power and lighting would be met. However, our examination at the selected area facilities revealed serious deficiencies. We observed that the file server room at the Taunton facility was located in a former bathroom that has exposed water pipes. We found that computer equipment was not in elevated racks and that there were no water detection devices. Our review at the Boston-Metro facility revealed that a table fan attached to the server room door provided the only ventilation for the room. We also observed that certain IT-related equipment was also located on the floor at greater risk to physical and water damage. We recommend that management consider placing computer equipment in either cabinets or racks to help prevent damage from water should one of the sprinklers discharge. With regard to fire detection and suppression controls, we observed the presence of hand-held fire extinguishers, smoke detectors, and alarms and that automatic fire suppression systems were in place at each regional facility visited during the course of the audit. Written policies and procedures for environmental protection should be enhanced to include emergency shut down procedures. We recommend that these procedures should be clearly posted in the server rooms of each facility.

Our examination of access security revealed that although user account management and password administration provided reasonable access security for network access, adequate access security controls were not in place or in effect for the Youth Service Information System (YSIS). We found that system access security controls needed to be strengthened for the YSIS application that captures, stores, and provides mission-critical and sensitive information. Our tests of authorized user accounts for the YSIS application revealed that 13 out of 720 persons who were assigned user accounts could not be identified on the March 2008 official personnel record. Our examination revealed that these unidentified authorized users were former or retired employees having employment termination dates going back to April 2002.

Our review of password administration revealed that the processes for granting and recording authorization and activating logon IDs and passwords for network access were appropriate. Our examination of the initial network logon indicated that employees were required to change passwords by a predetermined timeframe and that passwords had to be composed of a minimum of eight alphanumeric characters. However, our audit tests of access security for the YSIS application that processes confidential information, including client histories, committed offenses, and warrant information, revealed that there were no policies or procedures for password change or composition. Our audit revealed that management had not established a mandatory timeframe for changing passwords for access to YSIS and that passwords had not been changed on a regular basis. Our audit evidence indicated that many users have maintained the same password since being initially trained on the system. We also found that the application system does not have the ability to detect or record unauthorized logon or data-change activities. The lack of controls over password administration places DYS at a high level of risk for unauthorized access to sensitive data residing on its mission-critical application. The failure to use generally accepted procedures for password composition and use places DYS at risk of unauthorized access to, or modification of, YSIS data for anyone having or gaining access to the DYS network. Because of poor password composition requirements, individuals could gain a higher level of access privileges than they were initially authorized to have.

Our audit revealed that DYS could not provide reasonable assurance that the system of record for computer equipment could be relied upon, since a complete annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. The absence of a reliable inventory of computer equipment hinders DYS's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives. Our analysis disclosed that the inventory record did not contain essential information regarding historical cost, date of purchase, installation date, and life cycle status. We also found that inventory records were separately maintained by site managers at individual facilities and were not being reconciled with the master record maintained at the Central Office. Our audit test of the inventory record disclosed that of the 101 randomly selected IT assets, 17 items could not be located. Also, we selected 121 items at various locations and found that 39 of these assets were not recorded on the master inventory list. As a result, DYS could not provide reasonable assurance of the integrity of its inventory system of record.

Our audit revealed that DYS was not in compliance with the Office of the State Comptroller's reporting requirements regarding stolen or lost assets. We found that the DYS management staff was unaware of the reporting requirements of Chapter 647 of the Acts of 1989. Although DYS had notified law

enforcement within a timely manner, the Department had failed to notify the Office of the State Auditor of two incidents of the theft of computer equipment valued at \$24,820.

With respect to business continuity planning and off-site storage of computer media, we found that controls needed to be strengthened to ensure that processing of mission critical applications should IT systems be rendered inoperable. Our audit disclosed that a formal, tested disaster recovery and business continuity plan was not in place for the timely restoration of computer operations with regard to the Youth Services Information System application. We recommend that DYS, in conjunction with EOHHS, test its business continuity plan to assess its viability and establish a process for routinely updating the plan based on changes to the technology, business processes, or staffing. DYS should ensure that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained.

We found that DYS lacked adequate controls over off-site storage of backup copies of systems and data files. Our audit revealed that, contrary to sound business practices, an employee of DYS was taking backup media, including confidential information, to their personal residence. We recommend that DYS management find a secure off-site location to store its backup computer-related media.

Based on our observations and interviews, we found that DYS management and staff were dedicated to its mission to protect the public and prevent crime by promoting constructive changes in the lives of youth in their custody.

AUDIT RESULTS

1. Youth Services Information System

Our review of the mission-critical Youth Services Information System (YSIS), which was initially installed in 1998 to provide management with an automated case management system, revealed serious flaws in the functionality and security of the application system. We found that the YSIS application does not have the capability to track clients on a real-time basis, provide support staff with critical medical and educational assessments for each client, and provide management with the necessary information to effectively and efficiently monitor and evaluate programs and individual cases. DYS is well aware of these application deficiencies and has taken appropriate steps to acquire a new application system. However, a new system with the necessary information and functionality had not been acquired and implemented at the end of our audit. The absence of an enterprise-based and comprehensive case management system hinders DYS's ability to fulfill its business objectives, which include strengthening client services, increasing safety and security of clients and staff, increasing inter-agency collaboration, and enhancing public safety.

We found that DYS must depend on thousands of paper forms and spreadsheets that were often created by individual staff members for their exclusive use. The continued use of paper files has significantly impacted the workflow, and because YSIS is not an enterprise-based system, information between social workers, case managers, and clinicians cannot be shared in a timely manner. Our analysis of the data elements contained in the application indicated the absence of certain critical information. For example, we found that management could not place reliance on information in the YSIS database to determine whether a suicide assessment of a youth entering DYS custody had been performed within the required timeframe. We also found that client medical history information containing known allergies and other medical conditions were not being electronically recorded. The data in the application does not contain individual client emergency medical information, such as the "Permission to Treat" form. This form is necessary to provide emergency medical treatment in cases where the legal guardian of the youth cannot be contacted.

Our audit revealed that the information in the YSIS application does not support an automated daily inventory of available beds for the placement of youths who have been taken into DYS custody. The absence of an automated system to account for available beds has resulted in inefficiencies in placing clients in proper facilities. We found that as a result of not having a computerized bed count system,

DYS is incurring additional transportation expenses and is being hindered from being able to properly plan staffing levels to meet the needs of its clients at the various facilities.

We found that the YSIS application lacked sufficient security controls, such as the ability to capture or log event history information that would identify users who were accessing confidential information or making changes to records. According to DYS management, the age of the application has made it difficult to implement any important program changes including enhancing security controls or provide an audit trail to detect changes to client records and case management information.

The IT Governance Institute has promulgated information technology best practices through the publication titled "VAL-IT" that details criteria for organizations to align technology with business objectives. The document advises organizations to "*make sure the business direction to which expenditures on IT-enabled business investments should be aligned is understood, including the business vision, business principles, strategic goals and objectives, and priorities. Make sure there is a common and agreed understanding between the business and the IT function regarding the potential impact of IT on the business strategy and the role of IT in the enterprise, and ensure that this is broadly communicated.*" Fulfillment of this objective will require the replacement of the YSIS application and implementation of a business-aligned comprehensive case management system.

DYS management initiated the process to replace the current application by submitting a "Request for Response" (RFR) proposal through the Commonwealth's procurement website (Comm-PASS) in November 2005. An internal procurement management team conducted an extensive three-stage evaluation process resulting in a unanimous selection of a private vendor to develop the new application system. The new application would replace YSIS with an enterprise-based application that would provide management key evaluation and monitoring tools to effectively and efficiently meet business objectives. The new application would also meet ITD's data classification requirements and provide features to meet current industry security standards. DYS management has indicated through an investment brief submitted in April 2008 to the Commonwealth's Information Technology Division that the new application "*will allow the department to effectively manage their resources and, most importantly, their committed youths across the agency in real-time in order to provide the greatest benefit for the youth and the community.*" It is critically important that relevant and reliable information be readily available to authorized DYS staff when required to process cases and to act effectively in a timely manner to ensure the health and safety of clients. At the close of our audit DYS had yet to procure the necessary funding to acquire and implement the new system. As a result, the safety and welfare of youth under DYS custody continues to be jeopardized until a system is implemented that captures and provides all relevant data related to each case in a timely manner.

Recommendation:

We recommend that DYS management continue to seek approval for funding to support the acquisition and implementation of a new application system to replace YSIS. We recommend that DYS management seek to align use of technology with the mission, responsibilities and goals of the Department.

Auditee's Response:

DYS management agrees with the Auditor's recommendation and has been working for over two years to obtain funding to support the acquisition and implementation of a new application system to replace YSIS. As stated in the audit report "the absence of an enterprise-based and comprehensive case management system hinders DYS' ability to fulfill its business objectives which include strengthening client services, increasing safety and security of clients and staff, increasing interagency collaboration and enhancing public safety".

The Department of Youth Services (DYS) is seeking to replace the current system used to intake and track committed youths across the Commonwealth and promote an agency-wide enterprise system that will allow us to effectively manage resources and, most importantly, provide real time data on committed youths across the agency. Timely access to client information, such as medical or clinical documents and educational records, is critical. Our present reliance on a paper system is inefficient and ineffective and we are actively seeking to implement a new electronic enterprise management and client tracking system.

The ongoing effort is to move the agency forward toward an enterprise management system and replace the existing application. In order to execute and pursue that strategy, DYS hired Keane to manage the vendor selection process using their "Packaged Software Selection & Implementation (PSS&I) Methodology Framework": a software selection and implementation strategy that operates in tandem with a robust requirement analysis stage adopted from Rational Unified Process [RUP] methodology.

(For full background chronology of RFP process see Appendix)

Auditor's Reply

We acknowledge that DYS has followed an appropriate RFP process for acquiring a comprehensive and integrated case management system to meet its business needs. We urge DYS management to continue to pursue the necessary resources to develop and implement the new system. If the resources necessary to proceed are made available to replace YSIS, continued due diligence will need to be exercised over the system modification and implementation process. The application of system development life cycle methodology, or good project management techniques, will help ensure that modification and

implementation costs are minimized, the right set of features are built in, training and documentation are addressed, and the system functions as intended.

2. User Account Management and Password Administration

Our audit found that although access security over the Department's network appeared to be appropriate, controls needed to be strengthened to ensure that only authorized users have access to the YSIS application system and that user privileges are deactivated for individuals no longer authorized to access automated systems. Overall, we found that appropriate policies and procedures were documented, security administration had been assigned, and that appropriate rules for user account activation, password composition, and frequency of password changes were in place for user access to the DYS network.

Although we found that adequate controls were in place to authorize and activate user accounts to the DYS network, controls needed to be strengthened to ensure timely deactivation of access privileges for users no longer authorized to access the Department's automated systems. Our tests of system access security for DYS' automated systems indicated that there were inactive user accounts that had not been deleted for individuals who were no longer employed by the Department. Our tests of authorized user accounts indicated that 13 out of 720 persons who were assigned user accounts could not be identified on the March 2008 official personnel listing. For example, our audit test disclosed that an employee, who terminated employment with DYS in May 2002, still remained on the user account list as of March 2008. Moreover, our audit revealed that there were no formal policies and procedures in place requiring notification from the Human Services Division to the Systems Unit to initiate the removal of access privileges of individuals who terminate employment with the Department. Our audit evidence indicated that a reconciliation of the user account list to authorized employees was only being performed on a periodic basis.

Our audit revealed that increased monitoring of user accounts was required to evaluate user account access and identify user accounts that should be deactivated to ensure that only authorized individuals had access privileges to the Department's network and automated systems. The failure to deactivate or delete user accounts in a more timely manner places the Department's automated systems at risk of unauthorized access or having an individual gain higher access privileges than currently authorized. As a result, certain information residing on the DYS network or the YSIS application could have been vulnerable to unauthorized access.

The Control Objectives for Information and Related Technology (CobiT), issued by the Information Systems Audit and Control Association, is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners, and IT functions. Additional controls recommended by the CobiT control framework include having procedures to ensure timely action for requesting, activating, suspending and closing user accounts, having a control process to periodically review and confirm access rights, and regularly performing scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse or unauthorized change.

Regarding our examination of password administration for the mission-critical YSIS application we found that management had not established a mandatory timeframe for changing passwords. Our audit evidence indicated that many users have maintained the same password since being initially trained on the system. We also found that the application system does not have the ability to detect or record unauthorized logon or data-change activities. The lack of controls over password administration places DYS at a high level of risk for unauthorized access to sensitive data residing on its mission-critical application. The failure to use generally accepted procedures for password composition and use places DYS at risk of unauthorized access to YSIS by anyone having or gaining access to the DYS network. As a result, individuals could also gain a higher level of access privileges than they were initially authorized to have for this application system.

The Commonwealth of Massachusetts “Internal Control Guide for Departments” promulgated by the Office of the State Comptroller states, in part, “an employee’s password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibility.” CobiT’s control practices recommend that organizations have password policies that include “an appropriate and enforced frequency of password changes.” In addition, computer industry standards advocate that policies and procedures for all aspects of system access security be documented and approved to provide a basis for IT systems and data. The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access.

Recommendation:

We recommend that DYS perform an immediate review of the status of all active users to the network and application systems and deactivate access privileges for those individuals who no longer require access. We recommend that DYS management develop written policies and procedures requiring timely notification to the Systems Unit’s security administrator of any of changes in employee status that could

warrant change or deactivation of access privileges to the Department's network or application systems. We also recommend that the Department implement preventive and detective control mechanisms, such as vigilant monitoring of access accounts to ensure that only authorized individuals have appropriate levels of access to IT resources.

Regarding password administration over the YSIS application, we urge management to immediately implement policies and procedures to prompt users to change their passwords within an established timeframe.

Auditee's Response:

The DYS network administrator has conducted a review of all users of the network and deactivated access for those individuals who no longer work for the agency. DYS management will develop a written policy requiring notification to the network administrator of a change in an employee's status that would require deactivation.

Until the policy is developed, the DYS Human Resource Unit will send the network administrator an email when an employee has left DYS active employment. A confirming email will be sent to HR after the user has been deactivated.

YSIS does not have the functionality to allow users to change their own password. The network administrator will validate all YSIS user profiles, change the password and send an email notification to the users the password has been changed. This process will have to be executed every six months until YSIS is replaced.

The new JJEMS system will use the Access Identity Management System (AIMS) for a single sign-on that is linked to the EOHHS security policies.

Further, the DYS CIO is developing an IT survey to establish a baseline of several facets of the system which affect how data is stored, accessed, used in order to more precisely study data security.

Auditor's Reply

We commend the Department's action for addressing the security concerns related to user account management. We believe DYS should continue to ensure that user privileges be clearly specified and documented for every active user account and constantly monitored and evaluated to ensure that only authorized users are allowed access to DYS application systems and other IT resources.

3. Noncompliance with Chapter 647 Reporting Requirements

Our audit disclosed that DYS did not report to the Office of the State Auditor (OSA) the thefts of a total of 58 used laptop computers which the Department estimated the value to be \$24,820. Chapter 647 of the

Acts of 1989, an Act Relative to Improving the Internal Controls within State Agencies, requires agencies to immediately report unaccounted-for variances, losses, shortages, or thefts of funds or property to the OSA. Chapter 647 also requires the OSA to determine the internal control weaknesses that contribute to or cause an unaccounted-for variance, loss, shortage, or theft of funds or property; make recommendations to correct the condition found; identify the internal control policies and procedures that need modification; and report the matter to appropriate management and law enforcement officials.

Our audit revealed that the first theft was reported to the Boston Police on January 4, 2007 and that the second theft was reported on January 22, 2007. The Boston Police Department completed incident reports on both thefts and forwarded the reports to the Massachusetts State Police. However, since the Department was unaware of the reporting requirements of Chapter 647 involving missing or stolen equipment, a report of the thefts was never filed with the OSA. Subsequent to our discussions with DYS administrators, a written policy and procedure was developed and implemented to ensure that any future incidents of thefts or lost equipment would be reported to the OSA in compliance with the requirements of Chapter 647.

A primary cause of the thefts was traced to the fact that the computer equipment had been stored in a first-floor location highly visible from outside the building. We believe that the change of office location from the first floor to the fourth floor will minimize the risk factor of future thefts of computer equipment at the Central Office.

Theft of Notebook Computers

<u>Date of Theft</u>	<u>Description</u>	<u>Number of Stolen Items</u>	<u>Cost Per Item</u>	<u>Total Cost</u>
1/04/2007	Dell Notebook Computers	15	\$400	\$6,000
1/22/2007	Dell Notebook Computers	42	\$420	\$17,620
1/22/2007	Gateway Notebook Computer	1	\$1,200	\$1,200
Totals		58		\$24,820

Recommendation:

DYS senior management should familiarize themselves with all Chapter 647 internal control requirements. DYS should then implement and maintain policies and procedures that will ensure compliance with Chapter 647 of the Acts of 1989 and report all instances of unaccounted-for variances, losses, and thefts of funds or property to the Office of the State Auditor.

Auditee's Response:

DYS management is now familiar with chapter 647 and will have procedures put in place to ensure all unaccounted for variances, losses and thefts of funds or property are reported to the Office of the State Auditor and others as required by the law. The DYS Legal Unit will issue an advisory and a policy to inform all DYS staff of our reporting responsibilities under Chapter 647 and will coordinate these efforts with the EOHHS Compliance Office.

Auditor's Reply

We are pleased that DYS has currently familiarized management and staff with the requirements stipulated under Chapter 647. The objectives of Chapter 647 not only include notification of loss or stolen equipment or assets to be reported to the Office of the State Auditor, but also require state agencies to review and evaluate their internal controls. Safeguarding and reporting on the loss of computer equipment is critical not just because of the loss of the hardware, but also more importantly because of the data that may be stored on the equipment.

4. Inventory Control over Computer Equipment

Our audit disclosed that inventory controls over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the Department's inventory system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. We found that controls needed to be strengthened to update the inventory record when equipment is relocated, disposed of, or lost or stolen. We also found that inventory records were separately maintained by site managers at individual facilities but were not being reconciled to a master system of record maintained by the Central Office. In addition, inventory records were not being adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation had not been performed. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders DYS's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Our audit tests of the Department's system of record for IT-related equipment indicated weaknesses in the accounting of IT-related assets. The Department provided an inventory system of record that listed IT-related assets as of March 6, 2008. Based on a randomly selected sample of 101 items of computer equipment selected from the inventory record, we attempted to verify by inspection the existence and the recorded location of the computer equipment. We found that 17 pieces of computer equipment were not at the locations indicated on the inventory record and could not be found by the Department. Of the 84 items that were located, all were properly tagged, and the inventory system of record correctly listed tag and serial numbers, and location. Furthermore, to verify the integrity and completeness of the inventory system for computer equipment, we randomly selected 121 additional items of computer equipment from actual floor locations and determined whether all items were listed on the Department's system of record. We found that of the 121 items selected, 39 (32%) of the selected items were not recorded on the inventory record. The lack of a complete inventory of computer equipment hinders the Department's ability to properly account for available hardware systems and undermines its ability to detect missing or stolen equipment.

We found that although most of the appropriate data fields, such as description, identification tag, user name, serial number, and location were included in the data record, the system lacked data fields for historical cost, condition, acquisition date and installation date. Recording historical cost and acquisition date in inventory systems of record is required by Commonwealth of Massachusetts regulations for all departments to provide a comprehensive, auditable inventory record of fixed assets. By failing to record the historical cost of purchased or leased computer hardware items and their acquisition dates on DYS's inventory system of record, DYS was not in compliance with the Office of the State Comptroller's 2005 fiscal year fixed-asset requirements and Office of the State Comptroller (OSC) Memorandum No. 313A. In addition, inventory valuation for computer equipment could not be analyzed and evaluated, and we were unable to determine the total value of the inventory because the cost was not recorded in their respective data fields.

Without formal, documented, and tested procedures for performing an annual physical inventory count and reconciliation of the inventory record to purchase or lease documentation and surplus equipment records, DYS management cannot be adequately assured that its computer equipment is properly accounted for and that the inventory record is comprehensive, timely, and accurate. In addition, a periodic comparison of the computer equipment and the recorded accountability of the computer equipment will reduce the risk of unauthorized use, loss, or theft of computer equipment. We believe that the weaknesses in inventory control were the result of lack of adequate monitoring and management oversight, and proper assignment of inventory control responsibilities.

Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of 1989 states, in part, that “the agency shall be responsible for maintaining accountability for the custody and use of resources and assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts.” Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

A primary contributory factor to the control weaknesses in inventory control and the accounting of IT resources area was that senior management did not appear to rate inventory control as a high enough priority or adequately identify inventory control as an administrative management function.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that the Department strengthen current practices to ensure compliance with policies and procedures documented in the Office of the State Comptroller’s “MMARS Fixed Asset Subsystem Policy Manual and User Guide,” and its associated internal control documentation, and the Operational Services Division’s guidelines regarding the accounting for and disposal of property and equipment. The Department should implement these control procedures to help ensure that all IT-related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that the Department can maintain a comprehensive record of all IT-related equipment on a perpetual basis. The Department’s inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

We recommend that the Department perform an annual physical inventory and reconciliation of its IT resources to ensure that a relevant and reliable inventory record of IT resources is in place. We recommend that the inventory system of record be periodically verified through reconciliation to physical hardware, acquisition, and disposal records. The reconciliation and improved documentation will help ensure the integrity of the Department’s perpetual inventory system of record for IT-related assets, provide reasonable assurance that the inventory records can be used to support IT configuration management, and help safeguard computer equipment. We further recommend that the Department’s system of record for IT inventory be expanded to include data fields containing information relative to cost, condition, acquisition and installation dates, and status of the IT resource.

Auditee's Response:

The Dept of Youth Services has been working with EOHHS Secretariat to bring all DYS locations together to be directly supported by the EOHHS IT Operations Services Group. An agreement was reached in September of 2008, with implementation planned for November, 2008. DYS will transfer the six employees currently supporting DYS IT operations into the EOHHS Operations Services Group and become one of six HHS agencies supported by this consolidated effort. The combined resources in this unit will improve IT services to DYS by utilizing a larger pool of support personnel, assigning a site manager to each location and using EOHHS procedures, standards, tools and techniques.

In the area of inventory control the following service will be provided by EOHHS Operations Services.

- 1. Assures that an actual annual physical inventory is conducted.*
- 2. Establishes IT asset recording input and control guidelines for IT Site Manager*
- 3. Determines allocation and configuration of hardware and software.*
- 4. Assures that all hardware and software is entered into inventory database upon receipt.*
- 5. Determines and maintains IT asset warranties and maintenance contracts.*
- 6. Serves as liaison with external organizations for IT asset reporting purposes(e.g. facilities, budget, A&F, procurement)*

The inventory management database used by EOHHS "ARGIS" does capture cost, condition, acquisition, and install dates of equipment.

Improving Computer facilities at remote sites

The EOHHS network upgrade for the VOIP (voice over internet protocol) project requires all computer server and switching equipment locations to be brought up to standards required by Verizon. Environmental issues that were identified in the audit report will be corrected as part of the VOIP installation over the next 12 months.

Auditor's Reply

We commend the actions initiated by DYS in working with EOHHS to improve fixed-asset inventory controls. We believe a single comprehensive inventory control system for all DYS computer equipment is an important ingredient for the Division's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding computer equipment and assist DYS and EOHHS in making IT infrastructure and configuration management decisions.

We believe that controls to ensure adequate accounting of computer equipment will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record as prescribed in the recommended "operation service" guidelines. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any lost, stolen, or surplus equipment. In addition, these efforts should help minimize the risk of lost or stolen

equipment and improve the identification of the status of equipment for configuration management purposes.

5. Business Continuity Planning and Off-Site Storage

We determined that DYS had not formalized a comprehensive disaster recovery and business continuity plan for restoring critical functions in the event that automated systems were rendered inoperable or inaccessible. We acknowledge that DYS was aware of the need for business continuity planning. However, at the time of our audit, we determined that DYS's business continuity plan consisted of a draft copy of its Continuity of Operations Plan.

To ensure that a formal business continuity plan is documented and available, DYS should document recovery strategies with respect to various disaster scenarios. Without a comprehensive, formal, and tested recovery strategy, DYS may experience delays in re-establishing mission-critical functions, such as its YSIS application, various database information, and acquiring and installing IT resources needed to restore IT processing, as well as to timely recover backup information from off-site storage. The lack of a detailed, tested plan to address the resumption of processing capabilities may hinder the recovery of essential and confidential data should a disaster render IT systems inoperable. Without a formal, tested recovery strategy, DYS may experience difficulties in fulfilling its mission of public safety and providing essential services to youths in custody in an efficient and effective manner in accordance with its stated mission.

The objective of business continuity planning is to help ensure timely recovery of mission-critical 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 business practices and industry standards for computer operations support the need for DYS to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate contingency and recovery plans. To that end, DYS should assess the extent to which it is dependent upon the continued availability of information systems for all required processing and operational needs, and develop its recovery plans based on the critical aspects of its information systems.

Our audit revealed that contrary to sound business practices for providing appropriate controls for off-site storage of back-up media, DYS permitted storage of back-up media at an employee's personal residence. Since we could not validate the security of the off-site location, there is no assurance that the back-up media was secure and would be readily available to assist recovery efforts. In addition, the ability to provide adequate security of the off-site information may be at risk.

Recommendation:

We recommend that DYS management work to develop, implement, and test a disaster recovery and comprehensive business continuity strategy for its application system, databases, and network capabilities critical to the Department's operation. We recommend that DYS formally assess the impact of the loss of IT operations and determine the extent to which contingency plans can be developed to address recovery of critical business operations. We further recommend that DYS develop user area plans appropriate to the Department's IT processing environment and information accessibility requirements. Once a formalized plan has been adopted, we recommend that DYS test the plan to assess its viability and establish a process for routinely updating the plan based on changes to recovery efforts, technology, business processes, or staffing. DYS should ensure that all personnel responsible for business continuity tasks and activities be clearly identified and adequately trained.

Regarding the off-site storage of weekly back-up copies of computer media, we recommend that DYS management find a secure and easily accessible off-site location and prohibit storing back-up media at employees' personal residences.

Auditee's Response:

The YSIS production server is located at MITC. DYS has two backup servers for YSIS that are updated every night at midnight; one at 27 Wormwood Street, Boston, and one in the DYS Springfield office. In the event the YSIS production server is down, the end users have instructions to connect to the backup server in Boston. If the Boston server is down, they are instructed to connect to Springfield. This will give users access to data from the previous midnight.

Part of the agreement with EOHHS Operations Services Group is that they will develop, advance and execute an agency-wide information technology continuity & disaster recovery planning effort. (See item # 4 above.)

DYS intends to execute a contract for an off-site media storage program with Iron Mountain Storage Services. They will provide weekly pickup & storage of backup media. This will be in place in October 2008.

Auditor's Reply

We acknowledge DYS's action in having appropriate back-up procedures to aid recovery efforts. However, a comprehensive and well documented business continuity and contingency strategy is essential to ensure timely recovery of mission critical and essential business functions and systems. Until appropriate disaster recovery and continuity plans are completed, DYS needs to continue to focus on risk management and contingency planning.



The Commonwealth of Massachusetts

Executive Office of Health and Human Services

Department of Youth Services

27 Wormwood Street, Suite 400
Boston, MA 02210-1613

DEVAL PATRICK
GOVERNOR

TIMOTHY MURRAY
LIEUTENANT GOVERNOR

JUDYANN BIGBY, M.D.
SECRETARY

JANE E. TEWKSBURY, Esq.
COMMISSIONER

October 10, 2008

Mr. John Beveridge, Deputy Auditor
Office of the State Auditor
IT Audit Division
One Ashburton Place Room 1819
Boston, Ma. 02108

Dear Mr. Beveridge,

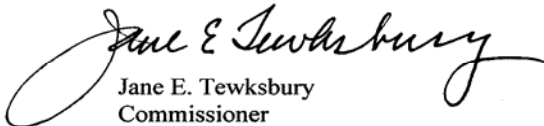
Attached please find the Department of Youth Services' (DYS) response to the Office of State Auditor's (OSA) Information Technology Audit conducted at this agency from January 17, 2008 through August 31, 2008 (covering the period of July 1, 2006 through August 31, 2008.)

As you know, we are in agreement with your recommendations as reviewed in the final briefing meeting with you on September 30, 2008. In the attached document, we have responded in detail to the five (5) findings listed in your audit results. I am pleased to let you know that we have begun implementing some of the OSA recommendations and plan to implement all recommendations as funding becomes available for the Department's Juvenile Justice Enterprise Management System (JJEMS).

We appreciate the professionalism demonstrated by your auditors during this engagement. During each and every discussion and meeting with members of the DYS staff, it was apparent that their goal was to help us safeguard critical client information and improve our protocols for technical operations. I hope you will convey my appreciation to them.

Again, thank you for the opportunity to respond to the Office of State Auditor findings. If you require additional information you may contact me or the DYS Chief Information Officer, Bob Brennan.

Sincerely,


Jane E. Tewksbury
Commissioner

Item 1 Youth Services Information Systems**Auditors Recommendation:**

We recommend that DYS management continue to seek approval for funding to support the acquisition and implementation of a new application system to replace YSIS. We recommend that DYS management seek to align use of technology with the mission, responsibilities and goals of the Department.

DYS Response

DYS management agrees with the Auditor's recommendation and has been working for over two years to obtain funding to support the acquisition and implementation of a new application system to replace YSIS. As stated in the audit report "*the absence of an enterprise-based and comprehensive case management system hinders DYS' ability to fulfill its business objectives which include strengthening client services, increasing safety and security of clients and staff, increasing interagency collaboration and enhancing public safety*"

The Department of Youth Services (DYS) is seeking to replace the current system used to intake and track committed youths across the Commonwealth and promote an agency-wide enterprise system that will allow us to effectively manage resources and, most importantly, provide real time data on committed youths across the agency. Timely access to client information, such as medical or clinical documents and educational records, is critical. Our present reliance on a paper system is inefficient and ineffective and we are actively seeking to implement a new electronic enterprise management and client tracking system.

The ongoing effort is to move the agency forward toward an enterprise management system and replace the existing application. In order to execute and pursue that strategy, DYS hired Keane to manage the vendor selection process using their "Packaged Software Selection & Implementation (PSS&I) Methodology Framework": a software selection and implementation strategy that operates in tandem with a robust requirement analysis stage adopted from Rational Unified Process [RUP] methodology.

On November 1, 2005, an RFR was issued to solicit detailed proposals from bidders and to procure services, a development tool or framework, or a Commercial Off-the-Shelf (COTS) application that meets DYS' requirements for a Juvenile Justice Enterprise Management System (JJEMS). The RFR was posted on Commonwealth's procurement website (Comm-PASS).

On August 31, 2006, after completing an extensive three-stage evaluation process, a procurement management team made up of both DYS business managers, representatives from ITD and EOHHS and technical consultants, was unanimous in its recommendation to DYS to commence negotiations with one of the eight bidders, Consilience Software.

Consilience Software has a good reputation working within EOHHS. The Department of Public Health (DPH) has purchased their software and developed several applications over the past three years. Consilience has recently completed an integration of the DPH applications into the Virtual Gateway and Access identity Management System

In March of 2007, DYS contract negotiations with Consilience were suspended due to lack of funding.

In March of 2008, the Executive Office of Health and Human Services (EOHHS) formed an IT steering committee made up of senior level managers from both the business and technology sectors of all EOHHS agencies. Deputy Commissioner Edward Dolan and Chief Information Officer Robert Brennan from DYS were appointed to serve on this committee. The first task of the committee was to evaluate and score 13 projects that had investment briefs submitted by various HHS agencies and make recommendation to ITD for FY 2009 IT bond funding.

The 13 projects were scored in six categories:

- Aligns with EHS goals
- Supports mission critical functions
- Contributes to overall EOHHS service oriented IT architecture
- Improves client experience and care.
- Increases efficiency/productivity
- Meets ITD technical and business principles

The Department of Youth Services' JJEMS project scored high in all categories, and placed fifth overall in order of priority. The steering committee also made note of the fact that DYS was poised to start its project immediately upon funding approval.

This new system will correct the application deficiencies reported in Item 1 Youth Services Information System of the Auditor's report of October 2008, by providing the following high level functional features:

- A web-based intake mechanism for new DYS committed and detained youths;
- An automated case management tool for DYS committed and detained youths that provides real time, integrated and readily accessible information;
- Tracking and historical transactions for DYS committed youths and detainees
- A systematic approach to applying available DYS services (education, medical, behavioral health, substance abuse, etc.) for a youth as needed;
- Approval workflow for managing the progress of committed youth through the Department's Continuum of Care (CoC);
- Service Oriented Architecture (SOA) in EOHHS Enterprise Service Bus (ESB) messaging infrastructure to support common intake data interchange with existing EOHHS Legacy Systems;
- Leverage the technologies and benefits of the Virtual Gateway;
- Integration with the EOHHS electronic document management system (EDM);
- Access Identity Management System (AIMS) for single sign-on that is linked to EOHHS security policies;
- A mechanism for DYS detention and program facilities to manage their daily utilization reporting obligations;
- A secure system to maintain sensitive client information including HIPAA protected information; and
- A mechanism to provide pre-defined, on demand reports.

Impact of Missed Opportunity

DYS does not have access to client information where and when it is needed. Crucial client data is scarce and data to manage and improve agency operations is limited and very difficult to generate.

In addition to the data problem, there is a process problem. DYS managers have worked hard to standardize operations and to deploy and enforce Department policies and procedures. However, without

a system to sustain these standard processes and to hold people accountable for following them, there is no mechanism to ensure compliance. Finally, YSIS inadequacies are causing a productivity problem. DYS and vendor staff are faxing, calling and mailing in order to get and give client information. Before decisions can be made, data from disparate sources - paper forms, spreadsheet reports, YSIS and YSIS reports - must be integrated and analyzed. Obviously, this time would be better spent working with clients.

Item 2 User Account Management and Password Administration

Auditors Recommendation:

We recommend that DYS perform an immediate review of the status of all active users to the network and application system and deactivate access privileges for those individuals who no longer require access.

We recommend that DYS management develop written policies and procedures requiring timely notification to the Systems Unit's security administrator of any changes in employment status that could warrant change or deactivation of access privileges to the department's network or application systems.

We also recommend that the department implement preventive and detective control mechanisms, such as vigilant monitoring of access accounts to ensure that only authorized individuals have appropriate levels of access to IT resources.

DYS Response

The DYS network administrator has conducted a review of all users of the network and deactivated access for those individuals who no longer work for the agency. DYS management will develop a written policy requiring notification to the network administrator of a change in an employee's status that would require deactivation.

Until the policy is developed, the DYS Human Resource Unit will send the network administrator an email when an employee has left DYS active employment. A confirming email will be sent to HR after the user has been deactivated.

YSIS does not have the functionality to allow users to change their own password. The network administrator will validate all YSIS user profiles, change the password and send an email notification to the users the password has been changed. This process will have to be executed every six months until YSIS is replaced.

The new JJEMS system will use the Access Identity Management System (AIMS) for a single sign-on that is linked to the EOHHS security policies.

Further, the DYS CIO is developing an IT survey to establish a baseline of several facets of the system which affect how data is stored, accessed, used in order to more precisely study data security.

Response to Item 3 Noncompliance with Chapter 647 Requirements**Auditors Recommendation**

DYS senior management should familiarize themselves with all Chapter 647 internal control requirements. DHS should then implement and maintain policies and procedures that will ensure compliance with Chapter 647 of the Acts of 1989 and report all instances of unaccounted for variances, losses, and thefts of funds or property to the Office of the State Auditor.

DYS Response

DYS management is now familiar with chapter 647 and will have procedures put in place to ensure all unaccounted for variances, losses and thefts of funds or property are reported to the Office of the State Auditor and others as required by the law. The DHS Legal Unit will issue an advisory and a policy to inform all DHS staff of our reporting responsibilities under Chapter 647 and will coordinate these efforts with the EOHHS Compliance Office.

Item 4 Inventory Control Over Computer Equipment**Auditors Recommendation**

To ensure that the inventory of IT resources is adequately maintained, we recommend that the department strengthen current practices to ensure compliance with policies and procedures documented in the Office of the State Comptroller's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment. The Department should implement these control procedures to help ensure that all IT related equipment is recorded on the inventory record in a complete, timely, and accurate manner so that the Department can maintain a comprehensive record of all IT related equipment on a perpetual basis. The Department's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

We recommend the Department perform an annual physical inventory and reconciliation of its IT resources to ensure that a relevant and reliable inventory record of IT resources is in place. We recommend that the inventory system of record be periodically verified through reconciliation to physical hardware, acquisition, and disposal records. The reconciliation and improved documentation will help ensure the integrity of the Department's perpetual inventory system of record for its related assets, provide reasonable assurance that the inventory records can be used to support IT configuration management, and help safeguard computer equipment. We further recommend that the Department's inventory system of record be expanded to include data fields containing information relative to cost, condition, acquisition and installation dates, and status of the IT resource.

DYS Response

The Dept of Youth Services has been working with EOHHS Secretariat to bring all DHS locations together to be directly supported by the EOHHS IT Operations Services Group. An agreement was reached in September of 2008, with implementation planned for November, 2008. DHS will transfer the six employees currently supporting DHS IT operations into the EOHHS Operations Services Group and become one of six HHS agencies supported by this consolidated effort. The combined resources in this

unit will improve IT services to DYS by utilizing a larger pool of support personnel, assigning a site manager to each location and using EOHHS procedures, standards, tools and techniques.

In the area of inventory control the following service will be provided by EOHHS Operations Services.

7. Assures that an actual annual physical inventory is conducted.
8. Establishes IT asset recording input and control guidelines for IT Site Manager
9. Determines allocation and configuration of hardware and software.
10. Assures that all hardware and software is entered into inventory database upon receipt.
11. Determines and maintains IT asset warranties and maintenance contracts.
12. Serves as liaison with external organizations for IT asset reporting purposes(e.g. facilities, budget, A&F, procurement)

The inventory management database used by EOHHS "ARGIS" does capture cost, condition, acquisition, and install dates of equipment.

Improving Computer facilities at remote sites

The EOHHS network upgrade for the VOIP (voice over internet protocol) project requires all computer server and switching equipment locations to be brought up to standards required by Verizon. Environmental issues that were identified in the audit report will be corrected as part of the VOIP installation over the next 12 months.

Item 5 Business Continuity Planning and Off Site Storage

Auditors Recommendation

We recommend that DYS management work to develop, implement and test a disaster recovery and comprehensive business continuity strategy for its application system, databases and network capabilities critical to the Department's operation. We recommend that DYS formally assess the impact of the loss of IT operations and determine the extent to which contingency plans can be developed to address recovery of critical business operations. We further recommend that the DYS develop user area plans appropriate to the Departments IT processing environment and information accessibility requirements.

Once a formal plan has been adopted, we recommend that DYS test the plan to assess its viability and establish a process for routinely updating the plan based on changes to recovery efforts, technology, business processes, or staffing. DYS should ensure that all personnel responsible for business continuity task and activities be clearly identified and adequately trained.

Regarding the off-site storage of weekly backup-up copies of computer media, we recommend that DYS management find a secure and easily accessible off-site location and prohibit storing back-up media at employee's personal residences.

DYS Response

The YSIS production server is located at MITC. DYS has two backup servers for YSIS that are updated every night at midnight; one at 27 Wormwood Street, Boston, and one in the DYS Springfield office. In the event the YSIS production server is down, the end users have instructions to connect to the backup server in Boston. If the Boston server is down, they are instructed to connect to Springfield. This will give users access to data from the previous midnight.

Part of the agreement with EOHHS Operations Services Group is that they will develop, advance and execute an agency-wide information technology continuity & disaster recovery planning effort. (See item # 4 above.)

DYS intends to execute a contract for an off-site media storage program with Iron Mountain Storage Services. They will provide weekly pickup & storage of backup media. This will be in place in October 2008.