A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

NO. 2004-1241-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS
AT THE SUFFOLK COUNTY JUVENILE COURT

July 1, 2001 through May 28, 2004

OFFICIAL AUDIT REPORT
DECEMBER 27, 2004

TABLE OF CONTENTS

INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	3
AUDIT CONCLUSION	6
AUDIT RESULTS	8
1. Physical Security	8
2. System Access Security	9
3. Business Continuity and Contingency Planning	12

INTRODUCTION

The Suffolk County Juvenile Court (SCJC) is organized under Chapter 119, Section 1 of the Massachusetts General Laws. The Court is located in the Edward W. Brooke Courthouse, 24 New Chardon Street, Boston, Massachusetts. The Court holds sessions at satellite locations in Boston, Dorchester, West Roxbury, and Chelsea. The Court's jurisdiction includes the cities of Boston, Chelsea, and Revere, and the town of Winthrop. The Court's organization and management structure consists of a First Justice, six Associate Justices, a Clerk Magistrate, an acting Chief Probation Officer, and is staffed by 94 employees. The Juvenile Court, which handles criminal and civil matters concerning defendants 17 years old and younger, has general jurisdiction over cases involving delinquency, children in need of services, care and protection petitions, adults contributing to the delinquency of minors, adoption, guardianship, termination of parental rights proceedings, and youthful offender cases.

From an information technology (IT) perspective, the Administrative Office of the Trial Court (AOTC) supports the mission and business objectives of the juvenile courts by administering the IT infrastructure, including mission-critical application systems installed on the file servers and mainframes located at the AOTC's Information Technology Department in Cambridge. In addition, the AOTC provides IT services and technical support to individual courts and maintains master inventory records for the courts under its jurisdiction.

At the time of our audit, the SCJC's computer operations were supported by 141 microcomputer workstations of which 88 were in the Probation Department, 43 in the Clerk's Office, six in the courtrooms, and four in the Judges' Lobby. Of the 141 microcomputer workstations, 129 were located at the New Chardon Street location and 12 workstations were located in the satellite offices. The workstations, with the exception of the Boston location, were connected by a router and two switches from the AOTC's wide area network (WAN) to the IBM Netfinity fileserver, located at the AOTC data center in Cambridge. The Boston location uses a line-of-site laser, located on the roof of the Brooke Courthouse that transmits a signal to the AOTC data center in Cambridge allowing the connectivity to the AOTC's WAN. Both the Clerk Magistrate's Office and the Probation Department use the Juvenile Court Records and Information System (JURIS). The system tracks juvenile subjects from the time a complaint or petition is filed against or on behalf of the individual through probation of the individual; maintains all pertinent docket and probation information; and updates information as it is entered. The Clerk Magistrate's Office also uses the Warrant Management System (WMS) to track

warrants issued for all courts under the jurisdiction of the AOTC. The Probation Department also uses the Criminal Activity Record Information System (CARI) to access information on all dispositions from courts regarding criminal offenses and restraining orders.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an audit of selected information technology (IT) general controls at the Suffolk County Juvenile Court from April 15, 2004 through June 15, 2004. The audit covered the period of July 1, 2001 through May 28, 2004. The scope of our audit included an evaluation of IT-related controls pertaining to IT physical security, environmental protection, system access security, inventory control over IT-related assets, business continuity and contingency planning, and on-site and off-site storage of backup copies of computer-related media.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for the IT processing environment. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent and detect unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access to automated systems available through the Court's workstations. Further, we sought to determine whether the SCJC, in conjunction with the AOTC, was exercising adequate password administrative controls for access to automated systems.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Court's IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. In addition, we determined whether the Court, in conjunction with AOTC, had a business continuity strategy, including user area plans, to assist the Court in regaining business operations supported by technology within an acceptable period should a disaster render computerized functions inoperable or inaccessible. In conjunction with reviewing business continuity planning, we sought to determine whether adequate on site and off-site storage of back up media was in effect to assist recovery efforts.

Audit Methodology

To determine whether adequate physical security was in place and in effect within the Court to prevent damage to or loss of IT-related equipment, we inspected the telecommunication and server room and areas where IT resources and workstations were located. We also conducted walkthroughs, observed security devices, and inspected the security office where closed circuit

television cameras were located. We interviewed the Director of Security at AOTC, who has the oversight responsibility of providing physical security for the SCJC. We determined whether procedures were in place to provide reasonable assurance that the Director of Security at AOTC would be notified in a timely manner of changes in personnel status (e.g., employment terminations, job transfers, or leaves of absence) that would impact electronic keycard privileges and possibly require deactivation of card privileges in the automated security system. In order to evaluate controls for gaining access to the Court, we requested a list of electronic keycard holders to the Court to verify whether those individuals were current employees.

To assess the adequacy of environmental controls, we examined the areas housing IT equipment at the Court to determine whether IT resources were subject to adequate environmental protection. We interviewed the Director of Facilities Management, and observed and evaluated the adequacy of certain environmental protection controls. Environmental protection controls reviewed included the presence of water and smoke detectors, fire detection and suppression measures, an uninterruptible power supply, and general housekeeping for all areas housing IT resources. We also reviewed the fire command center and fuel storage area for the back up generator. We confirmed the existence and functionality of the main and local controls of the heating, ventilation, and air conditioning system (HVAC) and observed the water shut-off valves for the alarm and sprinklers.

Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the application systems accessed through the microcomputer workstations located at the Court. Since the Court does not administer activation and deactivation of user accounts, we relied upon audit work performed for audit number 2002-1106-4T of AOTC's procedures for performing these functions. To determine whether only authorized employees were accessing the automated systems (JURIS, CARI, WMS, E-MAIL), we obtained a list of system users from AOTC and the Office of the Commissioner of Probation for individuals granted access privileges to the automated systems used by the Court and compared the lists to the Court's current payroll listing of employees. We reviewed control practices regarding logon ID and password administration and evaluated the extent of documented policies and guidance provided to the SCJC personnel. We determined whether all SCJC employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed and determined whether SCJC had complied with the Administrative Office of the Trial Court's "Internal Control Guidelines" regarding inventory control and whether generally

accepted inventory controls were in place. To assess compliance with AOTC's guidelines, we obtained a listing of IT- related assets from AOTC and compared it to SCJC's own listing for accuracy and completeness. We conducted inventory tests by validating equipment-specific information through examination of IT resources on hand to the inventory list and vice versa.

To assess the adequacy of business continuity planning, we evaluated the extent to which the Court had identified their business continuity requirements and had user area plans that could be activated in conjunction with AOTC's business continuity and disaster recovery plans to resume operations should the JURIS, WMS, and CARI systems be inoperable or inaccessible for an extended period. With respect to business continuity and disaster recovery planning, we interviewed management from the Court to determine whether the criticality of application systems had been assessed; risks and exposures to computer operations had been evaluated, and a written, tested business continuity and disaster recovery plan was in place and in effect. In addition, to evaluate the adequacy of controls that protect data files through the generation of on-site and off-site storage of backup copies of magnetic media and hardcopy files, we also examined the on-site daily backup copies of JURIS to determine the provisions for storage, frequency of backup, and adequacy of controls in place to protect the backup media. Furthermore, we interviewed Court personnel to determine whether they had been trained in the procedures of generating backup copies and were aware of on-site and off-site storage procedures and steps required to safeguard the backup media.

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 policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000. CobiT control objectives and management control practices were developed as a generally applicable and accepted standard for sound information technology security and control practices.

AUDIT CONCLUSION

Our audit disclosed that although the Court, in conjunction with AOTC, had internal controls in place for environmental protection and inventory control over IT-related assets, certain controls pertaining to physical security, system access security, and business continuity planning needed to be strengthened.

Our review revealed that there were adequate environmental protection controls in place and operating within areas of the Court housing IT resources with respect to general housekeeping; heating, ventilation, and air conditioning; emergency lighting; smoke, heat and water detectors; fire suppression system; and a fire alarm system connected to the local fire department. Our audit found that adequate inventory controls were in place to provide reasonable assurance that IT-related assets were properly identified, recorded, accounted for, and safeguarded from loss and theft.

With respect to physical security, our audit revealed that there were certain controls in place, such as visitors must pass through a metal detector and a hand-held magnetometer inspection when entering the Court. All packages must pass through an X-ray machine and all activities are under closed circuit surveillance. We found that areas housing computer equipment were inaccessible by the general public and were staffed by court employees. However, we determined that the Court, in conjunction with AOTC, needed to document policies and procedures related to physical security controls and to implement controls over the maintenance of electronic keycards. We found employees no longer employed by the Court who still had active keycard access.

Regarding system access, our audit disclosed that the Court, in conjunction with AOTC, had not established adequate system access security controls over its IT systems to prevent or detect unauthorized access or use. Appropriate policies and procedures were not in place to provide a control foundation for access security. We found that controls needed to be strengthened to ensure that user IDs and passwords would be active for only authorized personnel and that appropriate password standards would be followed. Security access privileges should be deactivated in a timely manner for users no longer needing authorized access to automated systems or on-line data.

At the time of our audit, the Court did not have business continuity or user plans to address the loss of automated processing should IT systems be inoperable. We found that the Court, in conjunction with the AOTC, had not performed a criticality assessment of application systems

and their associated risks. The Court was also unaware of any business continuity plans or strategies to be exercised by AOTC. The Court needs to address the business risks of not being able to rely upon the continued availability of AOTC-based systems or the loss of critical IT resources at the Court, and to develop, in conjunction with AOTC, appropriate continuity or contingency plans.

AUDIT RESULTS

1. Physical Security

Although at the time of our audit, the SCJC had certain physical security controls in place, physical security needed to be strengthened with respect to documented policies and procedures and electronic keycard management. Regarding controls in place, we found that all employees and visitors were required to enter the courthouse through either of the two main entrances, which are staffed by security personnel, and pass a metal detector and a hand held magnetometer inspection. Also, all packages are required to pass through an x-ray machine. There are 130 closed circuit television cameras that monitor activities through the interior and exterior of the courthouse. Security monitors located in an office security room are monitored 24/7 and record activities on VCR tapes. There are patrols within the building by Court personnel for all public areas on a 24/7 basis.

Our audit found, however, that Court management had not documented physical security policies and procedures. In addition, although keycards were issued to authorized Court personnel, we found that keycards for prior employees had not been deactivated to prevent unauthorized physical access.

We obtained a system generated list of active keycard holders from the AOTC system of record and compared it to a current payroll listing. Our review of the electronic keycard listings revealed that of the 67 active SCJC keycard holders, access security cards had not been deactivated from the keycard system for 13 individuals (19%) no longer employed by the Court. We found that the failure to deactivate the access security cards went as far back as July 31, 2001. After our concern regarding keycard management was brought to the auditee's and AOTC's attention during the audit, corrective action was initiated. Our subsequent review of the modified electronic keycard listing indicated that only current Court employees had active access security cards.

Generally accepted computer industry practices indicate that appropriate physical security controls need to be in place to ensure that information technology assets are operating in a safe and secure operating environment and that IT-related resources are protected from unauthorized access, use, damage, or theft. The Court needs to ensure that there is timely deactivation of access security privileges when authorized access is no longer required. Timely notification is required of individuals no longer authorized to gain physical access to secure areas. By more closely administering the validity of keycard access, the Court will strengthen its authentication controls in this area.

Recommendation:

We recommend that the Court, in conjunction with AOTC, establish documented administrative procedures for managing the keycard access system. The procedures should include requirements that prompt notification be made from the human resources department to the director of security at AOTC as well as the chief court officer at SCJC of all required changes in employee security access, including transfers of staff to other court facilities and terminations of employment, as well as prompt notification of lost or stolen keycards to enable timely deactivation of the access cards. The procedures should also require periodic reconciliation of the active access cards to current employees to identify the cards requiring deactivation.

Auditee's Response:

> *It has come to our attention that the AOTC has an exit form entitled Employee Checkout List, which is required to be filled out when a employee leaves the employ of any office within The Trial Court. The Clerk's Office, Probation Department and Judges' Lobby now have this form in our possession and it has been used as recently as last week when an employee of the Clerk's Office left to take on a new position in the Middlesex Juvenile Court. This completed exit form will be sent promptly to the Human Resource Department of the Trial Court and also to the Director of Security. There is a place on this form that addresses the I.D. Badge issue and a comment field to add any further information about employee security access, deactivation, or any changes in employee security access.*
>
> *The Suffolk County Juvenile Court will begin discussions with* [the] *Acting Director of Security about how best to begin a procedure to periodically reconcile active access cards to current employees to identify those cards requiring deactivation.*

Auditor's Reply:

We agree that the use of the Employee Checkout List should tighten physical security administration at the Court. Periodic reconciliation of this form with the keycard system and the payroll records should help ensure that only authorized individuals have active keycards.

2. System Access Security

Our audit disclosed that only authorized users had access to the JURIS and CARI systems, however, access privileges to WMS and E-Mail were not being deactivated for SCJC personnel in a timely manner. We also found that although adequate procedures were being followed in conjunction with AOTC to authorize and activate user privileges to the automated systems used by the Court, only limited documented policies and procedures existed at the Court regarding

access security controls and that administrative control procedures for user account deactivation needed to be strengthened.

Although control practices regarding authorization and activation of access privileges were in place, procedures for changing or deactivating user privileges needed to be improved. At the time of the audit, we found there was no formal process, or standard electronic form, for notifying the AOTC of changes in employment status that would require user account access privileges to be changed or deactivated. We found that access privileges to WMS and E-Mail were not being deactivated in a timely manner when a Court employee was transferred or terminated employment from the SCJC. Our tests revealed that access privileges had not been deactivated for eight out of 23 WMS users (35%) and three out of 22 E-Mail users (14%) from the Court who were no longer employees of the Court.

We determined that because neither the Court nor AOTC had established a mandatory time frame for changing passwords, passwords had not been changed on a regular or frequent basis for the AOTC-supported applications. We found that passwords had not been changed, in some cases, for periods ranging from three to seven years for application systems available through the Court's microcomputer workstations. Furthermore, system access security functions were not being used to prompt users to change their passwords for access to the desktop operating system and the JURIS and WMS applications. In addition, there was no minimum length of characters for passwords. We found that password composition, length, and frequency of change needed to be reevaluated, formally documented, and communicated to all users. Generally accepted access security procedures and password syntax rules require that passwords be comprised of at least eight alpha/numeric characters, not be easy to guess, be of sufficient length, and be changed periodically. In addition, authorization and authentication mechanisms should be reviewed and maintained to support security administration.

Access to computer systems, program applications, and data files should be authorized on a need-to-know, need-to-perform, and need-to-protect basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the Court's and AOTC's security administrators of any changes in user status that would impact the individual's level of authorization. Appropriate notification procedures should be in place to ensure that access privileges are modified in a timely manner when changes occur in job responsibilities or employment status.

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." In addition, computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for security administration and proper protection of information assets. The policies and procedures should address authorization for system users, activating and deactivating 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. Lastly, appropriate monitoring and evaluation mechanisms need to be in place to provide assurance that security policies and procedures are in effect to ensure that only authorized users have access to automated systems and on-line data files.

The failure to fully document and implement appropriate system access security policies and procedures places critical systems and data files at risk to unauthorized access, modification, or loss. Given the nature of the Court's activities and operations, and the sensitivity of information captured, stored and processed by the computer systems, access security to IT resources and systems is a critical IT-related function. As such, the viability of authorization and authentication mechanisms is extremely important to ensuring that only appropriate access is provided. In addition, access security and user account activity should be reviewed on a relatively frequent basis.

Recommendation:

To improve system access security controls at the Court, we recommend that the Court, in conjunction with AOTC, implement formal written access security procedures, including a standard electronic form to be completed by AOTC's Human Resources Department or the Court to promptly notify appropriate IT Department personnel at AOTC responsible for security administration. The form would identify changes in employee status that would necessitate change or deactivation of the user's access privileges. Such changes in employee status would include job responsibilities, departmental transfers, leave of absences or employment termination. Also, we recommend that management establish appropriate documentation regarding password configuration and timely changing of passwords.

Auditee's Response:

> *The Suffolk County Juvenile Court will begin discussions with* [the] *Chief Information Officer for the Trial Court, about drafting a standard electronic form, to be used throughout the Trial Court, which would allow the court to promptly notify the appropriate IT personnel about a change in employee*

> *access privileges. Our suggestion would be to incorporate these questions onto the exit form already being used by the Trial Court, a third copy of which would be sent to the IT Department. In the meantime, the Suffolk County Juvenile Court has begun discussions with . . . the juvenile court IT liaison, and she has run for us a list of personnel who currently have authorized access to the Warrant Management System (WMS), the Juvenile Records and Information System (JURIS) and the Comprehensive Electronic Office (CEO), in all five of our court locations so that we can make immediate changes in employee access.*
>
> *Our discussion with* [the Chief Information Officer] *will also include a recommendation that the AOTC establish appropriate documentation regarding password configuration and timely changing of passwords for all applications.*

Auditor's Reply:

Working with AOTC on access security standards for application systems should help to ensure that only authorized individuals have access to programs and data. It is important that the notification of change in employee status, such as changes in job responsibilities or leaves of absence, is completed and submitted in a timely manner to the security administrator. Standards for password administration and individual password capabilities should be tied to user profiles for all application systems, which would strengthen the framework for logical access security.

3. Business Continuity and Contingency Planning

Our audit revealed that the Court, in conjunction with the AOTC, had not collaborated to develop a formal business continuity strategy, including user area plans, that would provide reasonable assurance that critical business operations could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. Furthermore, the Court had not assessed the relative criticality of the automated systems supporting Court operations and identified the extent of potential risks and exposures to business operations. Although backup copies are generated by AOTC of computer-related media for the business functions processed through AOTC's file servers, our audit revealed that the Court, in conjunction with AOTC, had not developed contingency plans for user areas to address an extended loss of automated processing or access to online information. Without ensuring adequate disaster recovery and contingency plans, including required user area plans, the Court was at risk of not being able to perform certain functions should the automated systems be disrupted or lost. A loss of processing capabilities could result in significant delays in processing caseloads.

Without comprehensive, formal, and tested user area and contingency strategies, the Court's ability to access information related to the WMS and CARI operating on the AOTC's file servers, and the JURIS information operation on SCJC's file server, could be impeded. Without access to these application systems, the Court could be hindered from obtaining information regarding outstanding warrant information, or unable to confirm that fines, fees, and penalties were being collected by the Clerk's Office. Furthermore, the Court would be unable to access all online court dispositions regarding juvenile cases.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring operations either at the original site or at an alternate-processing site, and include appropriate user area plans outlining recovery or contingency steps. The user area plans should be coordinated with overall enterprise-based business continuity plans.

The success of the business continuity planning process requires management commitment and system user involvement to help ensure there is a clear understanding of IT processing requirements, that appropriate IT and user area plans are developed based on the relative criticality and importance of systems, and that adequate resources are available.

Generally accepted practices and industry standards for computer operations support the need for each entity 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. Therefore, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and should develop its recovery plans based on the critical aspects of its information systems.

Recommendation:

We recommend that the Court, in conjunction with the AOTC, perform a risk analysis of the IT systems and identify the impact of lost or reduced processing capabilities. The Court should assess the relative criticality of their automated processing and develop and test, in conjunction with AOTC, appropriate user area plans to address business continuity. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to Court operations or the IT environment. To support business continuity, the Court's user area plan should document the Court's recovery and contingency strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations to the extent

necessary within the needed time frames. We recommend that business continuity and user area plans be tested, and periodically reviewed and updated, as needed, to ensure their viability. The completed plans should be distributed to all appropriate staff members who should be trained in the execution of the plan under emergency conditions.

Auditee's Response:

> *The Suffolk County Juvenile Court has begun discussions with the Administrative Office of the Juvenile Court as well as with our IT liaison about developing a written, formal disaster recovery plan. There has always been an informal plan in our court whereby in the event that the computer was destroyed, our system tapes and data, which are kept off site, would be able to be loaded in several other of our juvenile courts' main frames, including but not limited to Cambridge, Lawrence, Worcester, etc. This would enable us to be up and running in a very short period of time, however, we recognize the need to establish a formal, written recovery plan that would document the Court's recovery and contingency strategies with respect to various disaster scenarios, the contents of which would be distributed to all appropriate staff members who would be trained in the execution of the plan under emergency conditions. As I have stated, these discussions have begun and will be carried out and implemented as quickly as possible.*

Auditor's Reply:

Documenting business continuity and contingency plans will accelerate recovery and diminish the time needed to recover mission-critical and important processing and network capabilities. The use of another court's computer system to restore and run the Court's systems may work, however, other factors, such as staff logistics, security, data entry and generation of backup copies, may be revealed. In addition to having a documented business continuity plan, recovery strategies should be formally reviewed and periodically tested to ensure their viability. The plan developed should address various disaster scenarios and clearly identify cooperative efforts necessary to assist in recovery efforts.