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. 2007-0145-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY CONTROLS AT THE DEPARTMENT OF CORRECTION

March 15, 2005 through December 6, 2007

OFFICIAL AUDIT REPORT
MARCH 12, 2008

TABLE OF CONTENTS

INTRODUCTION **1**

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY **3**

AUDIT CONCLUSION **6**

AUDIT RESULTS **8**

1. System Access Security **8**
2. Oversight of Records Management **10**

APPENDIX

Status of Prior Audit Results **13**

INTRODUCTION

The Massachusetts Department of Correction (DOC) was established under the provisions of Chapter 124, Section 1 of the Massachusetts General Laws (MGL). The Executive Office of Public Safety provides administrative oversight as well as strategic and tactical planning for DOC operations. The Department's primary mission is to promote public safety by imprisoning convicted felons while providing them with opportunities for rehabilitation and reintegration into society. The DOC is comprised of 18 institutions and a central office that provides administrative services to support the mission of the Department. The DOC employs approximately 5,000 people who work in conjunction with the Judiciary and law enforcement communities to incarcerate nearly 11,000 inmates within the Commonwealth. The DOC contracts with the University of Massachusetts Health Care to provide comprehensive medical services to all inmates. The Department received an appropriation of $453.5 million in state funds for fiscal year 2006 and an appropriation of $461.8 million in state funds for fiscal year 2007.

The Technology Services Division (TSD) is responsible for managing all computer operations for the DOC. At the time of our audit, overall staffing at the TSD consisted of 41 employees, of whom 30 were located in the central office and 11 field technical employees were located at various institutions. The TSD manages the DOC's file servers, routers, and switches that are located in various facilities to support local-area and wide-area network access within the DOC to the Inmate Management System (IMS) application and database, and Intranet applications. The DOC's main servers for the IMS, Web, Email, and Citrix systems are all located in the TSD's file server room located in Milford, Massachusetts. The TSD also supports approximately 3,000 microcomputer workstations located throughout the 18 institutions and the central office and has a field staff to provide technical services to the various institutions as well as a Help Desk function.

The TSD provides users with network communications, including access to the Internet and the DOC's Intranet, access to the Massachusetts Management Accounting and Reporting System, Human Resources/Compensation Management System, and the Criminal Justice Information System. The TSD also manages data file exchanges with various agencies, including the Criminal History Systems Board, Sex Offender Registry Board, Department of Revenue, Department of Mental Health, and the Federal Bureau of Investigation.

The DOC's main application system is a customized product called the Inmate Management System that was developed by Deloitte Consulting. The IMS application serves as the primary application system throughout the DOC. The IMS application consists of over 250 different modules. The primary

modules include inmate tracking, admissions and discharges, booking information, classification, sex offender history, medical information, and inmate scheduling.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed a follow-up audit of certain information technology (IT) general controls. Our audit, which was conducted from April 30, 2007 through December 6, 2007, covered the period of March 15, 2005 through December 6, 2007. The scope of the audit consisted of an evaluation of the status of a prior audit result in our audit report (No. 2004-0145-4T), issued March 14, 2005, regarding system access security. Our audit also included a review of controls related to IT organizational structure and a limited review of controls over data integrity for selected modules in the Inmate Management System (IMS).

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken with respect to our prior audit result and to review selected IT general controls. Our objective regarding system access security for user account management was to determine whether adequate controls were in place and in effect for the activation, maintenance, and deactivation of access privileges to ensure that only authorized personnel had access to the IMS. Furthermore, we sought to determine whether Technology Services Division (TSD) security staff were actively monitoring the management of user accounts. We also sought to determine whether the control environment, including policies, procedures, and the organizational management structure, provided reasonable assurance that IT-related control objectives would be achieved. A further objective was to assess the level of integrity of selected data contained in the IMS.

Audit Methodology

To evaluate whether corrective action was taken on our recommendations presented in our audit report No. 2004-0145-4T, we performed pre-audit work that included a review of prior audit work papers and gaining an understanding of DOC's current IT environment. We reviewed our prior recommendations regarding system access security and evaluated the appropriateness of current access security policies and procedures.

During our examination of access security controls, we reviewed policies and procedures to authorize, activate, and deactivate access privileges to the IMS application. The system, which resides on DOC's file servers, is accessed through microcomputer workstations located at the DOC's administrative offices and individual institutions. We reviewed control policies regarding login ID and password administration and password composition by evaluating the appropriateness of documented policies and

guidance provided to the DOC personnel, and by interviewing the DOC's security officer and IT management. In addition, we reviewed control practices used to assign DOC, contract employee, and outside agency staff access to the application programs and data files. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. 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.

In order to verify that all users of the IMS application system were current DOC employees, University of Massachusetts Health Care employees contracted with DOC, or outside agency employees, we obtained the IMS user account list containing 4,960 user accounts as of June 13, 2007. We compared the system-generated user account list to a DOC payroll list and a list of University of Massachusetts Health Care employees contracted to the DOC. We developed an exception list of those individuals no longer requiring access privileges to the IMS application. The full exception list was reviewed with DOC security personnel and we observed DOC deactivating user privileges of individuals no longer requiring access to the IMS application system. Our audit did not include an examination of controls over network security.

Regarding our review of IT-related organization and management, we interviewed senior management and obtained, reviewed, and analyzed existing IT-related policies, standards, and procedures related to topics covered in our follow-up review. We also reviewed the TSD organizational structure in relation to staffing levels.

Our tests of data integrity over the Inmate Management System (IMS) included a review of policies and procedures over data preparation, maintenance, and required internal reviews. To gain an understanding of the booking and admission module of the IMS system, we attended training sessions provided by DOC employees. To determine whether DOC had adequate controls over data entry for the initial booking module within IMS, we selected data elements related to initial booking and admissions, sentencing statutes, date of offense, docket number, jail credits, release dates, parole hearing, and earned time credits for good behavior. We also reviewed information pertaining to periodic reviews of the inmate's individual sentencing folder. We conducted a data integrity test using ACL audit software to select a random sample of 73 out of a population of 10,827 inmates located in 18 correctional institutions throughout the Commonwealth. We tested the sample inmate records to determine whether the statutory offenses, the length of sentences imposed by the Trial Court, and initial credits for time served awaiting trial were documented on the Mittimus. By definition, a Mittimus is a precept in writing, under the hand

-

and seal of a justice of the peace or other competent officer, directed to the jailer or keeper of a prison, commanding him to receive and safely keep a person charged with an offense therein named until he shall be delivered by due course of law. Source documents provided by the Trial Court were accurately and completely recorded in the IMS application. Our audit did not include a comprehensive review of all data elements available in the IMS application, but was limited to a review of selected data elements contained in the booking and admissions module. During our review we did not evaluate the validity of data computations and sentencing terms within the IMS application.

Our audit criteria consisted of relevant DOC policies and procedures and was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. Our audit criteria also included IT management control practices as outlined in the Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology" (CobiT).

AUDIT CONCLUSION

Based on our audit at the Department of Correction (DOC), we determined that internal controls in place provided reasonable assurance that adequate IT-related guidance for access security, data integrity, and staffing requirements was being provided by DOC. However, control practices for system access security and the monitoring and quality assurance review mechanisms of inmate data needed to be strengthened to ensure that all inmate data is accurate, complete, valid, and current.

Regarding our review of topics related to IT organizational structure and staffing requirements contained in our prior report (No. 2004-0145-4T, issued March 14, 2005), we found that management had performed a formal assessment of technical field staffing requirements needed to adequately maintain IT support services. In addition, the DOC had implemented further corrective action by increasing the IT technical staffing levels at individual correctional facilities. Our prior IT audit report had indicated that individual institutions had inadequate technical staffing levels to adequately maintain IT support services.

Our review of system access security controls for the Inmate Management System (IMS) that provides mission-critical information, such as inmate booking information, inmate tracking, and inmate classification, indicated that access security controls needed to be strengthened. Our review of the 4,960 user accounts revealed that 164 user accounts should have been deactivated and disabled. We found that, contrary to DOC's Standard Operating Procedure (SOP-002) regarding access security controls, the Technology Services Division (TSD) security administrator was neither being informed on a consistent basis of changes in user status (resignations, terminations, name changes) from contractors and outside agencies, nor was the TSD security administrator continuously monitoring user accounts. We found that 33 user accounts for former or current University of Massachusetts Health Care employees who were contracted to the DOC had active user IDs and passwords for which access privileges to the IMS system should have been terminated or modified to conform with the employee's current status and user requirements. Our audit disclosed that a user account for a former University of Massachusetts Health Care employee, who had been terminated in November 2006, had not been deactivated or disabled. We found that unauthorized access to the IMS system through the use of this user account continued through August 2007 even though the University of Massachusetts had immediately notified the DOC on the date of the employee's termination that the user account should be disabled. The user account was disabled by DOC in September 2007 upon notification by our office.

We also found that user account management needed to be strengthened for individuals who were not DOC or DOC-contracted employees. We found 131 active user accounts for individuals involved in public safety and law enforcement activities who no longer required access to DOC systems. These user accounts, which allowed read-only access to the Department's IMS application system, were

subsequently disabled by DOC when we brought the matter to their attention. Regarding password administration, we found that employees were required to change passwords on a pre-defined basis and that appropriate policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation and password length and composition were in place, and security requirements had been established.

Although our review of data integrity controls over the IMS indicated DOC had documented policies and procedures over data preparation, maintenance, and required internal reviews, adequate monitoring through periodic and routine quality assurance reviews needed to be consistently performed at all DOC institutions. Our data integrity test, which was based on a random sample of 73 inmate files from a population of 10,827 inmates who were located in 18 correctional institutions, demonstrated that DOC had adequate controls over data entry to the IMS for initial booking and admissions, sentencing statutes, date of offense, docket number, jail credits, release dates, parole hearing, and earned time credits for good behavior. However, our review of data integrity controls for the IMS application revealed that contrary to DOC policy, quarterly reviews of inmate data were not being performed at all institutions on a consistent basis. We found inconsistent monitoring as evidenced by five of the 18 DOC institutions that were not performing quarterly reviews of inmate data as required by DOC guidelines. The absence of scheduled and routine monitoring and evaluation of the inmate records increases the level of risk that data may not be accurate, valid, complete, and current. Subsequent to the end of our audit fieldwork, the DOC had developed plans to centralize the review functions.

AUDIT RESULTS

1. System Access Security

Our audit revealed that system access security controls for DOC's mission-critical application, the Inmate Management System (IMS), needed to be strengthened to ensure that only authorized users have access to the system. We found that policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation were in effect, and requirements for password composition and frequency of change were in place. Although there were written procedures in place requiring that DOC's contract vendors inform the Technology Services Division (TSD) when an employee or contractor terminates employment or services, our audit revealed instances when action had not been taken to remove expired, terminated, or suspended user accounts from IMS.

Our audit disclosed that a user account for a former University of Massachusetts Health Care employee, who had been terminated in November 2006, had not been deactivated or disabled. We found that unauthorized access to the IMS system through the use of this user account continued through August 2007, even though the University of Massachusetts had immediately notified the DOC on the date of the employee's termination that the user's account should be disabled. We immediately informed TSD management of this issue and the user account was promptly disabled. The activity on this user account had not been traced to specific users and the extent of compromised information had not been determined.

Our tests of system access security for the IMS application indicated that, contrary to sound access security practices and internal security policies, there were active user accounts that had not been deleted for individuals who were no longer affiliated with the DOC. Our review of the 4,960 user accounts indicated that 164 of these accounts should have been deactivated or disabled as a result of modifications to present job functions and responsibilities or continued employment. We also found that, contrary to DOC's Standard Operating Procedure (SOP-002) regarding access security controls, the TSD security administrator was not being informed on a consistent basis of changes in user status (resignations, terminations, name changes) from contractors and outside agencies and was not continuously monitoring user accounts.

Our tests of authorized user accounts indicated that all DOC employee user accounts were properly authorized and valid. However, we found that 33 user accounts for former or current University of Massachusetts Health Care employees who were contracted to the DOC had active user IDs and passwords with read and write privileges. These user accounts should have been disabled or modified as their current functions had been changed or terminated. We also found instances where the TSD had been notified of changes in the employment status of University of Massachusetts Health Care employees and DOC contract employees who had access to the IMS application, but TSD had failed to deactivate the user accounts. Further, at the time of our audit, we found 131 active user accounts for individuals involved in public safety

and law enforcement activities who no longer required access to DOC systems. These user accounts were subsequently disabled by DOC, once we brought the matter to the Department's attention.

Our audit revealed that the DOC had not consistently monitored compliance with the access security policy for deactivation or deletion of user accounts. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact the level of authorized access privileges. The failure to deactivate user accounts in a timely manner placed the DOC at risk of unauthorized access or use of established privileges, such as using another individual's user account to obtain higher access privileges. As a result, certain information residing on the DOC network, including the IMS, could have been vulnerable to unauthorized access and disclosure, resulting in a breech of confidentiality.

Standard Operating Procedure (SOP-002) regarding access security controls indicates "It is the responsibility of the agency to provide accurate and up-to-date records of employees who access IMS including requesting new accounts as well as the timely notification of terminated employees to the DOC Help Desk." The SOP requires external agencies to submit weekly reports of changes in employee status, including terminations. The procedure also requires DOC's help desk and security personnel to request the weekly reports if the reports are not submitted to DOC.

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 users. Additional controls from the CobiT control framework include establishing procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts; developing formal approval procedures outlining the data or system owner granting the access privileges; establishing a control process to review and confirm access rights periodically; and performing regularly scheduled comparisons of resources with recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

Recommendation:

We reiterate our prior recommendation that DOC perform a comprehensive review of the status of all active users of the IMS application and remove all access privileges for those individuals who no longer require access, or modify the access privileges to coincide with the employee's current work responsibilities. We urge DOC management to adhere to its established policies and procedures regarding written notification of changes in personnel status from contractors and outside parties to the Technology Services Division's security administrator to help ensure timely deactivation of access privileges. We recommend more vigilant monitoring for DOC and University of Massachusetts Health Care contract employees, as well as outside

public safety entities, to ensure that only appropriate access privileges are provided and that access is terminated in a timely manner for individuals no longer requiring or authorized to access to the IMS application.

Regarding the security breach of the contract employee's user account that was not terminated in a timely manner, DOC should perform a forensic examination to determine whether unauthorized actions had been initiated and to identify the potential impact of unauthorized access to confidential data.

Auditee's Response:

This is being addressed through current policies as well as revised procedures that address the identification and elimination of inactive user accounts. The IMS user profiles will continue to be reviewed for accurate user access privileges that coincide with employee's work responsibilities. The DOC is continuing to reinforce policies and procedures regarding written notification of changes in personnel status of contractors and outside parties to the Technology Services Security Administrator to help ensure timely deactivation of access privileges. The DOC is performing more vigilant monitoring of access accounts through weekly user account reports for identification of inactivity to ensure access privileges is terminated in a timely manner.

The DOC will perform a forensic examination of the user account that was not terminated in a timely manner to identify unauthorized access to confidential data.

Auditor's Reply

We believe system access security in DOC's IT environment is critical and commend the actions taken to improve controls in this area. We acknowledge DOC's efforts to enhance policies and procedures for access security based on our audit recommendations. We believe DOC 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 network application systems and data. We are pleased that the DOC will initiate a forensic examination for the unauthorized access of a user account of the former contract employee. We believe that once the results of the examination have been determined, the DOC should take immediate action to notify any applicable parties of an actual or potential breech of confidentiality.

2. Oversight of Records Management

Our audit revealed that several DOC institutions were not consistently performing periodic reviews of inmate records as required by Department policy. Our data integrity test, which was based on a random sample of 73 inmate files from a population of 10,827 inmates located in 18 correctional institutions, demonstrated that DOC had adequate controls over data entry for the initial booking and admissions within the IMS. This included data elements related to initial booking and admissions, sentencing statutes, date of offense, docket number, jail credits, release dates, parole hearing, and earned time credits for good behavior.

However, we found that five of the 18 DOC institutions were not performing quarterly, periodic, or annual reviews of inmate folders. The lack of consistent and routine monitoring of the inmate records may increase the level of risk that data contained in hardcopy and electronic media may not be complete, valid, and up to date. If the information contained in the IMS system is not complete, valid, and up to date, the potential exists that inmate sentences and release dates may not be accurately reflected in the system.

We determined that certain institutions were not in compliance with DOC policies regarding auditing and reviewing of IMS Inmate Case Folders. We found instances where policies and procedures regarding the review of inmate records were not communicated to relevant staff members at each institution. According to DOC management, certain institutions lacked adequate staff to fulfill the requirements mandated by the DOC to consistently monitor inmate records.

DOC's internal policy, 103 DOC 401 Booking and Admissions Policy, mandates that: *The following procedures must be adhered to concerning the booking and admissions process for all facilities. Audit procedures to ensure that the IMS and its utilization are reviewed on a quarterly basis. The deputy superintendent of operations shall be responsible to ensure that the audit is conducted, shall review the results, take corrective action, and include the audit information in his/her quarterly report. Audits shall include, but not be limited to the following: Review of five percent of the inmate population to verify that the IMS information required in the 103 DOC 401 – Booking and Admissions policy is complete and accurate (different inmates should be audited each quarter).*

The absence of continual monitoring and evaluation of the inmate records increases the level of risk that errors in inmate records may go undetected and may ultimately compromise data integrity. Subsequent to the end of our audit fieldwork, the DOC had developed plans to centralize these review functions.

Recommendation:

We recommend that DOC management communicate the requirements mandated in DOC policy 103 DOC 401 requiring the quarterly review of IMS information at each institution. We urge that management, in conjunction with the DOC internal audit group, ensure that the Deputy Superintendent at each institution continuously audit and review inmate files in accordance with DOC policies and procedures. We encourage DOC to continue to pursue its plans to centralize the records management functions for all 18 institutions and relocate the management of inmate records to the Concord and Framingham facilities.

Auditee's Response:

> *Department of Correction executive level administrators have issued a directive to all facility superintendents mandating that the requirements of Department policy 103 DOC 401 - Booking and Admissions be adhered to. Specifically, an emphasis was placed on*

the quarterly audit process of the Inmate Management System (IMS) required by the 401 policy.

Additionally, the superintendents were instructed to review the quarterly IMS audit via the facilities internal auditing system to ensure its completion.

Lastly, the Department's Policy Development and Compliance Unit (PDCU) shall continue to monitor the quarterly IMS audits of booking and admission information via their annual audits conducted at all Department facilities.

The DOC has performed a reorganization of the central records function, effective February 17, 2008.

Auditor's Reply

We recommend that DOC management reinforce and monitor compliance with its policies regarding the consistent auditing of IMS data. We are pleased that the DOC is centralizing the records function as part of a reorganization to improve controls for information in the IMS system. We believe that this will result in a more uniform method for helping to ensure data integrity.

STATUS OF
PRIOR AUDIT RESULTS

Summary and Disposition of Prior Audit Result from
The Office of the State Auditor's Report:
Audit Report No: 2004-0145-4T

Issue (Prior Conditions and Prior Recommendations)	Current Status (what has been done to address prior condition and recommendation)	Disposition
Inadequate System Access Security: **Recommendation**: We recommend that DOC perform an immediate review of the status of all active users of the IMS application and remove all access privileges for those individuals who no longer require access. We recommend that DOC management be more vigilant in the monitoring of access accounts for DOC employees-University of Massachusetts Health Care employees-as well as outside contractors to ensure that access privileges be terminated in a timely manner when individuals no longer require access to the IMS application.	Our current audit found that DOC had developed policies to improve access security controls and user account management. Our tests indicated that all DOC user accounts were properly authorized and valid. However, our tests indicated that DOC was not consistently adhering to SOP 002 – Outside Agency Account Management, as indicated by our audit results. User accounts for access to the IMS application were not being properly disabled for users no longer requiring access, or authorized to have access, to the mission-critical application, which may have placed the system at risk of unauthorized access.	Not Resolved