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. 2004-0145-4T

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

July 1, 2003 through December 3, 2004

OFFICIAL AUDIT REPORT
MARCH 14, 2005

TABLE OF CONTENTS

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 to DOC operations. The Department's primary mission is to promote public safety by imprisoning convicted felons while providing opportunities for rehabilitation and reintegration into society. The DOC is comprised of 17 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 10,000 inmates within the Commonwealth. The University of Massachusetts Health Care is contracted by the Department of Correction to provide comprehensive medical services to all inmates in DOC facilities. The Department received an appropriation of $425.9 million in state funds for fiscal year 2003 and an appropriation of $427.8 million in state funds for fiscal year 2004.

The Technology Services Division (TSD) is responsible for managing all computer operations for the Department. The TSD manages all of the Department's file servers, routers and switches located in various facilities to support local area and wide area network access within the DOC. The DOC's main servers for the IMS, Web, Email, and Citrix systems are all located in the TSD's file server room. In addition, the TSD supports approximately 3,000 microcomputer workstations located throughout the 17 institutions and central office. The TSD provides users with network communications including access to the Internet and the DOC's Intranet, access to Massachusetts Management Accounting and Reporting System, (NewMMARS), Human Resources/Compensation Management System (HR/CMS), and the Criminal Justice Information System. The TSD also manages data file exchanges with various agencies including the Criminal History Systems Board, Commonwealth's Sex Offender Registry, Department of Revenue, Department of Mental Health, and Federal Bureau of Investigation. Additionally, the TSD provides a Help Desk function, and a field staff to provide technical services to the various institutions.

The DOC's main application system is a customized product, called the Inmate Management System (IMS) that was developed by Deloitte Consulting. The IMS application was initially deployed at MCI-Framingham in September 2000 and now serves as the primary application system throughout the Department of Correction. The IMS application consists of over 300 modules and sub-modules. The main 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 internal control examination was limited to a review of certain IT general controls over and within the Department's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From May 17, 2004 through December 3, 2004, we performed an audit of selected information technology (IT) related controls at the Massachusetts Department of Correction's Technology Services Division (TSD) for the period covering July 1, 2003 through December 3, 2004. The scope of our audit included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security over the IMS application, inventory control over IT-related assets, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. In conjunction with our tests of inventory control, we also conducted a limited review of physical security and environmental protection over areas housing IT-related equipment at selected Department of Correction institutions.

Audit Objectives

The primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support its automated systems and to safeguard IT-related assets. We sought to determine whether the IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. 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. Our objective regarding system access security for user account management was to determine whether adequate controls were in place for the activation, maintenance and deactivation of access privileges to ensure that only authorized personnel had access into the Inmate Management System (IMS). Further, we sought to determine whether TSD security staff were actively monitoring the management of user accounts.

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 sought to determine whether adequate controls were in place for on-site and off-site storage of backup media to support system and data recovery operations. Furthermore, we determined whether an effective business continuity plan was in place that would provide reasonable assurance that mission-

critical IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible.

Audit Methodology

To determine audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant IT operations, reviewing and evaluating certain IT-related internal controls, and interviewing senior management at the DOC Central Office. In conjunction with our review of the internal control environment, we determined whether the TSD had developed, reviewed, approved, and implemented internal control documentation, including IT-related policies and procedures. In addition, we reviewed DOC internal audit reports and conducted interviews with the internal audit staff.

Regarding our examination of organization and management, we interviewed senior management, and obtained, reviewed, and analyzed existing IT-related policies, standards, procedures, as well as the TSD organizational structure. We also examined whether the TSD had an established chain of command, appropriate span of control, adequate level of oversight, segregation of duties, and clear points of accountability. We also sought to determine the level of TSD's strategic and tactical planning.

To evaluate physical security, we interviewed management, conducted walk-throughs of the DOC file server room at the Central Office as well as at selected institutions, and reviewed procedures to document and address security violations and/or incidents. We examined the existence of controls, such as office door locks, remote cameras, and intrusion alarms. We determined whether access to areas housing computer equipment was restricted to authorized personnel. Since the DOC facilities are highly sensitive and secure, our tests of physical security controls was limited to reviews of policies and procedures, interviews and observation. We also reviewed the areas housing the on-site and off-site backup media tapes.

To determine the adequacy of environmental controls, we conducted walk-throughs and evaluated controls to assess the sufficiency of documented control-related policies and practices. We examined the file server room and office areas housing selected IT equipment to determine whether IT resources were subject to adequate environmental protection. We also reviewed the areas housing the on-site and off-site backup media tapes. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. 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 IMS application residing on DOC file servers through the microcomputer workstations located at the DOC's administrative office and at the individual institutions. We reviewed control practices regarding logon ID and password administration by evaluating the appropriateness of documented policies and guidance provided to the DOC personnel. We determined whether all employees authorized to access the IMS application were required to change their passwords periodically and, if so, the frequency of the changes. In order to verify that all users of the IMS application system were either current DOC employees, University of Massachusetts Health Care employees, or DOC contract employees, we obtained the IMS user list containing 5,165 users as of July 30, 2004. We compared the user list to a DOC payroll list consisting of 4,972 employees dated July 30, 2004. We then compared the remaining users to a current University of Massachusetts Health Care employee listing and to a current DOC vendor listing. We developed an exception list from which we were able to identify those individuals no longer requiring access privileges to the IMS application. Our audit did not include an examination of controls over network security.

To determine whether adequate controls were in place and in effect to properly account for and safeguard computer equipment, we initially reviewed inventory control procedures for property and equipment and obtained an inventory of IT resources. We verified that appropriate fields of information were contained in the inventory record such as identification tag number, location, description, acquisition date and historical cost for computer equipment. We examined policies and procedures regarding fixed-asset inventory to determine whether the DOC was in compliance with the Office of the State Comptroller's regulations regarding fixed-asset control. We conducted an inventory test applying ACL audit software, selecting a sample of 73 out of 8,581 IT-related items listed on the DOC inventory, dated July 23, 2004. The audit team conducted tests of the selected items at the following DOC facilities: MCI-Norfolk, MCI-Concord, MCI-Cedar Junction, MCI-Bridgewater, MCI-Framingham, MCI-Bay State Corrections, MCI-Shirley, Sousa-Baranowski Correctional Center, MCI-Gardner, Central Headquarters-Milford, and the Technical Services Division in Norfolk. In addition, we judgmentally selected 70 items during our site visits and traced the items from the physical location to the master list. We also confirmed from the master inventory list to the physical location, the 13 highest value IT-related assets having an aggregate value of $680,922, representing 13% of the total inventory valuation of $5,291,320.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the network application

systems be 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. In addition, to evaluate the adequacy of controls to protect data files through the backup of on-site and off-site magnetic media, we visited a total of 11 facilities, interviewed DOC staff, reviewed physical security and environmental protection for areas housing the tapes, and we reviewed logs and determined that the backup tapes were being rotated on a regular basis.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. Criteria for the IT portion of our audit included IT management control practices as outlined in the Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology" (CobiT). The CobiT control model, which is based upon de jure and de facto standards, provides IT-related control objectives and generally accepted control practices.

AUDIT CONCLUSION

Based on our audit at the Department of Correction's Technology Services Division (TSD), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to organization and management, physical security, inventory control for IT resources, on-site and off-storage of backup copies of computer media, and business continuity planning would be met. However, our examination of controls over system access security revealed that policies and procedures should be strengthened to ensure that only authorized users have access to the Inmate Management System (IMS) application. In addition, we found adequate environmental protection controls in place over file server rooms for all but two of the institutions reviewed during our audit.

Our examination of the Technology Services Division's organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties, adequate span of control and clear points of accountability. In conjunction with our review of the internal control environment, we determined that the DOC had developed and implemented written, authorized, and approved IT-related internal control policies and procedures and had documented IT strategic and tactical plans. However, due to our observations of low staffing levels for technical support at individual institutions, we recommend that DOC management perform a formal assessment of technical field staffing requirements to adequately maintain support services.

Our audit revealed that physical security controls provided reasonable assurance that DOC's IT resources would be protected against unauthorized access. We found that at TSD's Central Office in Norfolk and at the selected institutions where we conducted our audit tests, DOC personnel were required to wear identification badges at all times. In addition, non-employees were subject to background identification checks by DOC personnel before gaining access to the individual institution, were escorted during the duration of their visit, and were required to wear visitor badges. Our audit test of the main file server room and the file server rooms at the selected institutions indicated that the rooms were locked and that access to the rooms were limited to TSD personnel. It is our understanding that the file server room in Norfolk will be relocated to the DOC main office in Milford in early 2005. During the course of our audit, we visited and observed the new location that will provide the DOC with enhanced physical security and environmental protection controls.

Our examination of environmental protection controls over the main file server room provided reasonable assurance that DOC's processing needs would be met. In addition, during

the course of our site visits to DOC facilities we found that appropriate environmental controls were in place to provide reasonable assurance that IT resources were being protected. We observed controls in place over file server rooms, office areas, DOC computer training labs and off-site storage locations. We found that control objectives related to general housekeeping, air conditioning, fire prevention and detection, emergency power and lighting, and emergency shut down would be met. However, our audit tests at two DOC facilities indicated certain weaknesses in environmental protection. Specifically, we found that control objectives related to general housekeeping at the file server room at MCI-Concord needed to be strengthened. We found that, contrary to sound IT-industry practices, the file server room was also being used as a storage room for non-IT-related assets and that controls relating to general housekeeping were not adequate. Our audit tests revealed that the file server room at MCI-Bridgewater (Warren Hall location) was not adequately protected from environmental hazards in that we found the file server located on the floor. This condition enhances the risk of water damage to the file server which could result in an interruption in access to vital applications.

Our review of system access security for the Inmate Management System (IMS) application that provides mission-critical information, such as inmate booking information, inmate tracking, and inmate classification, needed to be strengthened. Our tests indicated that a total of 18 individuals had access privileges, but were no longer employed at DOC. In addition, we found 27 University of Massachusetts Health Care employees and 17 DOC contract employees who had active user ID's and passwords were no longer affiliated in any capacity with the DOC and should have had their access privileges to the IMS system terminated. We found that contrary to DOC policy # 751 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 department heads and superintendents. As a result, access to the Department's mission-critical application may be at risk of unauthorized access. We recommend that the DOC enforce its current policy requiring that department heads, supervisors, and the DOC Human Resources Department notify the security administrator of changes in user status that could warrant modification or deactivation of user accounts. Regarding password administration, we found that employees were required to change passwords on a predefined 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.

With respect to IT-related inventory control, our tests indicated that hardware items were properly accounted for, locatable, and tagged. We also verified that software products were

being accounted for in the DOC's inventory records and confirmed that software product licenses were available. We found that the DOC was adhering to the policies and procedures promulgated by the State Comptroller's Office, had conducted annual physical inventories and performed reconciliations to the perpetual inventory record.

We found that the DOC had an adequate business continuity strategy and plan to provide reasonable assurance that IT functions could be regained within an acceptable time frame should processing be rendered inoperable or inaccessible. We determined that control procedures regarding the generation of backup copies of magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate. We also found that DOC management had conducted tests of the business continuity plan and had incorporated test results into their recovery strategy.

AUDIT RESULTS

1. System Access Security

Our audit revealed that system access security over DOC's mission-critical application system, the Inmate Management System (IMS), needed to be strengthened to ensure that only authorized users have access to the system. We found 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. We also found that employees were required to change passwords every sixty days. However, we found that although there were written policies and procedures in place requiring that the TSD be informed when an employee terminates employment at the DOC, we found instances where written notification was not provided by the DOC's Human Resources Department. In addition, we found instances where the TSD had not been notified of changes of employment status of University of Massachusetts Health Care employees as well as DOC contract employees that had access to the IMS application.

Our tests of access security for the IMS application system indicated that, contrary to sound access security practices, there were active user accounts that had not been deactivated for individuals who were no longer employed by the DOC or providing contracted services to the DOC. Our tests of the IMS application system indicated that 62 (1.2%) out 5,165 users were not listed on either the DOC July 2004 payroll, the University of Massachusetts Heath Care July 2004 employee listing, or the list of current DOC contractors. Our audit disclosed that one of the users, who still had active user privileges, had left the employment of the Commonwealth in December of 2002. Our audit tests revealed the following breakdown of individuals no longer affiliated with the DOC yet maintaining an active status on the IMS user list as of July 2004:

U.Mass Health Care former employees	27
DOC former employees	18
DOC former contractors	17
	62 (1.2% of users)

The DOC 's access security policy 751 addresses the issue of controls over the de-activation of user accounts. The policy states in part,*"termination of all network accounts and application access, including but not limited to the network operating system, IMS, the Internet, and email when an employee or outside entity is no longer engaged with the Department or upon the identification of a security violation. Superintendents and Division Heads are responsible to ensure that the Help Desk is notified pursuant to the 103 DOC 756 Information Technology Systems policy to remove or change IMS profiles in all instances when staff transfer, are*

promoted, or otherwise have a change in job function in order to limit staff access to IMS information to only that which is necessary for the performance of their current specific duties."

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform basis. 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 their level of authorization. The failure to deactivate user accounts in a timely manner places the DOC at risk to unauthorized access or use of established privileges (using another individual's user account having higher access privileges). Our audit tests revealed that DOC Superintendents and Division Heads were not notifying the TSD security administrator of changes in user status for DOC employees, University of Massachusetts Health Care employees and DOC contractors. Also DOC had not clearly requested this information from UMass Medical and was not thoroughly monitoring active user accounts. As a result, critical information, including inmate health care information on the DOC's systems, may have been vulnerable to unauthorized access, alterations, and deletions.

Computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, activation and deactivation of user accounts, notification of changes in user status, maintenance of authentication mechanisms, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access

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 urge DOC management to adhere to its established policies and procedures regarding written notification of changes in personnel status from the Superintendents and Division Heads to the Technology Services Division security administrator to help ensure timely deactivation of access privileges. We recommend more vigilant monitoring of access accounts for DOC employees, University of Massachusetts Health Care employees, as well as outside contractors providing services to the DOC, to ensure that access privileges be terminated in a timely manner when individuals no longer require access to the IMS application.

We further recommend that DOC management consider implementing elements of CobiT (Control Objectives for Information and Related Technology). CobiT, issued by the Information Systems Audit and Control Foundation, is a generally applicable and accepted standard for IT

security and control that provides a control framework for management, business process owners, IT functions, users, and auditors. In particular, the CobiT User Account Management Control for Data Security recommends, *"Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties. Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration."*

Auditee's Response:

> *The Technology Services Division has created new procedures to address the notification of employment status for employees, U.Mass Health Care staff, other contractors, and other state agencies. The new procedure directs the entities to notify the DOC Help Desk, in writing via email, of the change in employment status for a particular individual. In addition to these procedures, the Technology Services Division will also run weekly reports of all DOC accounts to identify inactivity that may have not been reported by other entities and subsequently, deactivate and/or delete the user account. The DOC has already performed an immediate review of all active users of the IMS application and removed all access privileges for those individuals who no longer require access. The DOC is continuing to reinforce policies and procedures regarding written notification of changes in personnel status to the Technology Services Security Administrator via the DOC Help Desk. The DOC is performing more vigilant monitoring of access accounts through weekly user account reports for identification of inactivity to ensure access privileges be terminated in a timely manner.*
>
> *The DOC will review the feasibility of implementing elements of CobiT in the next 90 days and will make recommendations to the Commissioner accordingly.*

Auditor's Reply:

We are pleased that the DOC has addressed access security controls for the IMS application by creating and enhancing new notification and monitoring procedures to review account status of all IMS application users. We feel that monitoring and improved communication of changes to user accounts both through the help desk and security administrator simultaneously will assist the DOC in terminating user accounts on a timely basis. We are pleased that DOC is

considering implementing elements of CobiT into their IT control environment. We will examine DOC's efforts to strengthen logical access security during our follow-up audit.

APPENDIX

DOC Response to the Office of the State Auditor's Report On the Examination of Information Technology-Related Controls at the Department of Correction's Technology Services Division

Page 7

Audit Report Statement: "However, our examination of controls over system access security revealed that policies and procedures should be strengthened to ensure that only authorized users have access to the Inmate Management System (IMS) application."

DOC Response: This is being addressed through current policies as well as new procedures that address the identification and elimination of inactive user accounts. In addition, the IMS user profiles have been reviewed for accurate user access depending on employee role.

Audit Report Statement: "In addition, we found adequate environmental protection controls in place over file server rooms for all but two of the institutions reviewed during our audit."

DOC Response: The two institutions have been notified of the environmental concerns in their respective server rooms. In addition, the Technology Services Division has begun to conduct quarterly environmental walkthroughs of all server rooms to ensure that controls continue to be in place. A follow-up walkthrough of these two facilities will be scheduled in March 2005.

Audit Report Statement: "However, due to our observations of low staffing levels for technical support at individual institutions, we recommend that DOC management perform a formal assessment of technical field staffing requirements to adequately maintain support services."

DOC Response: The Technology Services Division has requested that three positions be posted for interview and hire of technical field staff to maintain support services. In addition, a formal staffing analysis was performed by the Maximus Group previous to the Inmate Management System implementation. As a result of the analysis, the staffing levels for the Division have increased, however, due to staff turnover and past hiring freezes, the technical field staffing requirements lagged.

Page 8

Audit Report Statement: "Specifically, we found that control objectives related to general housekeeping at the file server room at MCI-Concord needed to be strengthened. We found that, contrary to sound IT-industry practices, the file server room was also being used as a storage room for non-IT-related assets and that controls relating to general housekeeping was not adequate. Our audit tests revealed that the file server room at MCI-Bridgewater (Warren Hall location) was not adequately protected from environmental hazards in that we found the file server located on the floor. This condition enhances the risk of water damage to the file server which could result in an interruption in access to vital applications."

DOC Response: The MCI-Concord management staff have been notified of the housekeeping and storage concerns in the MCI-Concord server room. They will address these concerns. The MCI-Bridgewater (Warren Hall) management staff have been notified of the environmental hazard and the Technology Services Division is requesting funds to purchase a server rack and mounting kit to remove the server off the floor. In addition, the Technology Services Division will continue to conduct quarterly environmental walkthroughs of all server rooms to ensure that controls continue to be in place.

Audit Report Statement: "We recommend that the DOC enforce its current policy requiring that department heads, supervisors, and the DOC Human Resources Department notify the security administrator of changes in user status that could warrant modification or deactivation of user accounts."

DOC Response: The DOC, in coordination with the Technology Services Division, plans to enforce the policy at management meetings where the process of notifying the security administrator will be reviewed and reinforced. In addition to these procedures, the Technology Services Division will also run weekly reports of all DOC accounts to identify inactivity that may have not been reported by other entities and subsequently, deactivate and/or delete the user account.

Page 10

Audit Report Statement: "Our audit revealed that system access security over the DOC's mission critical application system, the Inmate Management System (IMS), needed to be strengthened to ensure that only authorized users have access to the system…. Our tests of access security for the IMS application system indicated that, contrary to sound access security practices, there were active user accounts that had not been deactivated for individuals who were no longer employed by the DOC or providing contracted services to the DOC."

DOC Response: The Technology Services Division has created new procedures to address the notification of employment status for employees, U.Mass Health Care staff, other contractors, and other state agencies. The new procedure directs the entities to notify the DOC Help Desk, in writing via email, of the change in employment status for a particular individual. In addition to these procedures, the Technology Services Division will also run weekly reports of all DOC accounts to identify inactivity that may have not been reported by other entities and subsequently, deactivate and/or delete the user account.

Page 11

Audit Report Statement: "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 urge DOC that management adhere to its established policies and procedures regarding written notification of changes in personnel status from the Superintendents and Division Heads to the Technology Services Division security administrator to help ensure timely deactivation of access privileges We recommend more vigilant monitoring of access accounts for DOC employees, University of Massachusetts Health Care employees as well as outside contractors providing services to the DOC to ensure that access privileges be terminated in a timely manner when individuals no longer require access to the IMS application."

DOC Response: The DOC has already performed an immediate review of all active users of the IMS application and removed all access privileges for those individuals who no longer require access. The DOC is continuing to reinforce policies and procedures regarding written notification of changes in

personnel status to the Technology Services Security Administrator via the DOC Help Desk. The DOC is performing more vigilant monitoring of access accounts through weekly user account reports for identification of inactivity to ensure access privileges be terminated in a timely manner.

Audit Report Statement: "We further recommend that the DOC management consider implementing elements of CobiT (Control Objectives for Information and Related Technology)."

DOC Response: The DOC will review the feasibility of implementing elements of CobiT in the next 90 days and will make recommendations to the Commissioner accordingly.

Auditor's Rely

We are pleased that DOC management has initiated corrective action to strengthen control weaknesses brought forward both in the audit conclusion and audit result section of our report. Specifically, the remedial actions concerning environmental controls, system access security and technical field staffing levels should strengthen the DOC's IT control environment. We will examine the progress made by the DOC in these areas during our follow-up audit.