The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2010-1433-4T

DEPARTMENT OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE ESSEX SHERIFF'S DEPARTMENT

July 1, 2007 through December 30, 2009

OFFICIAL AUDIT REPORT

MAY 12, 2010

TABLE OF CONTENTS

INTRODUCTION

The Essex Sheriff's Department (ESD), formerly known as the Essex County Sheriff's Department, was established as an independent state agency on July 1, 1999, as a result of the abolishment of Essex County government pursuant to Chapter 300 of the Acts of 1998. Chapter 127 of the Acts of 1999 amended the Massachusetts General Laws by adding Chapter 34B, which stipulated that the Sheriff became an employee of the Commonwealth, but remained an elected official and retained administrative and operational control over the ESD, the jail, and the House of Correction.

The ESD serves the Essex County community and the Commonwealth by assisting in providing a safe and secure environment as well as correctional and educational services at its facilities. The ESD received funding appropriations from the Commonwealth of $49,517,213 in fiscal year 2008 and $46,066,000 in fiscal year 2009 for the operation of the jail, the House of Correction, and other statutorily authorized facilities and functions. As of November 30, 2009, the ESD had approximately 590 employees with an inmate capacity of 1,353 inmates. During the audit period, the ESD had a total average inmate census of 1,545 inmates. ESD's main facility, which is located in Middleton with a rated inmate capacity of 989, had an average inmate census of 1,200 inmates during our audit period. A second facility in Lawrence, which has a capacity of 340 inmates, had an average inmate census of 321 over the period. Lastly, a women's facility located in Salisbury has a capacity and census of 24 inmates.

As presently structured, the ESD is responsible for running and overseeing all aspects of its facilities, which consist of the Essex County Correctional Facility in Middleton, the Correctional Alternative Center in Lawrence, the Women in Transition Center in Salisbury, and three Community Corrections Centers located in Lawrence, Salisbury, and Lynn. The ESD has an extensive inmate support network in the areas of rehabilitation services, educational training, and vocational training. These courses and training include, but are not limited to, automotive technician, HVAC, graphic arts, culinary arts, adult basic education, computer skills, drug and alcohol counseling, substance abuse treatment, and anger management.

In addition to its correctional programs, the ESD is responsible for the service of legal papers and notices through the Department's Civil Process Division. The Civil Process Division is under full operational control of the Essex County Sheriff and employs 11 full-time employees consisting of a Director, Assistant Director, Head Deputy, two Lieutenants, and six clerks. The salaries of the full-time employees are funded through ESD's state appropriation account. The Civil Process Division also utilizes 31 Deputy Sheriffs serving Civil Process who are not state employees and are appointed pursuant to Chapter 37, Sections 3 and 11, of the Massachusetts General Laws. These non-state employee vendors and the Deputy Sheriffs are compensated through revenues generated by the Civil Process Division.

Profit and loss statements for the calendar year ending December 31, 2008 showed fees collected totaling $1,818,788, less operating expenses of $1,862,463, resulting in a loss from operations of $43,675. In past years, the Civil Process Division retained all revenues collected. However, Chapter 26, Section 639, of the Acts of 2003 requires that, starting in fiscal year 2004, the Civil Process Division must submit 50% of the increase in its fees to the Commonwealth. Effective February 1, 2004, Chapter 26, Section 639, of the Acts of 2003 requires the Civil Process Division to submit a report with the House and Senate Committees on Ways and Means detailing the civil process fees charged by the Civil Process Division. Records of the Civil Process Division show that $258,777 in fee increases for fiscal year 2009 was remitted to the Commonwealth's General Fund.

Computer operations at the ESD are supported by the Information Technology and Telecommunications (IT) Department. At the time of our audit, the IT Department, which was staffed by six individuals, supported and managed ESD's local area networks (LAN) to which approximately 232 computer workstations are connected. The IT Department also manages information technology (IT) resources at ESD's remote sites that house file servers, workstations, and other peripherals. The ESD network consists of 18 servers, the computer workstations, printers, routers, switches, hubs, (media converters, fiber optic cable, category5 cable), T-1 lines, and a firewall. The ESD domain is based on Windows 2003 Active Directory and TCP/IP. The ESD's servers include file/print servers, Citrix servers, domain servers, a GPS fleet server, an exchange server, and a backup server. The network configuration allows employees access to the ESD's mission-critical application, the Sheriffs Information and Reporting System (SIRS), shared peripherals, the Internet, and other management applications. The LANs are connected to the ESD's wide area network (WAN), which allows access to the Commonwealth's statewide WAN through redundant high-speed connections. The statewide WAN provides access to the Human Resources/Compensation Management System (HR/CMS), the Massachusetts Management Accounting and Reporting System (MMARS), and MassMail (e-mail system) to file servers located at the Commonwealth's data center in Chelsea. The Sheriffs Information and Reporting System, which was developed by the Commonwealth's Information Technology Division (ITD), was built upon a relational database that provides the ESD with inmate management information, electronic document generation, and other management capabilities.

The Office of the State Auditor had previously conducted an audit of the ESD in conjunction with a statewide review of the seven Sheriffs' Departments within the Commonwealth's system for the period July 1, 2002 to December 31, 2003. The purpose of that review was to determine whether the seven Sheriffs' Departments that were being transferred from county government to the Commonwealth's system had established internal controls over financial and program operations and were complying with applicable laws, rules, and regulations relating to their fiscal and operational activities.

Our current audit was limited to a review of certain IT general controls over and within the ESD's IT environment and a follow-up review to determine whether corrective action had been taken to address the audit results and recommendations in our prior audit, No. 2004-1433-3S.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Essex Sheriff's Department for the period July 1, 2007 through December 30, 2009. The audit was conducted from September 1, 2009 through December 30, 2009. The scope of our audit included an examination of physical security and environmental protection at the administrative headquarters in Middleton and two satellite locations, system access security for ESD's automated systems, inventory control for computer equipment and software, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. In conjunction with our audit, we reviewed IT-related policies and procedures for the areas under review. Our audit scope also included a follow-up examination of corrective actions taken by the ESD to address the audit results and recommendations contained in our prior audit report, No. 2004-1433-3S, issued April 19, 2006.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required. We sought to determine whether adequate physical security controls were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of IT assets. We determined whether sufficient environmental protection controls were in place to provide a proper IT environment to prevent and detect damage or loss of IT resources. In addition, we determined whether adequate controls were in place and in effect to provide reasonable assurance that only authorized users were granted access to network resources, including the SIRS application system and other business-related applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. An additional audit objective was to determine whether adequate controls were in place and in effect to provide reasonable assurance that all IT resources under ESD's charge were properly accounted for in a reliable inventory system of record.

We sought to determine whether adequate business continuity planning had been performed and whether disaster recovery and business continuity plans were in place to restore IT systems in a timely manner for mission-critical and essential business operations should the automated systems be unavailable for an extended period. In conjunction with our examination of business continuity planning, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media for systems and data files residing on the ESD's file servers. With respect to our

follow-up examination of our prior audit results and recommendations, we determined the extent and nature of corrective actions taken by the ESD to address these issues.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of the ESD's mission and business objectives. To gain an understanding of the primary business functions that were supported by the automated systems, we conducted pre-audit interviews with the managers and staff and reviewed ESD's enabling legislation and other laws affecting all sheriffs' departments. We also reviewed the ESD's website and selected documents, such as the Essex Sheriff's Department Internal Control Plan, last updated April 12, 2009. Through interviews, we gained an understanding of the information technology used to support the ESD's business operations. We documented the significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. We also reviewed our prior audit report to identify recommendations presented on our audit findings in the report. We developed our audit scope and objectives based on our pre-audit work that included an understanding of the ESD's mission, business objectives, and use of IT technology.

As part of our audit work, we reviewed the organization and management of IT operations that support the ESD's business functions. In that regard, we reviewed relevant policies and procedures, reporting lines, and IT-related job descriptions. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives, such as the Essex Sheriff's Department Internal Control Plan. Regarding our review of IT-related procedures, we interviewed senior management and staff and completed internal control questionnaires.

We interviewed ESD management to discuss internal controls regarding physical security and environmental protection over and within the administrative department and file server room housing computer equipment and on-site and off-site storage areas for backup copies of magnetic media. We inspected the administrative headquarters and the two file server rooms in ESD's work locations in Middleton, reviewed relevant documents, and performed selected preliminary audit tests. In conjunction with our review of internal controls, we performed a high-level risk analysis of selected components of the IT environment.

To determine whether adequate controls were in effect to prevent and detect unauthorized access to the office locations housing automated systems, we inspected physical access controls, such as locked

entrance and exit doors, the presence of Essex Sheriff's Department corrections officers within ESD facilities, and whether visitors were required to sign in and out. We reviewed access control procedures, such as the list of staff authorized to access the administrative headquarters and file server rooms and the presence of surveillance cameras and intrusion alarms. In addition, we reviewed control procedures regarding the physical keys and combination locks to the doors of the file server rooms and key management procedures for the distribution of physical keys to ESD managers and staff.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply, surge protectors, emergency power generators, and emergency lighting installed in the administrative headquarters and file server rooms. We reviewed general housekeeping procedures and determined whether only appropriate equipment and supplies were placed in the file server rooms. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the file server rooms. Furthermore, we checked for the presence of water detection devices within the file server rooms, and whether the servers and other computer equipment were on racks raised above floor levels to prevent water damage.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated application systems. To determine whether ESD's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the acting Chief Information Officer (CIO), who was responsible for controlling access to ESD's network resources, and evaluated selected access controls to the network and to the applications available through the network. In addition, we reviewed ESD's control procedures regarding remote access privileges to the network for ESD personnel. We determined whether ESD's internal control documentation included appropriate management control practices, such as an acceptable use policy for IT resources, and security awareness training. We interviewed ESD managers and staff regarding security procedures for authorized access to the automated systems and the control and monitoring of the ESD's network.

To determine whether the administration of logon IDs and passwords was being properly carried out, we reviewed and evaluated access control practices regarding provisioning of IT resources and activation and maintenance of user accounts. We reviewed the security procedures for access to the SIRS application system and other business-related applications with IT personnel. We reviewed control practices used to assign ESD staff access to network resources, including SIRS, the Massachusetts Management

Accounting and Reporting System (MMARS), and the Human Resources/Compensation Management System (HR/CMS). 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 and activating access to application software and related data files.

To determine whether selected users with active privileges were current employees or outsourced staff, we obtained the listings of individuals granted access privileges to SIRS, MMARS, and HR/CMS. We compared 89 out of 625 (14%) users granted access to SIRS, seven users (100%) granted access to MMARS, and nine users (100%) granted access to HR/CMS, as of October 7, 2009, to the personnel roster of current employees and outsourced staff. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so required, we reviewed the frequency of the changes. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition, length, and frequency of password changes.

Regarding inventory control over IT resources, we initially reviewed formal policies and procedures promulgated by the Office of the State Comptroller (OSC) regarding inventory control. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed the roles of ESD personnel regarding the accounting for computer equipment and software, reviewed the inventory control procedures for IT resources, and performed selected tests. During our fieldwork, we obtained from the acting CIO the hardware inventory record, as of October 20, 2009, that listed servers, computer workstations, notebook computers, and other computer equipment items. We determined whether computer equipment installed at the administrative headquarters and House of Corrections in Middleton and satellite locations in Danvers, Salem, and Salisbury was tagged with state identification numbers and whether ESD's inventory record accurately reflected tag numbers and equipment serial numbers. We reviewed the inventory record to determine whether appropriate data fields, such as description, state identification number, manufacturer's model number, serial number, location, and cost, were included for each piece of equipment listed in the record and provided sufficient information to identify and monitor computer equipment. We also performed data analysis on the inventory record to identify any duplicate records, unusual data elements, or missing values.

To determine whether the hardware inventory record accurately reflected computer equipment installed in Middleton and three satellite locations as of October 20, 2009, we initially reviewed all 519 items of computer equipment listed on the record. We selected a statistical sample for review of 108 (20.8%) items listed on the inventory record for equipment that was located in Middleton, Danvers, Salem, and Salisbury. We compared the tag numbers and serial numbers attached to the computer equipment to the

corresponding numbers listed on the inventory record. We determined whether serial numbers were accurately recorded on the record. Moreover, to further assess the integrity of the inventory record, we selected a judgmental sample of 42 additional computer equipment items installed in Middleton and Salem. We determined whether the 42 items had been properly assigned asset numbers, were tagged, and were properly recorded on the inventory record. In addition, we confirmed that the information recorded for all 18 of the servers listed on the inventory record was accurate and complete and that the equipment was installed at the ESD.

With respect to notebook computers, we initially determined the role of the ESD regarding the management and control of the computers. We determined whether information regarding all 21 notebook computers listed on the inventory was accurate and complete by identifying the actual equipment and comparing the equipment-based information to what was recorded on the inventory record. We reviewed control procedures for assigning notebook computers to ESD managers and staff. To gain an understanding of control procedures regarding the distribution to and return of the notebook computers from ESD staff, we interviewed the acting CIO.

To determine whether the ESD had complied with the OSC's regulations regarding accounting for fixed assets, we reviewed evidence supporting ESD's performance of an annual physical inventory. In addition, we sought to determine whether ESD's staff were aware of, and in compliance with, Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen assets. We reviewed documented inventory control policies and procedures, interviewed senior management to determine whether ESD had any incidences of missing or stolen IT-related equipment during the audit period, and verified whether any incidents were reported to the Office of the State Auditor. We determined whether any computer equipment had been designated as surplus or disposed of during our audit period.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to restore mission-critical and essential operations in a timely manner should the automated systems be unavailable for an extended period. We interviewed the acting CIO to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. We determined whether the written plan or other business continuity documents included sufficient information to support the resumption of the ESD's normal business operations in a timely manner.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed the acting CIO and IT staff responsible for generating backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of backup copies of mission-critical

and essential magnetic media at the administrative headquarters in Middleton and the off-site storage location in Danvers. We reviewed procedures for transferring to and retrieving from the off-site storage location backup copies of magnetic media. We inspected the ESD's file server rooms and reviewed the adequacy of physical security and environmental protection controls over the backup media stored in the room. We reviewed the location for off-site storage of backup copies generated by the ESD. To determine whether backup copies of magnetic media stored at the on-site and off-site locations were adequately safeguarded from damage or loss, we reviewed physical security over the on-site and off-site storage locations through observation at the sites and interviews with the acting CIO. We did not review ITD's procedures for generating and storing off-site backup copies of data files for the Massachusetts Management Accounting and Reporting System and the Human Resources/Compensation Management System.

To determine the nature and extent of the ESD's corrective actions taken to address our prior audit results and recommendations (No. 2004-1433-3S), we interviewed ESD senior management and staff, reviewed documented internal control policies and procedures, such as the Essex Sheriff's Department Internal Control Plan, and reviewed certain financial reports and documents, including the ESD's year-end GAAP transmittal for fiscal year 2009.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1), as issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Our audit of the Essex Sheriff's Department (ESD) disclosed that IT resources, including the file servers and workstations installed at the administrative headquarters in Middleton, were adequately safeguarded and environmentally protected. We determined that appropriate control practices regarding logon ID and password administration were in place and in effect to help provide reasonable assurance that only authorized parties could access network resources. Although we found that the ESD had developed certain controls regarding business continuity planning, the ESD needed to strengthen controls to provide reasonable assurance that normal business operations could be resumed in a timely manner should automated resources be unavailable for an extended period.

Our audit found that adequate physical security controls were in place over and within the administrative headquarters in Middleton and the file server rooms to provide reasonable assurance that access to IT resources would be restricted to only authorized persons and that IT resources would be safeguarded from damage or loss. We determined that ESD's correction officers were on duty 24/7 at the House of Corrections and adjacent administrative headquarters in Middleton, visitors were escorted and required to sign for and obtain a security badge prior to entering the headquarters' business offices, and that cameras were installed in appropriate locations. We found that appropriate key management controls were in place for the ESD's business offices. We determined that the ESD file server rooms were locked and that access was restricted to only authorized IT department staff.

We determined that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place in the administrative headquarters to help prevent damage to, or loss of, IT resources. We found that emergency procedures were posted in the administrative office areas. Our audit disclosed that the file server room was well organized, subject to temperature and humidity control, and there was an uninterruptible power supply (UPS) device in place to permit a controlled shutdown and prevent a sudden loss of data. The servers were placed on a rack above floor-level to prevent water damage, and the file server room had an automatic fire suppression system and a hand-held fire extinguisher available.

Regarding systems access security, we found that appropriate control practices were in place regarding the authorization of personnel to be granted access to network resources, activation of access privileges through the granting of a logon ID and password, and deactivation of access privileges. Furthermore, we found that access privileges would be deactivated or appropriately modified should ESD employees terminate employment or incur a change in job requirements. Our tests confirmed that, with the exception of two recently-terminated staff members, users granted access to SIRS were ESD employees

or outsourced staff, and that only current ESD employees had access to MMARS and HR/CMS. We determined that adequate policies and procedures were in place for password formation, use, and frequency of change.

With respect to inventory control over computer equipment, we found that although the ESD had well-documented and adequate internal controls regarding ordering and purchasing of fixed assets, computer equipment was locatable, and an inventory system of record for IT resources existed, control practices needed to be strengthened to provide reasonable assurance that all IT resources would be properly recorded and accounted for. Because the inventory had not been reconciled over the audit period, certain items of computer equipment had not been included in the official inventory system of record. We determined that computer equipment received by ESD, including 37 desktop computers, had not been recorded on the inventory system of record as of October 20, 2009. In addition, we found that several tag numbers affixed to the equipment had not been recorded on the inventory. We also determined that the inventory record did not contain two fields of information for asset cost and acquisition date, as required by the Office of the State Comptroller's (OSC) regulations. As a result, the inventory list could not be relied upon as a current, accurate, complete, and valid record of all computer equipment installed at the ESD. We determined that the ESD did maintain a current and complete list of licensed software, and that software licenses for the business-related applications were appropriately on file at the administrative headquarters.

Our audit indicated that, although the ESD maintained signed control sheets for notebook computers that were assigned to managers and staff, the forms lacked acknowledgement of user responsibilities for security and acceptable usage. We found that ESD was aware of Operational Services Division requirements regarding surplus property. Our review of compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that ESD personnel responsible for inventory were aware of the requirements, and that ESD had experienced two occurrences of stolen assets during the audit period which were subsequently reported to the Office of the State Auditor.

Regarding business continuity planning, we found that the ESD lacked an approved, comprehensive, and tested business continuity plan to address the loss of IT systems and processing capabilities. Our audit revealed that ESD had not developed a written business continuity plan containing detailed emergency/evacuation plans, a list of mission-critical systems, information related to the restoration of IT services, instructions regarding a declaration of an emergency, and a contact list. We found that ESD's controls were adequate regarding on-site and off-site storage of backup magnetic media.

To strengthen business continuity controls, we recommend that ESD perform a criticality assessment and risk analysis, develop a list of all potential disaster scenarios and instructions to follow for each event, document a list of vendors, and develop an emergency contact list to include appropriate ESD personnel. The ESD should develop user area plans for each business unit to use when automated systems are not available.

Regarding our review of the results and recommendations contained in our prior audit report on the Essex Sheriff's Department, No. 2004-1433-3S, we determined that three prior audit results, regarding thefts of civil process funds, deposit of civil process fees, and completion of the year-end GAAP transmittal report, had been resolved. We found that one prior result regarding legal clarification of deposits of telephone commissions remained unresolved.

AUDIT RESULTS

1. Disaster Recovery and Business Continuity Planning

Our audit disclosed that the Essex Sheriff's Department (ESD) had not developed a written business continuity plan containing detailed emergency/evacuation plans, a list of mission-critical systems, information related to restoration of IT services, instructions regarding a declaration of an emergency, and a contact list to provide sufficient recovery strategies or resources to restore normal business operations in a timely manner should automated systems be unavailable for an extended period. We also found that the ESD had not designated an alternate processing site. Depending on the nature and extent of a loss of IT systems or processing, the ESD could experience difficulties in regaining mission-critical and essential business processes within an acceptable period of time given the absence of a sufficiently comprehensive recovery and business continuity plan specific to the ESD.

We found that the following control practices related to business continuity needed to be enhanced or developed:

- Perform a criticality assessment and risk analysis;
- Designate an alternate processing site where computer systems can be restored;
- Document all potential disaster scenarios and instructions to follow for each specific event;
- Develop detailed procedures for establishing and relocating personnel to an alternate site, including designated staff for each site, supplies, and equipment;
- Develop a contact list, including IT personnel, to be notified in the event of an emergency and include all communication information, such as landline telephone numbers, cell phone, and e-mail;
- Develop departmental unit or user area plans that document the procedures to follow for each business unit to restore or continue business activities should automated systems be inoperable or unavailable for an extended time;
- Document detailed procedures regarding restoration of network services; and
- Develop schedules for testing a comprehensive business continuity plan, document the tests performed, and any corrective action taken.

We determined that at the time of our audit, the ESD had not developed and filed a Continuity of Operations Plan (COOP) with the Massachusetts Emergency Management Agency. The purpose of a COOP is to "provide for the immediate continuity of essential functions of an organization at an alternate facility for up to 30 days in the event an emergency prevents occupancy of its primary facility." The COOP should address important elements fundamental to business continuity planning, such as a listing

of essential business functions, designation of the ESD's mission-critical systems, notification procedures, contact information, and some detail on responsibilities for continuity of operations.

We found that the ESD had implemented on-site and off-site storage of backup copies of magnetic media for data files residing on ESD workstations, and that the ESD had established procedures for on-site and off-site storage of backup copies of magnetic media for systems under its charge. We found that the ESD had adequate physical security and environmental controls over the backup media at the on-site and off-site storage locations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption or loss of computer or network operations. Generally accepted industry practices and standards for computer operations support the need 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.

Contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. Appropriate user area plans should outline recovery or contingency steps with detailed steps to be followed to efficiently restore business operations. The user area plans should be coordinated with overall enterprise-based disaster recovery and business continuity plans.

Recommendation

We recommend that to strengthen disaster recovery and business continuity planning, ESD should:

- Review the list of disaster scenarios regarding the loss of IT systems that would impact ESD operations and business functions. Develop and update recovery and business continuity strategies for each of the disaster scenarios identified.
- Designate an alternate processing site to support the recovery of automated systems and develop and verify through testing a documented disaster recovery plan.
- Recommend that on an annual basis, or upon major changes to the operational or IT environment, ESD perform an enterprise-based risk analysis and criticality assessment of IT systems and

related capabilities. The risk analysis and criticality assessment should include external partners for which technical dependencies exist.

- Implement procedures to obtain from all parties, for which there are significant dependencies, an adequate level of assurance of the viability of disaster recovery and business continuity plans that support mission-critical and essential business functions.
- Establish a single organizational framework to which business process area plans and IT plans can be linked to an overall business continuity plan. In conjunction with the development of the business continuity plan, ESD should establish targets for acceptable time periods by which mission-critical IT operations need to be recovered.
- Develop and perform appropriate levels of testing to provide ESD with sufficient assurance as to the viability of recovery and business continuity plans. Tests should be performed on control practices that can be reviewed and evaluated independently of the test of recovery strategies in conjunction with the implementation of the alternate processing site. Once tests are completed, test results should be reviewed against expected test plan results and reviewed and approved by business process operations and IT management.
- Review business continuity requirements periodically or upon major changes to user requirements regarding the automated systems. We recommend that subsequent to testing the business continuity plan, the plan should be updated when needed to provide reasonable assurance that it is current and viable. The completed plan should be distributed to management and staff responsible to direct and perform recovery procedures.
- Ensure that management and staff are adequately trained to effectively execute disaster recovery and business continuity tasks and activities.

Auditee's Response

We have rectified, or are currently rectifying any and all shortcomings that were noted in your agency's audit. We are also updating existing internal controls and implementing new controls to keep us in compliance with existing state policies.

Auditor's Reply

We are pleased that corrective action is being taken to strengthen disaster recovery and business continuity planning.

2. Inventory Control over Computer Equipment

Our audit disclosed that the ESD's documented inventory control procedures and practices regarding computer equipment needed to be strengthened and formalized to ensure that IT resources would be properly accounted for in a complete and updated system of record. Our audit revealed that although the ESD had formal internal controls regarding ordering and purchasing of fixed assets, and its computer equipment items were locatable, the ESD did not maintain evidence of its performance of an annual physical inventory and reconciliation of fixed assets for fiscal year 2009. In addition, we found that the ESD did not maintain an updated and complete perpetual inventory system of record containing asset information that is required by the OSC.

We also found that the ESD did not maintain a formal policy to control the assignment and use of notebook computers. We determined that although the ESD did require employees assigned notebook computers to sign a control sheet, the form did not contain acknowledgement of responsibility for security and authorized use. The lack of a formal policy and procedures to control notebook computers could hinder the ESD's ability to properly account for available computer equipment.

Our audit disclosed that the ESD was not maintaining a complete inventory record of all computer equipment items on hand. We found that the ESD had not recorded 47 hardware items, including 37 desktop computers with an estimated cost of $28,675, on the inventory record of October 20, 2009. The 37 unrecorded desktop computers included 22 workstations and 15 individual computers used for training purposes. We initially discovered that there were unrecorded items during our audit testing of the ESD's purchased computer equipment. Our examination of 42 invoices and purchase orders for computer equipment acquired during the 2008, 2009, and 2010 fiscal years revealed that 20 items with a total invoice cost of $18,505.82 out of 80 (25%) received items had not been recorded on the inventory record.

Our audit revealed that, although the ESD stated that it had performed an annual physical inventory and reconciliation of fixed assets, it did not maintain evidence of its performance, as is required by the OSC. We found that, at the time of our audit, the ESD did not have formalized and approved policies and procedures pertaining to the inventory of IT resources. We determined that the ESD lacked adequate control procedures and practices to ensure the maintenance of a current, accurate, and complete perpetual inventory record of computer equipment. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is purchased, relocated, or disposed. As a result, the ESD could not provide reasonable assurance of the integrity of the inventory system of record and its reliability as a tool for accounting for and monitoring computer equipment. We initially examined the ESD's October 20, 2009 IT inventory listing and found that, although the record contained fields for the location and description of the items, it lacked fields for asset historical costs, dates of acquisition, and status. Further, other data fields containing information on asset tag numbers were incomplete. We found that, although computer equipment installed in the administrative headquarters and four other ESD locations had been properly tagged with state identification numbers, only 35% of the tag numbers had been recorded on the inventory record.

Data regarding asset costs, assigned numbers, and dates of acquisition are required by fixed assets regulations promulgated by the OSC. Information regarding the status of an item is useful information for supporting IT configuration management by noting the asset's status, such as awaiting deployment, being repaired, obsolete, or designated for surplus.

As a result, the ESD could not provide reasonable assurance of the integrity of the inventory listing, and the record could not be relied upon to assist in the accounting for and verification of computer equipment. Further, the incompleteness of the IT inventory listing as an inventory system of record for computer equipment hindered the ESD's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, meet IT configuration objectives, and serve as a reliable record of IT equipment.

During the course of audit, we provided guidance to the ESD in creating an inventory listing that will serve as its official system of record for IT resources. Subsequently, we reviewed the revised IT inventory listing of December 29, 2009 and found that it contained the 37 previously unrecorded desktop computers. We also noted that the data fields of historical cost and date of acquisition remained unrecorded on this revised IT inventory listing.

Recommendation

To ensure that inventory control over IT resources is adequately maintained, we recommend that the ESD strengthen documented inventory control policies, procedures, and practices to ensure compliance with policies and procedures promulgated in the Office of the State Comptroller's "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation. Specifically, the ESD should record all received computer equipment items within seven days and perform a complete annual physical inventory and reconciliation of computer equipment to ensure that an accurate, complete, valid, and current inventory record of IT resources is in place.

We recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical inventory, acquisition, and disposal records. Also, the ESD should include on its inventory system of record additional data fields to record cost amounts and dates of acquisition of purchased or leased items.

With respect to the ESD's monitoring of IT-related equipment, ESD should improve documentation supporting the annual physical inventory, including a reconciliation of the physical inventory to ESD's inventory records. This improved documentation will help ensure the integrity of ESD's perpetual inventory system of record for IT-related assets and provide reasonable assurance that ESD's inventory records can be effectively used to support IT configuration management and help safeguard its computer equipment. Further, once ESD has completed an annual physical inventory of computer equipment, we recommend that ESD maintain supporting documentation of the physical inventory performed and its reconciliation to the perpetual inventory system of record.

Finally, with respect to notebook computers, we recommend that the ESD develop a formal policy requiring that users who are assigned notebook computers must sign a responsibility and acceptable usage

form. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment.

Auditee's Response

> *We have rectified, or are currently rectifying any and all shortcomings that were noted in your agency's audit. We are also updating existing internal controls and implementing new controls to keep us in compliance with existing state policies.*
>
> *Also, we wanted to respond to one issue detailed on page 11, paragraph 2 in the Audit Conclusion. It is stated there that "37 desktop computers had not been recorded on the inventory system." While this is true, the computers in question were recorded in a second inventory list, which our department kept separate due to a misinterpretation of inventory policy. All of these computers were listed and fully accounted for, albeit on a subordinate list.*

Auditor's Reply

We acknowledge that management at the Essex Sheriff's Department had rectified, or was in the process of rectifying, discrepancies and weaknesses noted at the end of the audit period. We also acknowledge that the 37 desktop computers not recorded on the inventory system of record during our initial review were fully accounted for; however, only 15 individual computers located in a classroom setting were recorded in an additional inventory record. Of the other 22 desktop computers, 10 were determined to be fiscal year 2008 and 2009 purchases that were not recorded on the IT inventory system of record, and 10 other desktop computers were still in storage and had not been recorded on the inventory system of record as of October 20, 2009. Another two desktop computers were found during our physical inventory test of computer equipment but were not recorded on the inventory system of record listing of October 20, 2009.

3. Prior Audit Result Unresolved - Legal Clarification for Deposit of Telephone Commissions

Our prior audit, No. 2004-1433-3S, revealed that legal clarification was needed regarding the collection and disposition of telephone commissions. Our current audit disclosed that this matter has not been adequately resolved. Our prior audit had disclosed that the ESD was depositing telephone commissions into its Inmate Canteen Fund. However, the revenue may belong to the Commonwealth's General Fund, because of the change in the ESD's legal status from a county government entity to an independent agency of the Commonwealth. Chapter 29, Sections 1 and 2, of the General Laws states that revenue payable to the Commonwealth, unless otherwise specified, should be deposited into the Commonwealth's General Fund. Conversely, Chapter 127, Section 3, of the General Laws states that revenue from the sale of goods and services in correctional facilities may be expended for the general welfare of all inmates, at the discretion of the Superintendent. Since telephone commissions may meet the revenue criteria of both

laws, our prior audit noted that legal clarification was needed to resolve the issue as to which law applies. Our current audit disclosed that ESD continues to deposit telephone commission funds into its Inmate Canteen Fund and that legal clarification has not yet been attained or legislation enacted to clarify which General Law applies. The ESD maintains that it will continue to deposit telephone commissions into its Inmate Canteen Fund for the benefit of the inmates and will follow Chapter 127, Section 3, of the General Laws.

Our current audit also determined that the ESD had not obtained legal clarification regarding disposition of the telephone commissions.

Recommendation

We continue to recommend that the ESD seek legal clarification from the Office of the Attorney General regarding which law applies to the deposit of telephone commissions.

4. Prior Audit Results Resolved

a. Compliance with Chapter 647 of the Acts of 1989

Our prior audit, No. 2004-1433-3S, disclosed that thefts totaling $9,384 from the ESD's Civil Process Division's Enterprise Checking Account were not reported to the Office of the State Auditor (OSA) in accordance with Chapter 647 of the Acts of 1989, which requires that all unaccounted-for variances, losses, shortages, or thefts of funds or property be immediately reported to the OSA. ESD officials stated that a Civil Process Division check was stolen and used to create counterfeit checks that were later cashed against its account. ESD officials stated that they felt this theft was not a Chapter 647 reportable condition, since the bank made full restitution to the Civil Process Division. The ESD Internal Affairs Division conducted an investigation and reported irregularities to law enforcement officials. However, the ESD's actions did not preclude it from adhering to Chapter 647 of the Acts of 1989 and immediately reporting all unaccounted-for variances, losses, shortages, or thefts of funds or property to OSA.

During our current audit, we conducted interviews with ESD senior management and reviewed documented policies and procedures, including the ESD's Internal Control Plan, last updated on April 12, 2009. We determined that the ESD had implemented appropriate formal policies and procedures to comply with Chapter 647 of the Acts of 1989. In addition, our audit disclosed that the ESD had two occurrences of stolen assets during our audit period, a notebook computer that was stolen on October 14, 2009, and a theft of $7,608 from the Inmate Canteen fund that was discovered on November, 30, 2009. We determined that the ESD submitted Chapter 647 incident reports regarding these thefts to the OSA on November 30, 2009 and January 4, 2010, respectively.

b. Deposit of Civil Process Fees

Our prior audit disclosed that, in accordance with Chapter 37, Sections 3 and 11, of the General Laws, Deputy Sheriffs throughout the Commonwealth collect fees for the service of civil process. Further, the civil processing fees retained by the Civil Process Division (CPD) were "offline" and not accounted for, reported and recorded on the Massachusetts Management Accounting and Reporting System. Chapter 29, Section 2, of the General Laws requires that all Commonwealth revenue be paid into the Commonwealth's General Fund. Our prior audit disclosed that civil processing fees were being collected and retained for the ESD by the CPD, whose employees worked under the direct operational control of the Sheriff to process transactions and handle all actions related to serving civil process. Our prior audit disclosed that clarification was needed in regards to whether CPD fees should be deposited into the Commonwealth's General Fund or retained by the ESD. Subsequently, the Legislature enacted Chapter 26, Section 639, of the Acts of 2003, which allowed certain sheriffs' departments that filed a required detailed report of all CPD fees to the Legislature by February 1, 2004 to retain 50% of the increase in such fees over a 2003 baseline amount and to deposit the balance with the Office of the State Treasurer (OST).

Our current audit determined that the ESD had filed the required report providing details on its CPD fees with the Legislature prior to the stated deadline. We also reviewed CPD fee amounts remitted by the ESD to the OST in fiscal year 2009 to determine compliance with the law. We determined that $258,777.21 was remitted to the General Fund; representing fee increases for the period July 1, 2008 to June 30, 2009.

c. Year-End GAAP Transmittal Report

Our prior audit report disclosed that the ESD did not submit a complete year-end GAAP transmittal report to the Office of the State Comptroller (OSC) for fiscal year 2003. Our audit disclosed that certain accounts with June 30, 2003 balances, such as the Work Release Account, $83,181, Inmates' Canteen Fund, $32,916, and the Inmates' Account, $224,495, should have been reported to the OSC. ESD officials stated that they did not complete the GAAP report since they had only one asset, other than buildings, valued at over $50,000. OSC's GAAP instructions contain filing requirements for six financial areas, and not just assets valued at over $50,000. These areas include accounts receivable, compensated absences, fixed assets, lease disclosure, assets held in trust, and materials and supplies. During the course of our prior audit, ESD officials stated they were reviewing reporting requirements and seeking guidance from OSC on submitting all reports. Our current audit disclosed that the ESD had submitted a complete year-end GAAP report for fiscal year 2009 in accordance with OSC's GAAP instructions.