The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

TEL (617) 727-6200
FAX (617) 727-5891

No. 2009-1257-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS AT THE EASTERN DISTRICT ATTORNEY'S OFFICE

August 1, 2005 through July 24, 2009

OFFICIAL AUDIT REPORT

DECEMBER 28, 2009

TABLE OF CONTENTS

INTRODUCTION

The Eastern District Attorney's Office (EAS), formerly known as the Essex County District Attorney's Office, is an independent entity within the Executive Branch of the government of the Commonwealth of Massachusetts. It was established under the provisions of Chapter 12, Section 12, of the Massachusetts General Laws and is one of 11 similar offices. EAS provides law enforcement, prosecution, crime prevention, and victim support services to the 34 cities and towns that constitute the district. At the time of our audit, the District Attorney's Office was staffed with 188 employees, including Assistant District Attorneys, Victim Witness Advocates, Juvenile Justice Coordinators, State Police investigators assigned to EAS, Child Abuse Investigators, and support staff. The Office's staff, who work in conjunction with the Judicial Branch and law enforcement communities, handle approximately 40,000 cases each year. EAS received an appropriation of $8,580,122 of state funds for fiscal year 2008 and an appropriation of $8,532,931 of state funds for fiscal year 2009.

As of June 30, 2009, EAS occupied space at 16 locations within the district where it conducts business. EAS pays rent for the main administrative office, located at Ten Federal Street in Salem, and a second location at 121 Central Street in Lynn. In all the other locations, EAS is a rent-free tenant-at-sufferance of either the Trial Court (nine locations) or local municipalities (five locations).

Computer operations at EAS are supported by its Management Information System (MIS) Department. At the time of our audit, the MIS Department, which consisted of four individuals, supported and managed the Office's local area networks (LAN), to which approximately 225 computer workstations are connected. The MIS Department manages information technology (IT) resources at EAS's remote sites that house file servers, workstations, and other peripherals. The LANs are connected to EAS's wide area network (WAN), which allows access to the Commonwealth's statewide WAN through redundant high-speed connections. The LANs consist of nine servers, which include file/print servers, a Citrix server, database servers, report servers, intranet information servers, and the computer workstations. The WAN includes industry standard CISCO routers and Verizon communication equipment. The network configuration allows employees access to EAS's case management system, legal research software, shared peripherals, the Internet, and management applications.

EAS's primary case management application, the DAMION application system, was developed by Constellation Justice Systems. The DAMION system is built upon a relational database that provides EAS with case management, court hearing, and court disposition information, and electronic document generation and management capabilities. 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.

EAS receives technology support from the Massachusetts District Attorneys Association (MDAA), which is an independent association chartered to provide baseline technology services to the 11 elected District Attorneys of the Commonwealth. MDAA's principal mission is to manage major business technology initiatives for the District Attorneys. These technology projects include managing the District Attorneys' WAN and overseeing the rollout of the DAMION case management system and conversion to electronic document management. The MDAA assists in long-term planning for common technology projects, coordinates the implementation of statewide projects such as MassMail, and is the liaison for the various District Attorneys to the Information Technology Division of the Executive Office for Administration and Finance.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within EAS's IT environment and selected financial-related controls.

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 Eastern District Attorney's Office (EAS) for the period August 1, 2005 through July 24, 2009. The audit was conducted from February 6, 2009 through July 24, 2009. The scope of our audit included an examination of physical security and environmental protection at the administrative office in Salem and two satellite locations, system access security for EAS's automated systems, and inventory control practices for computer equipment and software. We examined controls regarding disaster recovery and business continuity planning, including provisions for the 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 areas under review. Our audit scope also included an examination of controls regarding selected financial-related activities of EAS, including forfeited funds and automobiles pertaining to drug-related law enforcement activities.

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 DAMION application system and other business-related office applications, and that procedures were in place to prevent and detect unauthorized access to automated systems. Another objective was to determine whether adequate controls were in place and in effect to provide reasonable assurance that all IT resources under EAS's charge were properly accounted for.

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 mission-critical and essential business operations in a timely manner 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 EAS's file servers. With respect to our examination of selected financial-related activities, we determined whether adequate controls were in place and in effect to ensure proper accounting and safeguarding of forfeited assets resulting from law enforcement-related activities.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of EAS'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 EAS's enabling legislation, EAS's website, and selected documents, such as the "Eastern District Attorney's Office Internal Control Plan," last updated March, 2008. Through interviews we gained a high-level understanding of the information technology used to support EAS'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 developed our audit scope and objectives based on our pre-audit work that included an understanding of EAS'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 EAS'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 "Eastern District Attorney's Office Internal Control Plan." Regarding our review of IT-related procedures, we interviewed senior management and staff, and completed internal control questionnaires.

We interviewed EAS management to discuss internal controls regarding physical security and environmental protection over and within the administrative office 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 office and the file server rooms in EAS work locations in Salem and Lynn, 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 business offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, the presence of State Police officers within the EAS office, 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 office and file server rooms in Salem and Lynn and the presence of surveillance cameras and intrusion alarms. In addition, we reviewed control procedures regarding the physical keys and locks to the doors of the file server rooms and key management procedures for the distribution of physical keys to EAS 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 office 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 level 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 EAS'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 MIS Director, who was responsible for controlling access to EAS's network resources, and evaluated selected access controls to the network and applications available through the network. In addition, we reviewed control procedures regarding remote access privileges to the network for EAS personnel. We determined whether EAS's internal control documentation included control practices, such as an acceptable use policy for IT resources, and security awareness training. We interviewed EAS managers and staff regarding the control and monitoring of EAS's network, including security procedures regarding system access to the automated systems.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with IT personnel for access to the DAMION application system and other business-related applications. We reviewed control practices used to assign EAS staff access to network resources, including DAMION and the Massachusetts Management Accounting and Reporting System (MMARS). To determine whether adequate controls were in place to ensure that access privileges to the automated

systems were granted to only authorized users, we reviewed and evaluated procedures for authorizing 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 DAMION, MMARS, and HR/CMS, compared 196 (100%) users granted access to DAMION, eight users (100%) granted access to MMARS, and five users (100%) granted access to HR/CMS as of April 30, 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, 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 first 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 EAS 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 the hardware inventory record, as of January 30, 2009, from the MIS Director. Workstations, servers, and notebook computers listed on the record were valued at $186,553. We determined whether computer equipment installed at the administrative office in Salem and satellite locations in Lynn and Salem was tagged with state identification numbers and whether EAS's inventory record accurately reflected tag numbers and equipment serial numbers. We reviewed the inventory record to determine whether appropriate "data fields," such as 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, as of January 30, 2009, accurately reflected computer equipment installed in Salem and three satellite offices, we initially reviewed the 591 pieces of computer equipment listed on the record. We selected a statistical sample of 104 (17.6%) items listed on the record, located in Salem, Lynn, and Peabody, for review. We compared the tag numbers and serial numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record and determined whether serial numbers were accurately recorded. Moreover, to assess the integrity of the inventory record, we selected a judgmental sample of 20 pieces of computer equipment installed at locations in Salem, Lynn, and Peabody. We determined whether the 20 pieces of equipment had been properly assigned asset numbers and were tagged and properly recorded on the

inventory record. We confirmed seven (77.8%) of the nine servers listed on the hardware inventory record to the actual equipment installed at EAS. We determined whether any computer equipment had been designated as surplus or disposed of during our audit period.

With respect to notebook computers, we initially determined the role of EAS regarding the management and control of the computers. We reviewed control procedures for assigning notebook computers to EAS managers and staff. To gain an understanding of control procedures regarding the distribution to and return of the notebook computers from EAS staff, we interviewed the MIS Director and Network Administrator.

To determine whether EAS had complied with Office of the State Comptroller's regulations regarding accounting for fixed assets, we reviewed evidence supporting EAS's performance of an annual physical inventory. In addition, we sought to determine whether EAS's staff were aware of, and in compliance with, Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen assets, reviewed documented inventory control policies and procedures, interviewed senior management to determine whether EAS 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.

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 MIS Director 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 reviewed and evaluated the "Essex County District Attorney's Business Continuity Plan," last updated on January 8, 2009. We determined whether the written plan and other business continuity documents included sufficient information to support the resumption of EAS's normal business operations in a timely manner. In addition, we conducted an interview with the Massachusetts District Attorneys Association's (MDAA) Chief Technology Officer to determine the current status of MDAA's business continuity planning and ongoing IT infrastructure upgrade project that will impact the 11 District Attorney Offices.

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 MIS Director and 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 office in Salem and the off-site storage location in Lynn. We reviewed procedures for transferring to and retrieving from the off-site storage location

backup copies of magnetic media. We inspected EAS'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 off-site storage location for backup copies generated by EAS. We did not review ITD backup procedures for transactions processed through MMARS and HR/CMS. To determine whether backup copies of magnetic media stored on-site and off-site were adequately safeguarded from damage or loss, we reviewed physical security over the on-site and off-site storage locations through observation and interviews with the MIS Director.

To gain and record an understanding of selected financial-related activities, we interviewed EAS management, identified sources of revenue, and reviewed the "Eastern District Attorney's Office Internal Control Plan" and other documented policies and procedures for cash and accounts receivable. To determine whether documented controls and recordkeeping were adequate to provide reasonable assurance that cash and other forfeited assets resulting from law enforcement activities were properly accounted for, we interviewed EAS management and staff, reviewed applicable Commonwealth laws and EAS formal policies and procedures, such as the "Essex County District Attorney's Forfeiture Manual." We reviewed forfeiture case file information maintained by EAS for adequacy of documentation and evidence of supervisory approvals. We reviewed the listing provided by EAS of forfeited assets from fiscal year-2008 closed cases containing 205 assets and selected a statistical sample of 17 (8.3%) listed assets, including three automobiles. We verified the recorded amount for EAS's statutory share of forfeited cash initially seized and deposited in bank by local police departments and transferred by the State Treasurer into an account designated for seized assets. We traced EAS's share of the seized cash to a special law enforcement trust fund established by Chapter 94C, Section 47(d), of the General Laws, "the Controlled Substance Act." With respect to seized automobiles in our audit sample, we reviewed custody of the vehicles and examined award letters signed by the District Attorney assigning ownership of the automobiles to local police departments within the district, in accordance with statutory authority.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. 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

Based on our audit at the Eastern District Attorney's Office (EAS), we found that information technology (IT) resources, including the file servers and workstations installed at the administrative office in Salem, were adequately safeguarded, environmentally protected, and properly accounted for. 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 EAS had documented important controls regarding business continuity planning, such as the designation by the Massachusetts District Attorneys Association (MDAA) of an alternate processing site, and that court-related work could continue, EAS needed to strengthen controls, in conjunction with the MDAA, to provide reasonable assurance that normal administrative 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 office in Salem and the file server room 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 State Police officers assigned to EAS were on duty during all business hours at the administrative office, visitors were escorted and required to sign for and obtain a security badge prior to entering the building's business offices, and that cameras were installed in appropriate locations. We found that appropriate key management controls were in place for EAS's business offices. We determined that the file server room was locked by means of a physical key and that access was restricted to selected EAS staff.

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

Regarding systems access security, we found that appropriate control practices 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 were in place. Further, we found that access privileges would be deactivated or appropriately modified should EAS employees terminate employment or incur a change in job requirements. Our tests confirmed that, with the exception of two recently transferred staff members, users granted access to DAMION were EAS employees or outsourced staff, and that only current EAS employees had access to the Massachusetts Management Accounting and Reporting System and the Human Resources/Compensation Management System. 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 EAS's control practices provided reasonable assurance that IT resources were properly accounted for in the inventory system of record. We determined that the inventory system of record for computer equipment, as of January 30, 2009, could be relied upon as a current, accurate, complete, and valid record of computer equipment installed at EAS. However, we determined that the record did not contain required columns of information for acquisition dates and historical cost. We determined that a list of software licenses was maintained. Our review of compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that EAS staff responsible for inventory were aware of the requirements and that EAS had one occurrence of missing or stolen computer equipment during the audit period, which was reported to the Office of the State Auditor on January 29, 2009. We found that EAS maintained 38 notebook computers that were assigned to managers and staff. We also found that EAS maintained sign-in/out logs for all notebook computers and that the status of the computers was periodically monitored.

Regarding business continuity planning, we found that EAS was not adequately covered by an approved, comprehensive, and tested business continuity plan to address the loss of IT systems and processing capabilities. Our audit revealed that although EAS had documented important control practices in the "Essex County District Attorney's Business Continuity Plan," this document did not contain detailed emergency/evacuation plans or list mission-critical systems, information related to restoration of IT services, and instructions regarding a declaration of an emergency. In addition, although the MDAA had designated an alternate processing site in Worcester for the 11 District Attorney Offices, the MDAA's infrastructure upgrade at the site was not yet completed at the time of our audit. We found that EAS's controls were adequate regarding on-site and off-site storage of backup magnetic media.

To strengthen controls, we recommend that EAS, in conjunction with the MDAA, 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 internal and external personnel. EAS should develop user area plans (specific documented plans and procedures for each business unit) to use when automated systems are not available.

With respect to selected financial-related activities, we found that EAS's control practices provided reasonable assurance that cash and other forfeited assets resulting from law enforcement activities would be properly accounted for.

AUDIT RESULTS

Business Continuity Planning

Our audit disclosed that although the Massachusetts District Attorneys Association (MDAA) had documented certain important control practices regarding business continuity planning in the "Essex County District Attorney's Business Continuity Plan," none of the written documentation provided sufficient recovery strategies or resources to restore normal business operations in a timely manner should automated systems be unavailable for an extended period. Depending on the nature and extent of a loss of IT systems or processing, the Eastern District Attorney's Office (EAS) 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 EAS.

Areas requiring strengthening with respect to business continuity-related control practices included, but were not limited to EAS's need to:

- Perform a criticality assessment and risk analysis;
- 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, that provides all communication information, such as landline telephone numbers, cell phone, and e-mail;
- Develop user area plans that document the procedures that each business unit would follow should automated systems be unavailable;
- Document detailed procedures regarding restoration of network services; and
- Develop schedules for testing a comprehensive business continuity plan, and document the tests performed and any corrective action taken.

We determined that at the time of our audit, EAS had not developed an overall Continuity of Operations Plan (COOP). Although EAS is not specifically required to have a COOP in place, development of an overarching business continuity plan can strengthen the development of a disaster recovery and business continuity framework. 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." To a degree the COOP should address important elements fundamental to business continuity planning, such as a listing of essential business functions, designation of EAS's mission-critical systems; notification procedures, contact information, and some detail on responsibilities for continuity of operations.

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

We determined that, at the close of our audit, the MDAA had developed a draft disaster recovery plan for the 11 District Attorney offices, listed mission-critical systems, and had designated an alternate processing site.

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 area plans should be coordinated with overall enterprise-based disaster recovery and business continuity plans.

Recommendation

We recommend that to strengthen business continuity planning, EAS, in conjunction with the Massachusetts District Attorneys Association, should:

- Perform an enterprise-based risk analysis and criticality assessment of IT systems and related capabilities on an annual basis, or upon major changes to the operational or IT environment. The risk analysis and criticality assessment should include external partners, such as the MDAA, for which technical dependencies exist.
- Review the list of disaster scenarios regarding the loss of IT systems that would impact EAS operations and business functions, and further develop and update recovery and business continuity strategies for each of the disaster scenarios identified.

- Implement procedures to attain 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 business continuity framework to which business process area plans and IT plans can be linked. In conjunction with the development of the business continuity plan, EAS 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 EAS 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 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

EAS agrees with the SAO audit (2009-1257-4T) that excellent internal controls are already operating within EAS. As SAO acknowledges, seized and forfeited assets are properly obtained, maintained and accounted for at EAS.

With regard to the IT function that was the principal focus of the audit; EAS also has an excellent control system. As recognized in the audit, EAS maintained a complete, accurate and up-to-date inventory of its IT assets, both of hardware and software. EAS believes that significant progress on the development of a Business Continuity Plan has already been made. To begin with, EAS shares SAO recognition that, even in the event that the IT resources at Ten Federal Street are unavailable, EAS can continue the core-mission functions of criminal prosecution and victim/witness services while the "hot-site" back-up now being created by MDAA comes online. EAS has already developed and stored away from Ten Federal Street the critical contact information that would be needed to rapidly restore its IT operations. With regard to administrative functions including payroll and accounts-payable processing, Ten Federal Street serves chiefly as an access location, since those functions actually operate on the Commonwealth's WAN. A plethora of alternative access sites are available, including the EAS office in the Fenton Judicial Center in Lawrence. EAS recognizes the need to enhance its Business Continuity Plan. EAS strives to manage its resources in appropriate ways, including on-going review of measures for continuity of operations in the face of foreseeable events.

Auditor's Reply

As noted in our audit conclusion, we acknowledge that EAS has controls in place to address physical security, environmental protection, logical access security, inventory control over computer equipment,

and selected financial-related activities for cash and other forfeited assets. Although a loss of IT capabilities would not impair EAS from conducting criminal prosecution and victim/witness services, we are pleased that it recognizes the need to enhance its business continuity plan in concert with the efforts underway at MDAA.