The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

STATE HOUSE, BOSTON 02133

SUZANNE M. BUMP, ESQ.
AUDITOR

TEL (617) 727-2075
FAX (617) 727-2383

**No. 2010-1408-4T**

# DEPARTMENT OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY CONTROLS AT THE SEX OFFENDER REGISTRY BOARD

**July 1, 2007 through August 12, 2010**

**OFFICIAL AUDIT REPORT**

**FEBRUARY 15, 2011**

# The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

SUZANNE M. BUMP, ESQ.
AUDITOR

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


February 15, 2011

2010-1408-4T

Saundra Edwards, Chairperson
Sex Offender Registry Board
P.O. Box 4547
Salem, Massachusetts 01970

Dear Chairperson Edwards:

Enclosed is an audit report for your review. This audit of the Sex Offender Registry Board covers the audit period July 1, 2007 through August 12, 2010. This is one of a number of audits commenced and largely completed during the tenure of my predecessor, State Auditor A. Joseph DeNucci. Should you desire more information relative to this audit, please contact me.

I look forward to fostering a cooperative relationship between our respective offices. If my staff or I may be of assistance at any time, please do not hesitate to call upon us. I know we both share the goal of making government work better.

Sincerely,

Suzanne M. Bump

# TABLE OF CONTENTS

## INTRODUCTION

The Sex Offender Registry Board (SORB) was established pursuant to Chapter 74 of the Acts of 1999, codified through Chapter 6, Sections 178C-178Q, of the Massachusetts General Laws. The SORB is an administrative agency within the Executive Office of Public Safety and Security (EOPSS). According to the SORB's mission statement, its primary purposes are to register and classify all sex offenders, as defined by Chapter 6, Section 178C, of the General Laws in a timely and efficient manner, disseminate the classification level in accordance with the law, and provide appropriate information and services to victims who have been abused by the sex offenders who are within the SORB's jurisdiction.

The salaries of the SORB's employees are funded through the SORB's state appropriation account. The SORB received a Commonwealth appropriation of $4,928,494 for fiscal year 2009 and $3,983,913 for fiscal year 2010. The SORB's headquarters are located in Salem. As of July 30, 2010, the SORB was comprised of a Chairperson and 58 employees, including the Board of Directors, an Executive Director, a Chief Financial Officer, a General Counsel, and an Information Security Officer, as required by Executive Order 504. The SORB consists of the following departments: Board, Legal, Hearings, Operations, Program/Administrative Services, and Victim Services.

SORB is also responsible for maintaining the Commonwealth's database of sex offender information. These functions serve to provide the public with information to raise the level of safety in the community. The SORB works closely with local law enforcement agencies and the State Police to ensure the proper registration of sex offenders who live, work, and/or attend an institution of higher education in Massachusetts. In addition to registration responsibilities, the SORB is the sole agency responsible for the classification of each registered sex offender.

The SORB's classification of a sex offender determines if and how information pertaining to an offender may be released to the public. Currently there are three classification levels for sex offenders under the SORB's process. Level 1 is the least onerous classification that the SORB can assign to a convicted sex offender. The SORB assigns offenders with a low risk to re-offending and a low risk of dangerousness to the public to Level 1. Sex offenders presenting a moderate risk of re-offending and have a moderate risk of dangerousness are assigned to Level 2. Offenders with high risk of re-offending and a high risk of dangerousness are assigned to Level 3. Sex offenders classified as Level 2 or Level 3 are required to appear annually before the police department where the offender resides, or appear before the police department every 45 days if the offender is homeless. In addition, information on Level 3 sex offenders is posted on the Internet.

As a result of Executive Order 510, the responsibility for managing and providing information technology services has recently transitioned to the Secretariat level. Within the EOPSS, the recently formed Office of Technology and Information Services (OTIS) has assumed this responsibility, and the two information technology personnel that were employees of the SORB are now EOPSS employees. One individual is assigned to the Infrastructure Services Group and the other to the Enterprise Applications and Database Services Group within OTIS, and both report to new managers within this new organization. The Secretariat Chief Information Officer (SCIO) maintains overall management control of all IT systems and services within the EOPSS and its agencies.

The Sex Offender Registry Application (SORAPP) is the mission-critical computer application used by the SORB to manage and track information and events associated with the registration of sex offenders within the Commonwealth. This vendor-built application is currently hosted at the SORB; however, under IT consolidation, arrangements are being made to physically move this application to the Public Safety Data Center located at the Massachusetts Information Technology Center (MITC). According to the SORB's Executive Director, this transition is expected to take place during Fiscal Year 2011. In the past, the SORB enlisted the services of contracted information technology vendors to supply support for the SORAPP application systems at the SORB. Effective August 1, 2010, any required services and support would be provided by OTIS.

The SORB's business operations are supported by a Local Area Network (LAN) consisting of file servers, workstations, and notebook computers. The Commonwealth's shared services, such as the Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), are accessed via the Commonwealth's Public Safety Network managed by the EOPSS' OTIS. The SORB has no direct connection to MAGNET. Traditionally, the SORB has used Symantec anti-virus software for scanning of the LAN and all individual workstations; however, in FY 2011 McAfee enterprise anti-virus software will be deployed by OTIS. Security management of the information technology systems is the responsibility of the EOPSS' OTIS IT Information Security Officer.

Our current audit was limited to a review of certain IT general controls over and within the SORB's IT environment and a follow-up review to determine whether corrective actions had been taken to address the audit results and recommendations in our prior audit report, No. 2006-1408-3S.

# 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 Massachusetts Sex Offender Registry Board (SORB) for the period July 1, 2007 through August 12, 2010. The audit was conducted from March 2, 2010 through August 12, 2010. The scope of our audit included an examination of documented IT policies and procedures, physical security, and environmental protection at SORB's office in Salem, system access security for the SORB'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 SORB to address the four prior performance-related audit results and recommendations contained in our audit report No. 2006-1408-3S, dated June 5, 2006.

## Audit Objectives

Our primary audit objective was to determine whether SORB's IT-related internal control environment and documented policies and procedures provided reasonable assurance that control objectives would be achieved to support their business functions. In this regard, we sought to evaluate whether adequate controls were in place to provide reasonable assurance that IT-related 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 SORAPP 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 the SORB'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 SORB'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 SORB to address these issues.

**Audit Methodology**

To determine our audit scope and objectives, we initially obtained an understanding of the SORB's mission and business objectives. To gain an understanding of the primary business functions that were supported by automated systems, we conducted pre-audit interviews with the managers and staff and reviewed the SORB's enabling legislation and other laws affecting its operations. We also reviewed the SORB's website and selected documents, such as the Sex Offender Registry Internal Control Guide, last updated August 14, 2009. Through interviews, we gained an understanding of the information technology used to support the SORB'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 the SORB's mission, business objectives, and use of IT technology.

As part of our audit work, 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 Sex Offender Registry Internal Control Guide. Regarding our review of IT-related procedures, we interviewed senior management and staff and internal control questionnaires completed by SORB's employees.

We interviewed the SORB's 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 office and the file server room, 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, 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 office and file server room, and checked for the presence of surveillance cameras and intrusion alarms. In addition, we reviewed control procedures regarding the combination lock to the door of the server room and key management procedures for the distribution of physical keys for the office to the SORB's 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 office and server room. We reviewed general housekeeping procedures and determined whether only appropriate equipment and supplies were placed in the server room. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the server room. Furthermore, we checked for the presence of water detection devices within the server room, 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 SORB'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 IT Network Manager, who was responsible for controlling access to the SORB's IT resources, and evaluated selected access controls to the network and applications available through the network. In addition, we reviewed the SORB's control procedures regarding remote access privileges to the network for SORB personnel. We determined whether SORB's internal control documentation included appropriate management control practices, such as an acceptable use policy for IT resources, and security awareness training. We interviewed SORB managers and staff regarding security procedures for authorized access to the automated systems and the control and monitoring of the SORB's network.

To determine whether the administration of logon ID 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 Sex Offender Registry Application (SORAPP) system and other business-related applications with IT personnel. We reviewed control practices used to assign SORB staff access to network resources, including SORAPP, the Massachusetts Management Accounting and Reporting System (MMARS), and the Human

Resources/Management Compensation 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 SORAPP, MMARS, and HR/CMS and compared 61 out of 61 (100%) users granted access to SORAPP, six out of six users (100%) granted access to MMARS, and six out of six users (100%) granted access to HR/CMS, as of March 5, 2010, to the personnel roster of current employees and outsourced staff. We determined whether appropriate user ID and password administrative procedures were followed, such as appropriate password composition, length, and frequency of password changes. In addition, as a test for password lockout, we observed three users signing in to SORAPP, one for MMARS, and one for HR/CMS.

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 SORB 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 IT Network Manager the hardware inventory record, as of February 28, 2010, that listed servers, computer workstations, notebook computers, and other computer equipment items. We determined whether computer equipment installed at the office was tagged with state identification numbers and whether the SORB'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, as of February 28, 2010, accurately reflected computer equipment installed at SORB's office, we initially reviewed the 262 items of computer equipment listed on the record. We selected a statistical sample for review of 121 (46%) items listed on the inventory record. 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. Further, to assess the integrity of the inventory record, we selected a judgmental sample of 30 additional items of computer equipment. We determined whether

the pieces of equipment had been properly assigned asset numbers, were tagged, and were properly recorded on the inventory record.

With respect to notebook computers, we initially determined the role of the SORB regarding the management and control of the computers. We determined whether information regarding all 50 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 SORB managers and staff. To gain an understanding of control procedures regarding the distribution to and return of the notebook computers from IT Department staff, we interviewed the IT Network Manager.

To determine whether the SORB had complied with the OSC's regulations regarding accounting for fixed assets, we reviewed evidence supporting SORB's performance of an annual physical inventory. In addition, to determine whether SORB'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 SORB 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 IT Network Manager 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 SORB'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 IT Network Manager and IT staff responsible for generating backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site storage of backup copies of mission-critical and essential magnetic media at the SORB's server room and off-site electronic vaulting of data files. We inspected the SORB's server room and reviewed the adequacy of physical security and environmental protection controls over the backup media stored in the room. We did not review the off-site storage location in Chelsea. To determine whether backup copies of magnetic media stored on-site were adequately safeguarded from damage or loss, we reviewed physical security over the on-site storage

location through observation at the site and interviews with the IT Network manager. We did not review EOPSS' OTIS procedures for generating and storing off-site backup copies of data files for MMARS and HR/CMS.

To determine the nature and extent of the SORB's corrective actions taken to address our prior audit report results and recommendations, we interviewed senior management and staff and reviewed documented internal control policies and procedures. In addition, we received hands-on training from SORB managers and staff regarding the Sex Offender Registry Inquiry System (SORIS) application, reviewed certain documentation on sex offenders, and performed selected tests to verify information within SORAPP. Specifically, we performed sample audit testing of SORAPP files regarding annual registrations of sex offenders, payment of annual registration fees, verifications of sex offender addresses, and timeliness of the SORB's notifications to the Registry of Motor Vehicles to suspend drivers' licenses of absconder sex offenders.

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 Sex Offender Registry Board (SORB), we found that IT resources, including the file servers and workstations installed at the SORB's office in Salem, were adequately safeguarded and environmentally protected. We determined that documented IT policies and procedures were adequate to provide guidance for IT areas we reviewed, but improvements could be made in the level of documentation. We also 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. We found that although SORB had a valid inventory system of record, there was no evidence of an annual physical inventory and reconciliation, and the inventory record lacked a field for historical cost. Although the SORB had developed certain controls regarding business continuity planning, we found that it 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 SORB's office and the server room to provide reasonable assurance that access to IT resources would be restricted to authorized persons only and that IT resources would be safeguarded from damage or loss. We observed that private security officers were on duty patrolling the office complex where the SORB's office is located. We observed that visitors to SORB's office were required to obtain and sign for a security badge prior to entering the office. We also determined that surveillance cameras were installed in various locations outside of the SORB's office. Further, we found that appropriate key management controls were in place for the SORB's office and for the server room. We determined that the SORB's server room was kept locked and that access was restricted to IT staff only.

We determined that adequate environmental protection controls, such as smoke detectors and fire alarms, were in place to help prevent damage to, or loss of, IT resources. We found that emergency evacuation procedures were posted in the administrative office areas. We observed that the file server room was well organized, had appropriate temperature and humidity controls, and had 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 nearby.

Regarding system 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 SORB employees terminate employment or incur a change in job requirements. Our tests confirmed that users granted access to the mission-critical SORAPP application were SORB employees, and that only current SORB employees had access to MMARS and HR/CMS. We determined that documented policies and procedures needed to be improved regarding password formation, use, and frequency of change.

With respect to inventory control over IT resources, we found that SORB had documented policies and procedures regarding ordering and purchasing of fixed assets, computer equipment was tagged and locatable, and there was a valid inventory system of record for IT resources. We also determined that the SORB did maintain a current and complete list of licensed software, and that software licenses were kept on file at the SORB office**.** However, control procedures and practices could be strengthened to provide reasonable assurance that computer equipment would be properly monitored. Our audit disclosed that, although SORB management claimed that it had taken an annual physical inventory of computer equipment, it did not maintain evidence of the physical inventory or its reconciliation to SORB's asset records**.** We also determined that the SORB inventory record did not contain a required field of information for historical asset costs. This information is required by the Office of the State Comptroller's (OSC) fixed assets regulations. SORB should maintain documented evidence of conducting a physical inventory and reconciliation of the inventory records annually and consider adding a field of information for cost to the inventory system of record.

Our audit indicated that the SORB was maintaining signed control sheets for assigned notebook computers, and that these forms contained acknowledgement of user responsibilities for security and acceptable usage. We found that SORB was complying with the Operational Services Division (OSD) guidelines regarding disposition of fixed assets and had obtained and maintained evidence of surplus status approval from the OSD for disposed computer equipment. Our review of compliance with Chapter 647 of the Acts of 1989 reporting requirements for missing or stolen Commonwealth assets revealed that SORB staff responsible for fixed assets were aware of these requirements and that SORB had experienced two occurrences of stolen assets involving two notebook computers and two Blackberry mobile phones in separate incidents in 2007 that had not been timely reported to the Office of the State Auditor. Upon our recommendation, SORB's management reported these stolen equipment items to the OSA during our current audit fieldwork.

Regarding business continuity planning, we found that the SORB 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 the SORB had not developed a written business continuity plan containing disaster recovery elements including 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. We found that SORB's controls were adequate regarding on-site and off-site storage of backup magnetic media.

To strengthen controls, we recommend that the SORB, in conjunction with the EOPSS, 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 SORB personnel. The SORB should develop user area plans and specific documented plans and procedures 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 SORB, No. 2006-1408-3S, we reviewed and updated all four of the following prior performance-related audit results: Sex Offender Registration Fee Collection; Factors Adversely Affecting the SORB's Performance; Sex Offender Address Verifications and Notifications to the Registry of Motor Vehicles, and Costs Related to the SORB's Operations. Our current audit determined that these prior audit results had been resolved. However, timeliness of the SORB's notifications to the RMV regarding absconder offenders could be further improved.

## AUDIT RESULTS

### 1. Disaster Recovery and Business Continuity Planning

Our audit disclosed that the SORB 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, necessary 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 SORB had not designated an alternate processing site. Depending on the nature and extent of a loss of IT systems or processing, the SORB 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 SORB.

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 period of 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 SORB had developed an informal Continuity of Operations Plan (COOP), but had not filed it with the Massachusetts Emergency Management Agency (MEMA). 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 the SORB's mission-

critical systems; notification procedures, contact information, and some detail on responsibilities for continuity of operations.

We found that the SORB had implemented on-site and off-site storage of backup copies of magnetic media for data files residing on SORB workstations, and that the SORB 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 SORB had adequate physical security and environmental controls over the backup media at the on-site storage location.

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 disaster recovery and business continuity planning, SORB should:

- Review the list of disaster scenarios regarding the loss of IT systems that would impact SORB 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.
- 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 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 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, the SORB 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 the SORB 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, that 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**

*The Sex Offender Registry Board (SORB) has reviewed the OSA findings and recommendations regarding business continuity and disaster recovery planning, and is working with the Executive Office of Public Safety and Security (EOPSS) Office of the Secretariat Chief Information Officer (SCIO) to implement the steps necessary to address the areas of concern referenced within the audit. The Office of Technology and Information Systems (OTIS) under the direction of the SCIO is currently developing an enterprise strategy for all EOPSS agencies concerning disaster recovery of IT systems. It is our understanding that all enterprise systems including SORAPP and SORIS will be housed and maintained within the Public Safety Data Center at the Massachusetts Information Technology Center (MITC). Disaster recovery systems will be located at the Mass State Police General Headquarters (GHQ) until the second Commonwealth Data Center in Springfield, MA becomes operational in 2012. Concerning business continuity, the Office of the SCIO has dedicated OTIS personnel assigned to inventory and prioritize essential applications and IT systems within EOPSS. This exercise was conducted during FY 2010 and an inventory exists. The SORB will continue to work with the SCIO and OTIS to ensure that the SORB assets, business operations, and IT service requirements are well documented and that essential services are accounted for in the event of system or facility failure. The OTIS business continuity director is working with ITD and MEMA on these plans. This is an ongoing process.*

*The SORB will continue to work with the SCIO and OTIS to address these findings and establish agency processes and protocols that provide clear direction for staff to ensure the integrity of essential services and resources is maintained. We will also rely on OTIS to establish, implement and maintain the required IT services in support of these requirements. Further information or response may be obtained from the SCIO-EOPSS.*

**Auditor's Reply**

We acknowledge that SORB recognizes the need to enhance its business continuity and disaster recovery planning to address the areas of concern referenced within our audit report. We are pleased that SORB will continue to work with the SCIO and OTIS to implement steps necessary to provide adequate assurance that mission-critical and essential IT systems and operations can be regained within an acceptable period of time. In that light, we reiterate the importance of having a business continuity planning process in place and that disaster recovery and business continuity plans be appropriately tested.

## 2. Prior Audit Results Resolved

### a. Sex Offender Registration and Fee Collection

Our prior audit of the SORB, No. 2006-1408-3S, determined that the SORB was neither billing nor collecting the Sex Offender Registration Fee that is required under Chapter 6, Section 178Q, of the Massachusetts General Laws.

The Sex Offender Registry Board is required to collect an annual registration fee from each offender, as follows:

> *The sex offender registry board shall assess upon every sex offender a sex offender registration fee of $75, herein after referred to as a sex offender registry fee. Said offender shall pay said sex offender registry fee upon his initial registration as a sex offender and annually thereafter on the anniversary of said registration…. A sex offender's duty to pay the fee established by this section shall only terminate upon the termination of said offender's duty to register as a sex offender as set forth in section 178 G.*

Our prior audit noted that the SORB had stopped billing and collecting the $75 sex offender registry fee. Our current audit disclosed that this matter had been resolved and SORB was registering and billing sex offenders for the annual fee. However, SORB needed to improve on collecting the fee. Specifically, our audit review determined that the SORB was mailing annual notification letters to sex offenders notifying them of their responsibility to register as sex offenders and to pay the annual $75 fee. We also note that, effective July 1, 2010, as an additional incentive for collections, the SORB has been granted a Commonwealth revenue retention account for the collection of the sex offender registration fees.

We tested a statistical sample of 87 Level 3 sex offender files in the SORAPP database for compliance with registration and fee payment as of June 30, 2009 and June 30, 2010. Regarding registrations, we found that, for June 30, 2009, the SORB had registered 80, or 92%, of the tested offenders; three had not registered and were in violation of the law; and four were incarcerated and not in violation of the law. As of June 30, 2010, of the 87 Level 3 offender files we tested, 15 were not yet due to register in 2010 and three were incarcerated. Of the remaining 69 offenders qualified for registration, the SORB had registered 67, or 98.5%, and two or 1.5% offenders had not registered and were in violation of the law.

Regarding payment of the annual registration fee, we found that improvements were still needed. Specifically, our audit testing revealed that of 87 tested Level 3 offender files, as of June 30, 2009, only six, (6.9%) were paid; 39 (44.8%) were unpaid; 39 (44.8%) were granted waivers for indigency by SORB; and three (3.4 %) offenders were incarcerated. We found that, as of June 30, 2010, only five (5.7%) were paid; 33 (37.9%) were unpaid; 30, (34.5%) were granted waivers for indigency by SORB; three (3.4%)offenders were incarcerated; and 16 (18.3%) were not yet due to register in 2010.

We suggest SORB consider methods and procedures to improve collection of these fees.

**b. Factors Adversely Affecting the Sex Offender Registry Board's Performance**

Our prior audit of the SORB noted that improvements were needed in the following areas of the SORB's performance:

**Registering and Classifying Sex Offenders from the Board of Probation Database (Initial 15-year look-back requirement)**

Chapter 6, Section 178C, of the General Laws defines a "sex offender" as:

> *a person who resides, works or attends an institution of higher learning in the Commonwealth and who has been convicted of a sex offense or who has been adjudicated as a youthful offender or as a delinquent juvenile by reason of a sex offense or a person released from incarceration or parole or probation supervision or custody with the department of youth services for such a conviction or adjudication or a person who has been adjudicated a sexually dangerous person under section 14 of chapter 123 A, as in force at the time of adjudication, or a person released from civil commitment pursuant to section 9 of said chapter 123 A, whichever last occurs, on or after August 1, 1981.*

Our prior audit noted that SORB had not reconciled the Department of Probation database record of 1981 through 1996 Sex Offenses with SORB records, nor had information on the look-back requirement been integrated into the SORB's mission-critical SORAPP application.

Our current audit determined that SORB senior management, as soon as the SORB was legally permitted, started to register and classify information in 1998 from the Board of Probation's database and added 9,778 files going back to 1981 to the SORAPP database and began to register and classify sex offenders. We determined that, as of May 14, 2010, SORAPP contained data on 20,773 persons, of which 10,995 were Level 1, Level 2, or Level 3 sex offenders required to register during 2010.

**Delays in Classification of Sex Offenders Due to Hearing Process and Limited Number of Hearing Sites**

Our prior audit disclosed lengthy delays in classification of sex offenders due to the complex hearing process and a limited number of hearing sites. Specifically, our prior audit determined that the SORB had only seven hearing sites and a backlog of 964 cases awaiting classification. Our current audit determined

that the SORB had added 31 hearing sites, for a current total of 38. In addition, the backlog of cases awaiting classification hearings had been reduced to 276 cases as of May 14, 2010, according to SORB management. This 71% reduction in case backlog was due to the additional hearing sites and the SORB's streamlining of the classification process, both for offenders requesting hearing as well as those who do not contest classification status. The SORB currently has reduced the classification process from one year to 180 days, according to SORB management.

**Differing Definitions of Sex Offenders among the States**

Our prior audit determined that each state is governed by its own laws, and that a registered sex offender required to register in one state may not have to register in another. Our current audit determined that the Department of Justice (DOJ) through its Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) has taken the lead in establishing a national standard among the states for sex offender laws. Our review determined that according to the DOJ, SORB had made significant efforts to pursue the goal of substantially implementing the Sex Offender Registration and Notification Act (SORNA), which is Title I of the Adam Walsh Child Protection and Safety Act of 2006 (Public Law 248-109). SORNA provides a comprehensive set of minimum standards for sex offender registration and notification in the United States. SORNA aims to close potential gaps and loopholes that existed under prior law and generally strengthens the nationwide network of sex offender registration and notification programs. Each state must comply with the provisions of Title I as explained in the guidelines in order to substantially implement SORNA. According to the SORB's Executive Director, Massachusetts is currently one of four states that were "in material compliance" with SORNA, as of June 30, 2010.

**Penalties Not Always Enforced for Failure to Register**

Our prior audit determined that even when sex offenders are convicted and incarcerated, the courts require the offender to register prior to release. Registration and re-registration of individuals who have been convicted or adjudicated as sex offenders under the law is one of the principal elements of the SORB's mission. In order for the system to be successful, the SORB needs the cooperation of the local police departments, to apprehend, and the judicial system, to prosecute to the fullest extent that the law permits, those individuals who fail to register and/or have repeatedly failed to maintain their registration with the SORB. Penalties for the failure of a sex offender to register are as follows:

Chapter 6, Section 178H, of the General Laws states:

> *(a) A sex offender required to register pursuant to this chapter who knowingly: (i) fails to register; (ii) fails to verify registration information; (iii) fails to provide notice of a change of address; or (iv) who knowingly provides false information shall be punished in accordance with this section.*

> *(1) A first conviction under this subsection shall be punished by imprisonment for not less than six months and not more than two and one-half years in a house of correction nor more than five years in a state prison or by a fine of not more than $1,000 or by both such fine and imprisonment.*
> *(2) A second and subsequent conviction under this subsection shall be punished by imprisonment in the state prison for not less than five years.*

Our current audit determined that the SORB had made significant efforts to improve notification to sex offenders of penalties for failure to register. Specifically, our review determined that the SORB was stating on notification forms sent to sex offenders that failure to register is a criminal offense subject to prosecution. In addition, our review determined that the SORB was conducting trainings for Assistant District Attorneys and Trial Court judges on failure to register cases and effective prosecution and conviction of absconder sex offenders.

**c. Offender Address Verification Compliance and Notification to the Registry of Motor Vehicles**

Our prior audit noted that the SORB had mixed results with several initiatives undertaken to increase compliance with sex offender registration and requirements, including working with police departments on verification of addresses, as well as notification to the Registry of Motor Vehicles (RMV) regarding absconder offenders. To increase the accuracy of the sex offender database, Chapter 26, Section 227, of the Acts of 2003 was enacted, which added Section 22(J) to Chapter 90 of the General Laws. This law requires that the RMV, upon notification from the SORB that a sex offender is in violation of registration, "shall suspend or prohibit issuance or renewal of a license, learner's permit, right to operate a motor vehicle or certificate of motor vehicle registration held by such sex offender." In addition, the SORB had implemented the Post Classification Address Audit of Registered Sex Offenders program allowing police departments to monitor and record offender compliance with registration requirements for Level 3 offenders by conducting random audits on the registered addresses within their jurisdiction. In July, 2005, the SORB expanded the program by requesting that each police department verify each address, (based upon a current address listing of Level 2 and Level 3 sex offenders as registered by that department, or the department in which the offender resides, as well as a form to record the results of an address audit), as recorded in the official SORB database, for each Level 2 or Level 3 offender in its jurisdiction.

Although this program was initiated for the purpose of better monitoring and tracking of sex offenders, our prior audit disclosed that its results had been somewhat mixed, as 17 local police departments out of the 180 communities with Level 3 sex offenders are either not participating, or are only marginally participating, in the audit program. Results from those 17 police departments indicate that only 18 of the 170 Level 3 sex offenders had addresses confirmed.

Our current audit disclosed substantial improvement in both sex offender address verifications and SORB notifications to the RMV. We determined that all communities in the Commonwealth are now participating, either directly or indirectly, in address verification of sex offenders and that the SORB is maintaining the confirmed addresses in the SORAPP database. Specifically, we tested a statistical sample as of June 30, 2009 of 86 Level 3 sex offenders residing in 31 communities. Of these 86 offenders, three were incarcerated and three others had not registered and were in violation. Our tests disclosed that of the remaining 80 Level 3 sex offenders, all 80 had addresses that were confirmed by police departments.

We found that the SORB, in accordance with Chapter 90, Section 22, of the General Laws, was notifying the RMV to suspend the drivers' licenses of absconder sex offenders, but the notifications were not performed in a timely manner. We tested a statistical sample of 82 Level 3 absconder sex offenders from 34 communities as of June 30, 2009. Our audit testing disclosed that the SORB had notified the RMV of 63 absconders, 12 were already incarcerated and considered by law not in violation, and seven others had no Massachusetts driver license. Regarding timeliness of the SORB's notifications to the RMV, we found that for the 63 absconder notifications we tested, the SORB took a weighted average of 163.4 days to notify the RMV. During our audit fieldwork, we recommended to the Executive Director and staff that SORB establish procedures to improve timeliness of notification to the RMV. Although there is no timeline stipulated under law, SORB's management stated that they had an informal policy of 90 days to notify the RMV, and they agreed with our recommendation to establish a new goal of 60 days to complete future notifications. This benchmark for timeliness becomes more important, in light of the 90 additional days maximum that Commonwealth regulations allow the RMV to suspend driver licenses after receiving notification from the SORB.

### d. Costs Related to Sex Offender Registry Operations

Our prior audit of the Sex Offender Registry Board (SORB) noted that SORB should work in conjunction with the Executive Office of Public Safety and Security (EOPSS) in evaluating costs in the following areas:

#### Training Costs

Our prior audit report recommended that the SORB should request that the EOPSS once again visit the topic of studying law enforcement costs relative to sex offender training costs to small police departments (population under 10,000), medium police departments (population over 10,000, under 50,000), and large police departments (population over 50,000). Our current audit determined that training costs to local police departments represented primarily initial training costs and not ongoing training costs. Specifically, during our current audit, the SORB's Executive Director stated that "SORB established a

training room at the agency, which is used to train law enforcement personnel on SORIS. SORB does not charge law enforcement for the SORIS training or use of SORIS. Thus, there are no known costs incurred by police departments to implement SORIS in their respective departments.

**Dissemination of Information to the Public**

We previously noted that the bulk of costs to police departments relative to the establishment of the sex offender registry stemmed from disseminating information to the public. The Act requires police departments to disseminate information to the public in two ways: first, police are required to provide information concerning Level 2 and Level 3 offenders to citizens who inquire at the police department as to registered sex offenders living or working in their jurisdiction ("citizens' requests") as mandated by the General Laws, Chapter 6, Section 178J. Second, for all Level 3 offenders working or residing in their jurisdiction, police must implement a "community notification plan" to notify organizations in the community which are likely to encounter such sex offenders, and to notify individual members of the public who are likely to encounter such sex offenders ("community notification") as mandated by the General Laws, Chapter 6, Section 178K.

Since citizens' requests apply solely to sex offenders classified as Level 2 and 3, and community notification applies solely to sex offenders classified as Level 3, the breakdown of dissemination costs is inextricably intertwined with the SORB's classification process. Also, dissemination costs are dependent upon a variety of factors. Initially, police departments were given wide discretion under the Act as to how to implement their community notification plans. Therefore, police department policy decisions on how to disseminate information will widen the range of costs per jurisdiction. Furthermore, the costs of community notification are mainly predicated upon the population of the jurisdiction and the number of sex offenders working or residing in the jurisdiction.

During our current audit, we determined that the SORB is maintaining the SORAPP and SORIS systems and conducting free SORIS training sessions that are available to all police departments. Through this training and access to SORIS, the trained police department staff members are able to appropriately disseminate information on sex offenders as allowed under the law.

**Technology System Upgrades**

Our prior audit report noted concerns that the SORB would bear the responsibility for programming costs associated with systems used to maintain and access sex offender information.

Our current audit determined that, as a result of Executive Order 510, the responsibility for managing and providing information technology services has transitioned to the Secretariat level. Within the EOPSS, the Office of Technology and Information Services (OTIS) has assumed this responsibility, including

costs related to storage of the SORAPP and SORIS systems and systems upgrades that are expected to occur during fiscal year 2011.

**Additional Costs**

Our prior audit report recommended that SORB request that the EOPSS once again visit the topic of studying law enforcement costs relative to any additional costs to police departments for the establishment of the sex offender registry. This study should be used to help in seeking aid for communities to create and foster a more proactive environment to monitor registered offenders. These potential costs were identified as registration costs, address verification costs, personnel hours needed to provide information to the SORB, and investigation costs.

Our current audit determined that the SORB had communicated with the EOPSS regarding studies of law enforcement costs related to managing sex offenders, but there were no known studies performed at the state level. In addition, police departments are aware that sex offender management is a vital community concern, and nearly all communities are participating, either directly or indirectly, in sex offender registration and management.