The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2009-0074-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS OFFICE FOR VICTIM ASSISTANCE

July 1, 2007 through July 16, 2009

OFFICIAL AUDIT REPORT

JANUARY 4, 2010

TABLE OF CONTENTS

INTRODUCTION	**1**
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	**3**
AUDIT CONCLUSION	**8**

INTRODUCTION

The Massachusetts Office for Victim Assistance (MOVA) was first established by Chapter 258B of the Massachusetts General Laws in 1984 as an independent state agency whose purpose was to promote and ensure the implementation of victim rights and to advocate for and assist victims of crime. The activities of MOVA are governed by the Victim and Witness Assistance Board, whose chair is the Attorney General. The other four board members, which include two district attorneys and two crime victims, work together with the Attorney General and the MOVA staff to set policy for crime victim issues in the Commonwealth. The MOVA's business operations are located at One Ashburton Place, Boston, Massachusetts. At the time of our audit, MOVA had a staff of 18 employees who provide a broad array of services and programs, including but not limited to:

- Victims of Crime Act (VOCA), which is a federal program that provides funding for state- and community-based organizations to offer free mental health counseling and a range of other specialized services for crime victims. VOCA distributes funds to various programs across the state to help survivors of homicide victims, children who witness violence and victims of child abuse, domestic violence, sexual assault, drunk driving, hate crimes, and elder abuse, among others.
- SAFEPLAN which is MOVA's statewide, court-based program that provides specially trained and certified advocates to assist victims of domestic violence seeking protection from abuse. SAFEPLAN advocates help victims of domestic violence to plan for their safety and obtain 209A Restraining Orders (also called Abuse Prevention Orders) through the courts. In addition, the program provides crisis assessment and intervention, including referrals to local support services, information on legal and safety options, and accompaniment to court proceedings.
- The Massachusetts Victim Assistance Academy (MVAA), which was established to ensure that crime victim service providers can best address the needs of crime victims. MVAA provides a weeklong 40-hour training with a "victim-centered" approach that has been deemed a "model for the nation." The curriculum emphasizes how the crime victim's experience changes over time and across the various systems with which they interact (e.g., criminal justice, medical, mental health, victim advocacy, media). The MVAA offers this type of curriculum in order to foster a better understanding of the victim's experience and collaboration among providers. The MVAA curriculum and structure is guided by the efforts of a diverse group of providers and survivors representing both the criminal justice system and community-based organizations.
- The Sexual Assault Nurse Examiner (SANE) Program, which is an initiative with the primary goal of improving the care for victims of sexual assault in Massachusetts. This is accomplished through the development of a statewide, standardized method of evidence collection and the provision of high-quality, coordinated care within the medical, legal, forensic, and advocacy communities. MOVA and the Massachusetts Department of Public Health (DPH) jointly administer the SANE Program. Another critical goal is one of public safety: SANE nurses conduct forensic examinations and evidence collection in hospital emergency departments and, for children, in children's advocacy centers across

the state. These critical skills and services are significant for improving criminal investigations and achieving high successful prosecution rates of sex offenders through the quality of the evidence that is collected and testimony given by the nurse advocates.

- The Victims of Drunk Driving Trust Fund (DDTF), which was enacted on March 8, 2002 to provide assistance to victims of drunk drivers. According to the enabling statute, anyone who is convicted, placed on probation, granted a continuance without a finding, pleads guilty to, or admits to a finding of sufficient facts for operating a motor vehicle while under the influence of intoxicating liquor, marijuana, narcotic drugs, depressant, or stimulant substances is subject to an assessment of $50. The courts collect this assessment, which is not subject to a waiver for any reason. The State Treasurer is the custodian of the fund, and the MOVA is charged with awarding and administering grants from this fund.

According to MOVA, in fiscal year 2008, it received a total of $12,781,879 in state and federal funds. A total of $8,610,816 was received from the federal government, of which $8,049,336 was for a three-year grant. $3,804,817 was received from state government and $366,246 was received from the DDTF. In fiscal year 2008, MOVA's expenditures totaled $11,838,412, of which $340,651 was from the DDTF.

MOVA's IT operations are supported by an IT configuration consisting of a local area network (LAN) composed of one file server and 20 workstations. MOVA has nine notebook computers that can be loaned out to staff upon proper completion of sign-out sheets. MOVA's systems are connected to MAGNet, the Commonwealth of Massachusetts wide area network (WAN), and use anti-virus software for scanning the LAN and all individual workstations. Major application systems used by MOVA include the Human Resources Compensation Management System (HR/CMS) and Massachusetts Management Accounting and Reporting System (MMARS). MOVA has one individual in an information technology position who is responsible for the operation and security of MOVA's IT systems.

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

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 Office for Victim Assistance (MOVA) for the period July 1, 2007 through July 16, 2009. The audit was conducted from April 13, 2009 through July 16, 2009. The scope of our audit included an examination of physical security and environmental protection at the administrative office, system access security for MOVA's automated systems, inventory control over computer equipment and software, and disaster recovery and business continuity planning, including provisions for the on-site and off-site storage of backup copies of magnetic media.

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 to prevent unauthorized use, damage, or loss of IT resources. In addition, 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.

We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT resources and automated systems. We determined whether adequate controls were in place to provide reasonable assurance that only authorized users were granted access to network resources, including the Human Resources Compensation Management Systems (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS) and other business-related office applications, and that appropriate user account management practices are in place to help prevent unauthorized access to automated systems. Another objective was to review and evaluate inventory control practices regarding the accounting for computer equipment and to determine whether there was a software inventory.

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 MOVA's file server.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of MOVA'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 management and reviewed MOVA's enabling legislation, website, mission and business functions, and selected documents, such as MOVA's "Information Technology Internal Control" dated March, 2009. Through interviews, we gained an understanding of the information technology used to support MOVA'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.

In conjunction with our audit, we reviewed IT-related policies and procedures for the areas under review and determined whether written, authorized, and approved policies and procedures 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. Regarding our review of IT-related procedures, we interviewed the Director of Finance and Technology who oversees the IT-related functions. We developed our audit scope and objectives based on our pre-audit work that included an understanding of MOVA's mission, business objectives, and use of IT.

We interviewed MOVA management to discuss internal controls regarding physical security and environmental protection over and within the administrative office, the file server closet housing computer equipment, and the on-site and off-site storage areas for backup copies of magnetic media. We inspected the administrative office and the file server closet, reviewed relevant documents, and performed selected preliminary audit tests.

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 security at the entrance to the building housing the MOVA administrative office; and whether visitors were escorted to their desired location within the MOVA office. We reviewed physical security over the area housing MOVA's file server. In addition, we reviewed control procedures regarding access to MOVA's office area, including management of physical keys distributed to MOVA staff and controls over the keypad combination lock for the door to the agency.

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 hand held fire extinguishers), and an uninterruptible power supply. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the file server closet or in the vicinity of computer-related equipment. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the file server closet and whether temperature and humidity were regulated and continuously monitored. Furthermore, we checked whether the file server and other computer equipment were placed in racks and 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 MOVA's control practices regarding system access security adequately prevented unauthorized access to automated systems, we sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the Director of Finance and Technology, who is responsible for controlling access to MOVA's network resources. Furthermore, we evaluated selected access controls to the network and application systems residing on the network. We determined whether MOVA's internal control documentation included control practices, such as an acceptable use policy for IT resources.

To determine whether the administration of logon ID and passwords were being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the Director of Finance and Technology regarding access to HR/CMS and MMARS as well as other business-related applications.

To determine whether adequate controls were in place to provide reasonable assurance 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. We sought to determine whether appropriate procedures were in place to document the authorization of staff to be granted access privileges to network resources. We tested 100% of all users working at the MOVA office and reviewed documentation for authorizing access privileges to the network. To determine whether selected users with active privileges were current employees, we obtained the list of all 16 individuals granted access privileges to the network and compared it to the full list of MOVA users granted access to the network. Another objective was to determine whether all employees authorized to access the

automated systems were required to change their passwords periodically and the frequency of the 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 MOVA's inventory control procedures for IT resources and performed tests, including tracing of items purchased to the inventory record, tracing items on the inventory record to the actual item and location, and verifying serial numbers and asset tag numbers.

During our fieldwork, we obtained the hardware inventory record, as of November 30, 2008, from the Director of Finance and Technology. We reviewed the inventory record to determine whether appropriate "data fields," such as serial identification number, asset tag number, make, manufacturer's model number, location, cost, and date of purchase were included for each piece of equipment listed in the record and that sufficient information was provided to identify and account for the computer equipment.

To determine whether the hardware inventory record accurately reflected computer equipment installed, we selected all 51 items (100%) listed on the inventory record for review. We compared the serial numbers and asset tag numbers attached to the computer equipment to the corresponding numbers listed on the hardware inventory record. We determined whether the serial numbers and asset tag numbers were accurately recorded on the inventory record. For notebook computers out on loan, we compared the hardware inventory item numbers with those recorded on the sign-out sheet maintained by MOVA staff. We identified IT purchases and determined whether they were properly recorded on the inventory record and were currently in use. We sought to determine whether MOVA was in compliance with the reporting of missing or stolen assets as required by Chapter 647 of the Acts of 1989. We reviewed documented inventory control policies and procedures and interviewed senior management to determine whether any IT equipment had been lost, stolen, or put into surplus during the 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 Director of Finance and Operations 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 the "Backup Tapes Exchange and Schedule," "Building Evacuation Procedures," "MOVA Contact Information (staff)," and the "Severe Weather Plan," all dated April 2009.

We also reviewed the "MOVA Phone Tree" dated May 2009. We determined whether the "Information Technology Internal Control" and other business continuity documents included sufficient information to support the resumption of the MOVA's normal business operations in a timely manner.

To determine whether controls were adequate to ensure that software and data files for business applications would be available should the automated systems be rendered inoperable, we interviewed the Director of Finance and Technology and staff responsible for generating backup copies of magnetic media. To determine whether backup copies of magnetic media stored onsite were adequately safeguarded from damage or loss, we reviewed physical security over the on-site storage location through observation. We inspected the MOVA's file server closet and reviewed physical security and environmental protection controls over the backup media stored in the room. We reviewed procedures for transferring to and retrieving backup copies from the off-site storage location. We inspected the off-site storage location used for storing backup copies and reviewed the "Backup Tapes Exchange Schedules and Instructions" as of April 28, 2009, which documents the distribution and return of backup copies of magnetic media from the off-site storage location.

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 in July 2007.

AUDIT CONCLUSION

Our audit disclosed that the Massachusetts Office for Victim Assistance (MOVA) had adequate internal controls in place regarding physical security and environmental protection over IT equipment, and that appropriate controls were in place and in effect for system access security and inventory control of computer equipment. In addition, we determined that appropriate controls regarding the generation of backup copies of magnetic media for on-site and off-site storage were in place and in effect. We found that although MOVA did not have a comprehensive formal disaster recovery and contingency plan, the office has documented policies and procedures related to IT activities and controls related to business continuity and contingency plans to adequately continue business functions should business continuity strategies need to be exercised in the event of a disaster.

Our audit found that adequate physical controls were in place over and within the administrative office area and the file server closet to provide reasonable assurance that access to IT resources would be restricted to only authorized persons and that computer equipment would be safeguarded from damage or loss. We determined that visitors to MOVA are greeted at the reception desk and escorted to the desired location in the office. We found that appropriate key management controls were in effect and that the office was locked during non-business hours.

We found that adequate environmental protection controls, such as smoke detectors, fire alarms, automated fire suppression system, emergency lighting, and air conditioning for areas housing microcomputer workstations, were in place to help prevent damage to, or loss of, IT resources. Evacuation procedures were posted in the corridors of the building housing MOVA. Our audit disclosed that the file server closet was well organized, temperature and humidity levels within the closet were appropriate, and an uninterruptible power supply (UPS) device was in place to permit a controlled shutdown and to prevent sudden loss of data. The file server was placed above floor level on a rack to prevent water damage. The metal cabinet housing the file server has a physical key. A hand-held fire extinguisher was in the vicinity of the file server closet available for employee use.

Regarding system access security, we found that appropriate control practices regarding the authorization of personnel to be granted access to the network resources, activation of access privileges through the granting of a logon ID and password, and deactivation of access privileges were in place. We found adequate controls in place to ensure that access privileges would be deactivated, or appropriately modified, should MOVA employees terminate employment or incur a change in job requirements. A security officer was designated, policies and procedures were documented, and MOVA staff were

required to sign an acknowledgement statement regarding unacceptable use of the computer. Our tests confirmed that users granted access to the network were MOVA employees listed on the current personnel roster. 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 MOVA'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, as of November 30, 2008, could be relied upon as a current, accurate, complete, and valid record of computer equipment installed at MOVA. 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 and stolen Commonwealth assets revealed that MOVA was in compliance with requirements. We found that MOVA maintained appropriate controls regarding the assignment and return of notebook computers, such as sign-out/sign-in sheets.

Our audit revealed that MOVA has documented policies and procedures related to business continuity planning including "Information Technology Internal Control," "Backup Tapes Exchange and Schedule," "Building Evacuation Procedures," "MOVA Contact Information (staff)", and the "Severe Weather Plan," all dated April 2009, as well as a "MOVA Phone Tree" dated May 2009. Our audit indicated that MOVA was not using agency-managed mission-critical applications and that the risk of loss of processing capability would have a low impact on MOVA's operations. As a result, we determined the business continuity documents included sufficient information to support the resumption of the MOVA's normal business operations within an acceptable time period should a disaster occur and render IT operations inoperable.

Auditee's Response

We agree with the audit results and your recommendations and appreciate your dedication of time and flexibility in our collaborative efforts.