The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

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

No. 2010-0037-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY RELATED CONTROLS AT THE GEORGE FINGOLD LIBRARY

June 29, 2006 through April 13, 2010

OFFICIAL AUDIT REPORT

JANUARY 6, 2011

TABLE OF CONTENTS

INTRODUCTION

The George Fingold Library, also known as the State Library of Massachusetts, is a state agency that was formally established in 1826. In 1960, under Chapter 380, Section 1, the name was changed from the State Library of Massachusetts to the George Fingold Library. Over the years, the library has grown from a collection of statute books, maps, and government documents into a multifaceted resource for state legislators, legislative staff, executive personnel, state employees, historians, genealogists, and the general public. It is the continuing mission of the library to serve the research needs of state government and other interested parties as an official depository of Massachusetts state documents. Users can obtain access to documents and publications in hardcopy, electronic, and microform. The Library's budget for fiscal years 2009 and 2010 was $1,192,572 and $703,755, respectively.

According to Chapter 6, Section 33, of the Massachusetts General Laws, the George Fingold Library's Board of Trustees is comprised of the Senate President, Speaker of the House, and the Secretary of the Commonwealth, who act as ex-officio trustees, and three other members appointed by the Governor. The Governor's appointees are each appointed annually for a four-year term beginning June first of the year of the appointment. Four members of the Board, or their designees, shall constitute a quorum for the conduct of the official business of the Board.

The Library, which is located in the Massachusetts State House in Boston, provides both on-site and remote electronic access to bibliographic records of its collections through an online public access catalog. The general public and state government employees have access to databases and other online resources. There is an inter-library loan program that allows state employees to submit a request to the State Library to obtain books or articles from another library.

Chapter 412 of the Acts of 1984 established the depository program that requires that each state agency shall provide the State Library eight copies of its publications for reference. Two of the eight copies are to be cataloged and added to the library's permanent collection to allow other libraries across the United States to have access to publications in Massachusetts. Since 1975, the State Library has microfilmed all Massachusetts documents in its collection and these documents are accessible through the library's online public access catalog.

The Library uses two mission-critical systems. The first mission-critical system, C/W Mars, is supported by Central/Western Massachusetts Automated Resource Sharing, Inc., which is located in Worcester, Massachusetts. C/W Mars is a network consortium of over 140 public, academic, school, regional, and special library members, including the George Fingold Library. C/W Mars members share an Innovative

Interfaces, Inc., Millennium integrated library system which has combined collections of more than eight million items. The second mission-critical application is DSpace, which is used as an electronic depository for the Massachusetts State Documents Virtual Library. Government documents that are available through DSpace are scanned or captured in electronic form for users to access over the Internet.

The Office of the State Auditor's audit was limited to a review of IT general controls regarding disaster recovery and business continuity planning.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed a follow-up audit of certain information technology (IT) general controls. Our audit, which was conducted from March 1, 2010 through April 13, 2010, covered the period of June 29, 2006 through April 13, 2010. The scope of the audit consisted of an evaluation of the status of prior audit results in our audit report No. 2006-0037-7T, issued June 28, 2006, regarding business continuity and contingency planning.

Audit Objectives

Our primary objective was to determine whether corrective action had been taken to implement recommendations regarding disaster recovery and business continuity planning as identified in our prior audit report issued on June 28, 2006. We sought to determine whether the George Fingold Library had a documented business continuity plan that outlines strategies to regain business operations should IT systems become inoperable or library operations need to be relocated. We also determined whether adequate procedures were in place for off-site storage of backup copies of electronic media required for the restoration of IT systems used by the Library.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included reviewing audit results and recommendations that were provided in the prior audit report. In addition, we sought to obtain an understanding of the State Library's disaster recovery and business continuity plans including a Continuity of Operations Plan (COOP). Once the pre-audit work was completed, we determined the scope and objectives of the follow-up audit.

To assess the extent of corrective action regarding disaster recovery and business continuity planning and to determine whether the Library's COOP had been enhanced, we held interviews with State Library staff to determine whether the criticality of the applications systems had been assessed and whether a risk analysis of computer systems had been conducted. We determined whether a comprehensive COOP was in place and in effect and whether it had been reviewed, tested, and approved. We also reviewed the adequacy of provisions for off-site storage of backup copies of electronic media.

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

AUDIT CONCLUSION

Our audit indicated that although the Commonwealth's Information Technology Division (ITD) generates and stores backup copies of data files for the automated systems used by the George Fingold Library, the Library does not have a sufficiently detailed business continuity plan for recovering business operations. We confirmed that ITD provides off-site storage of electronic backup copies at state facilities as well as at a third-party vendor location for the systems used by the library. In addition, the Library has an agreement with the vendor of one of the systems used by the Library that system data files will be backed up at the vendor's site.

Although the Library has a documented Continuity of Operations Plan (COOP), the plan does not contain detailed instructions for recovering business operations and had not been reviewed, approved, or tested. We found that more details were needed to ensure that an effective COOP would be in place. For example, although the plan states that an alternate location must have sufficient space and equipment to sustain operations for up to 30 days, there were no contingencies regarding staff, equipment, computers, or other resources for the alternate processing site. There was also no user agreement in place with the alternative site detailing what services the Library would be expected to receive in order to continue business operations.

We confirmed that the Library's mission-critical systems are backed up off-site by the Information Technology Division and Central/Western Massachusetts Automated Resource Sharing, Inc. However, the Library's COOP did not indicate any explanations of agreements with, or actions to be taken by, ITD or Central/Western Massachusetts Automated Resource Sharing, Inc. to restore the application systems used by the Library. In addition, while the COOP lists one mission-critical application system, according to Library staff, both DSpace and C/W MARS are mission-critical systems.

We found that in addition to not having sufficient details in the COOP, the plan contained information that appeared to be incorrect. For example, the plan referred to flyaway kits for the Emergency Relocation Group Advance Team; however, no kits were created and the team was never established. Moreover, although the plan stated that a relocation site must have sufficient space and equipment to sustain operations for a period of up to 30 days, the Library staff acknowledged that there had not been any discussions with personnel from the alternate site concerning the availability of space or equipment. In addition, although the COOP stated that semiannual reviews of space allocations should be conducted, there was no evidence that they were performed. Also, although the COOP identified management positions for the Library staff, the responsibilities for each position for recovery or business continuity

tasks were not documented and the name and contact information of the persons holding the management positions were not provided.

State agencies have been required to document their planning efforts for the continuity of operations and government per executive orders of the governor. Between 1978 and 2007, Governors Dukakis, Romney, and Patrick issued three separate executive orders requiring agencies of the Commonwealth to develop plans for the continuation of government services. In 1978, Executive Order No. 144 mandated that the head of each agency within the Commonwealth "make appropriate plans for the protection of its personnel, equipment and supplies (including records and documents) against the effects of enemy attack or natural disaster, and for maintaining or providing services appropriate to the agency which maybe required on an emergency basis." In 2007, Executive Order No. 475 mandated "Each agency within the executive department shall conduct activities on a quarterly basis that support the implementation of its Continuity of Government and Continuity of Operations plan and shall submit a quarterly report…" and "…Each secretariat within the executive department shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice [its] Continuity of Operations plan." In September 2007, Executive Order No. 490 mandated "Whereas, to achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security."

AUDIT RESULTS

1. Prior Audit Result Resolved - Disaster Recovery Planning of IT Systems

Our prior audit report, No. 2006-0037-7T, indicated that although the George Fingold Library had a written Continuity of Operations Plan (COOP), the plan was not tested and did not contain detailed disaster recovery instructions for recovering IT systems operated by the Library. The plan, which was approved by the prior State Librarian, provided a high-level framework for addressing business continuity planning, but not disaster recovery planning.

Our current review of disaster recovery planning revealed that the file server that had been located in the State House at the Library had been moved to the Commonwealth's Information Technology Division's (ITD) primary data center, which provides on-site and off-site backup services for Library files. It is our understanding that ITD would be instrumental in the recovery of the Library's automated system should a disaster render the system inoperable.

2. Prior Audit Result Unresolved - Business Continuity Planning

Although the Library has a documented Continuity of Operations Plan (COOP), the plan has not been enhanced to include instructions necessary for continuation of operations to provide library-related services at an alternate location. Although an alternative operational site is identified in the COOP, an interagency agreement was not in place outlining the availability of the site to support business continuity. We note that the Library did conduct a business continuity exercise in 2006 for Library employees to relocate to the alternative site. However, there was no documentation of any specific recovery tests that may have been conducted. In addition, there are no documented instructions for staff to follow should they need to relocate to the alternate site.

The Library has performed a risk analysis to assess the criticality of automated systems and to identify application system priorities and critical resources. Although Library staff indicated that there are two mission-critical application systems, only one of the mission-critical systems was listed in the COOP.

Although the Library has a documented COOP, the plan lacks sufficient detail to serve as a business continuity plan. The COOP is not sufficiently tailored to the Library's operating environment and business functions. Essentially, the Library needs to develop a more detailed business continuity plan that will provide sufficient guidance to enable recovery of essential Library operations and research capabilities. The business continuity plan should address both the State House and alternate operational sites.

Recommendation

The George Fingold Library should develop a business continuity plan and enhance the current Continuity of Operations Plan (COOP) to include instructions necessary for recovery of business operations at an alternate operations site. We recommend that the business continuity plan and COOP be formally reviewed, tested to the degree possible, and approved. The Library should ensure that the plans are reviewed periodically, or upon major changes to the Library's IT resources or operating environment. Should changes be required to the plans, the changes should be formally reviewed and approved, and tested to the degree possible.

The plans should include detailed staff instructions to cover various disaster recovery scenarios. We recommend that recovery responsibilities be clearly identified and that contact information be specified for all Library employees, contact personnel at the alternate site, the Information Technology Division (ITD), and vendors. The business continuity plan should identify required resources and ensure that instructions are in place to acquire equipment needed to regain operations at the alternate site, such as computers, printers, scanners, fax machines, etc., and to access office space for Library staff. The business continuity plan, in addition to addressing continuing operations, should provide contingencies for accessing hardcopy books, documents, and reports in the event of a disaster.

The business continuity plan should identify requirements for IT capabilities and application systems. The plan should identify the overall disaster recovery strategy to be executed by ITD to assist the Library in regaining business operations. The plan should also identify specific IT-related processes or procedures that Library staff need to perform, if any. Understandably, recovery of business operations and access to IT capabilities will require a coordinated effort on the part of the Library and ITD.

Auditee's Response

> *The State Library of Massachusetts will follow the recommendations from the Office of the Auditor and develop a business continuity plan to update our Continuity of Operations Plan (COOP). The State Library of Massachusetts intends to update its COOP to reflect Executive Order 490. The updated plan will detail how the Library intends to provide services to the public from remote locations in the event of a disaster.*

Auditor's Reply

We acknowledge the Library's goal to update its Continuity of Operations Plan for business continuity and document its planned efforts to provide services to the public from designated remote locations. Once viable recovery and continuity plans are in place, they should be periodically reviewed and tested to provide an adequate degree of assurance of their continued viability. We recommend that Library staff be trained with respect to business continuity responsibilities.