

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. 2008-0054-4T

**OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS
PERTAINING TO
BUSINESS CONTINUITY PLANNING FOR
MASSACHUSETTS REHABILITATION COMMISSION**

May 22, 2007 through July 16, 2010

**OFFICIAL AUDIT
REPORT
OCTOBER 19, 2010**

TABLE OF CONTENTS

INTRODUCTION	1
---------------------	----------

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	2
---	----------

AUDIT CONCLUSION	4
-------------------------	----------

AUDIT RESULTS	5
----------------------	----------

Business Continuity Planning

APPENDICES

I	Executive Order 144	10
II	Executive Order 475	12
III	Executive Order 490	15
IV	Continuity Planning Criteria	19
V	References	21

INTRODUCTION

The Massachusetts Rehabilitation Commission (MRC) is authorized under Chapter 6, Section 7A, of the Massachusetts General Laws, and is placed under the Executive Office of Health and Human Services. The Commission is staffed by approximately 740 employees under the direction of a full-time Commissioner of Rehabilitation. Three hundred forty of the Commission's employees are direct-service counselors. Oversight and guidance are provided by an Advisory Council of 14 members who serve without compensation. The MRC operates from one administrative office, 27 area offices, and five district offices located in various cities and towns throughout the Commonwealth. The Commission's mission statement is as follows:

MRC promotes equality, empowerment and productive independence of individuals with disabilities. These goals are achieved through enhancing and encouraging personal choice and risk-taking for independence and employment. The Massachusetts Rehabilitation Commission provides comprehensive services to people with disabilities that maximizes their quality of life and economic self-sufficiency in the community.

MRC's primary objective is to provide its clients with an array of comprehensive services that help to maximize their quality of life and enable them to become economically self-sufficient. Specific programs to assist the MRC's clients include, but are not limited to, the Disability Employment Project (DEP), Independent Living Project (ILP), Rehabilitation Services (RS), Support Housing Program (SHP), Minorities Disabilities Support Program (MDSP), Personal Care Assistance (PCA), and a statewide Head Injury Program.

The Commission's business operations are supported by an IT configuration consisting of a local area network that is comprised of eight file servers and more than 400 desktop computers at its central office in Boston, as well as 26 additional servers throughout the state, serving approximately 15,766 active consumers. The Commission is connected to the Commonwealth's wide area network, MAGNet, which requires access to the Massachusetts Information Technology Center in Chelsea. MRC's operations are totally funded by the federal government; however, the Commission operates under the laws and regulations of the Commonwealth.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, from March 31, 2008 through July 16, 2010 and April 8, 2010 through July 16, 2010, we performed an audit of selected information technology (IT) related controls regarding disaster recovery and business continuity planning at the Massachusetts Rehabilitation Commission (MRC) for the audit period of May 22, 2007 through July 16, 2010. The scope of our audit was to assess the extent to which MRC had addressed business continuity planning for business operations supported by technology and had in place adequate on-site and off-site storage of backup copies of magnetic media. Our audit included an assessment of the agency's capabilities to restore critical applications and related business processes and efforts to partner with the Information Technology Division (ITD) for business continuity support.

Audit Objectives

We sought to evaluate whether an effective business continuity plan had been developed and that adequate resources would be available to provide reasonable assurance that mission-critical and essential business operations would be efficiently recovered should IT operations be rendered inoperable or inaccessible for an extended period of time. We determined whether the business continuity plan had been tested and reviewed and approved to provide reasonable assurance of the plan's viability. In this regard, our objective was to also assess whether backup copies of electronic application systems and data files were being generated and stored at secure on-site and off-site locations.

Because MRC is dependent upon ITD's Massachusetts Information Technology Center (MITC) for application systems that support budgetary and human resources functions, we sought to determine whether MRC and ITD had collaborated on identifying IT recovery requirements and had developed appropriate business continuity plans. We sought to identify the degree of assistance provided by ITD to help MRC develop viable business continuity plans and to provide alternate processing and backup storage facilities and recovery plans to ensure timely restoration of MRC's data files and systems supported by MITC.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and performing a preliminary review of documentation concerning business contingency and disaster recovery planning at MRC. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

We interviewed senior management to obtain an understanding of the internal control environment, primary business functions, and stated controls. We obtained an understanding of the Commission's mission-critical functions and application systems by requesting, obtaining, and reviewing agency documentation as well as interviewing business process owners for contingency planning and IT staff, which support IT functions for the agency. Documentation was requested but not limited to the agency's plans for the continuation of agency operations, such as Continuity of Operations Plans (COOPs), Continuation of Government (COG), Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP). We also interviewed ITD staff members that were assigned business continuity planning responsibilities to determine the extent of DRP/BCP services provided to the MRC. In addition, we determined whether MRC was complying with Executive Order No. 490, issued September 26, 2007.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included Executive Orders 144, 475, and 490; 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

Regarding disaster recovery and business continuity planning at the Massachusetts Rehabilitation Commission (MRC), we determined that although documentation of the strategies for recovering information technology (IT) capabilities under MRC's charge needed to be strengthened, there is a reasonable likelihood that MRC would be able to resume mission-critical business operations, but possibly not within an acceptable time period. We determined that although MRC had established a disaster recovery and business continuity framework with documented roles and responsibilities, MRC was unable to submit an approved formal disaster recovery plan from its vendor, CBE Technologies, or a business continuity plan. The Commission could experience delays given that disaster recover and business continuity plans for IT resources need to be more detailed.

We believe that MRC could reduce the risk of failing to resume business functions supported by technology within an acceptable time period by developing and approving more comprehensive recovery plans and ensuring that all staff members responsible for instituting the recovery plans are adequately trained. We found that MRC's continuity of operations and government plans contained multiple characteristics of disaster recovery and business continuity planning; however, MRC does not presently have an approved or tested formal disaster recovery plan or business continuity plan. Because of this, MRC is not in compliance with Executive Order No. 490, which requires annual documented training and exercises of all approved recovery plans.

Regarding backup processing, MRC creates an ongoing mirror image of the critical applications (MRCIS, CS Database, and MRCNET) to the Commission's alternate site in Worcester. MRC's contractor CBE Technologies performs an annual disaster recovery test to support the servers at the Worcester site. On-site, backups are performed daily and weekly on magnetic tapes, which are kept securely in fireproof safes. In addition, MRC does not have any applications or backup copies of data residing at the Massachusetts Information Technology Center (MITC) in Chelsea; however, MRC relies on the Information Technology Division (ITD) at MITC to utilize the state's wide area network, MAGNet, as well as MassMail.

In regards to MITC, ITD performs an annual disaster recovery test at the out-of-state vendor-supported Sungard facility in New Jersey; however, the recovery testing is limited to only a portion of the application systems supported at the center. In addition, the state does not have an alternate state-owned processing and backup facility for the systems operated at MITC. At the time of our audit, ITD was in the process of attempting to establish a second data center as an alternate site in western Massachusetts, which would greatly benefit the agencies under the Executive Office of Health and Human Services, including MRC.

AUDIT RESULTS

Business Continuity Planning

We determined that the Massachusetts Rehabilitation Commission (MRC) had a high-level continuity of operations plan (COOP) and a continuity of government plan (COG) containing multiple elements of business continuity and disaster recovery planning. However, MRC did not have a formal documented business continuity plan (BCP) or disaster recovery plan (DRP). Planning for a disaster can have many steps or phases in order to minimize the impact on clients. A COOP is a high-level documented strategy for executives planning agency continuation of operations. A BCP is more detailed and should encompass a disaster recovery plan and user area plans. MRC should work with the Information Technology Division (ITD) to develop a formal approved documented Business Continuity Plan / Disaster Recovery Plan that is tested at least annually.

The Commission's business operations are supported by an IT configuration consisting of a local area network that is comprised of eight servers and more than 400 desktop computers at its central office in Boston, as well as 26 additional servers throughout the state, serving approximately 15,766 active consumers. We found that MRC had appropriate environmental protection controls in place over its IT environment. For example, MRC's server room in Boston was well maintained and had fire detection and suppression equipment, backup air-conditioning, and a building-supplied backup generator. We also found that physical security controls were generally adequate over areas housing IT resources.

MRC owns, develops, and maintains all of its application systems. The Commission has performed a risk assessment and determined that the mission-critical and essential applications are MRCIS, CS Database, and the Commission's intranet (MRCNET). There are ten additional databases that contain client information throughout the state. If IT capabilities were lost, MRC would need to restore processing within 48 hours.

MRC has designated the Worcester office as its alternate processing and backup site in the event an emergency or disruption of service renders the Boston office inoperable or uninhabitable. The alternate site is large enough to accommodate all critical personnel within 12 hours and contains proper equipment, software, and telecommunication systems to sustain a disaster for up to 30 days. In addition, MRC contracts vendor services with CBE Technologies to support server failure using the application Double-Take. If any of MRC's servers were rendered inoperable, Double-Take can immediately switch to the servers at the Worcester office without being delayed or losing any data. The procedure is tested annually to ensure its viability.

Regarding on and off-site backup procedures, MRC creates an ongoing mirror image of the critical applications to the Commission's alternate site in Worcester. On-site, backups are performed daily and weekly on magnetic tapes, which are kept securely in fireproof safes.

State agencies have been required to perform and 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 (see Appendices I, II, and III) 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 that "Each secretariat and agency shall conduct activities on a quarterly basis that support the implementation of its Continuity of Government and Continuity of Operations plans and shall submit a quarterly report" and "Each secretariat and agency shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice Continuity of Operations plans." 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."

Business continuity plans should be tested to validate their viability and to reduce both the risk of errors and omissions as well as the time needed to restore computer operations. In addition, an effective recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios that would render IT systems inoperable. Specifically, the plan should identify how essential services would be provided in each scenario without the full use of the data processing facility, and the manner and order in which processing resources would be restored or replaced. Furthermore, the plan should identify the policies and procedures to be followed, including details of the logical order for restoring critical data processing functions, either at the original site or at an alternate site. The plan would also identify and explain the tasks and responsibilities necessary to transfer and safeguard backup magnetic copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, support the need for comprehensive and effective backup procedures and business continuity plans for organizations that depend on technology for information processing. Contingency planning should be viewed as a process to be incorporated within an organization, rather than as a project completed upon the drafting of a formal documented plan. Since the criticality of systems may change, a process should be in place that will identify a change in criticality and amend the contingency plans accordingly. System modifications to IT equipment configurations and user requirements should be assessed in terms of their impact to existing business continuity plans. (See Appendix IV for additional criteria.)

Recommendation

We recommend that the Massachusetts Rehabilitation Commission strengthen its business continuity process by developing and maintaining appropriate recovery strategies to regain mission-critical and essential processing within acceptable time periods. We also recommend that MRC further develop and test in conjunction with ITD a more comprehensive and formal business continuity plan that incorporates a disaster recovery plan. MRC needs to ensure that the business continuity plan documents recovery strategies with respect to various disaster scenarios, and contains all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. In addition, MRC should develop detailed user area plans to document contingencies and the steps to be followed to continue business operations to the extent possible should IT resources be unavailable. We recommend that all recovery and continuity planning documents be available in hardcopy and electronic media and stored off-site in secure and accessible locations. As part of disaster recovery planning, MRC should test the viability of its alternate processing site. After the plan has been tested, MRC should document the results of the test and evaluate the scope and results of the tests performed.

MRC should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans. MRC should specify who should be trained in the implementation and execution of the plans under all emergency conditions and who will perform each required task to fully implement the plans. Furthermore, the completed business continuity and user area plans should be distributed to all appropriate staff members. We recommend that MRC's IT personnel be trained in their responsibilities for recovering business operations in the event of an emergency or disaster, including training on manual procedures to be used when processing is delayed for an extended period of time.

In conjunction with ITD, MRC should establish procedures to ensure that the criticality of systems is evaluated, business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the automated systems, and appropriate business continuity plans are developed for

the applications residing on MRC's regional servers and the servers at MITC. As part of business continuity planning, MRC should incorporate a strategy in which the Commission collaborates with the Division of Capital Asset Management in the event that an additional alternate processing site is needed to ensure the continuity of operations. The finalized version of MRC's business continuity plan should also incorporate its vendor CBE Technologies DRP.

We recommend that the Commission follow Executive Order No. 490 for continuity of operations and business continuity planning. Included in this order are requirements for each secretariat and agency to conduct activities to support its Continuity of Government and Continuity of Operations plans. The executive order also requires agencies to conduct training and submit an annual report on the detailed plans to the Executive Office of Public Safety and Security. We also recommend that MRC continue working with ITD on business continuity and disaster recovery planning.

Auditee's Response

The Massachusetts Rehabilitation Commission plans to add the following information to the MRC COOP as an addendum:

- 1. Current EHS and MRC COOP plans call for relocation of our network servers and applications to Chelsea, at the MITC,*
- 2. The MRC COOP details our use of the Worcester Area Office located at 359 Main Street, Worcester, MA 01608 in the event of closure of our AO office. Our managers and supervisors have been instructed to have available contact information for staff so that employees can be reached with alternate assignments.*
- 3. Many of the program staff frequently work outside their assigned office as part of their jobs. This work would not be affected by denial of access to AO. Key staff in MRC programs have VPN access so can reach electronic files at AO, including access to our Enterprise Systems MRCIS and the CS Database.*
- 4. In the event of a long term loss of access to AO, staff, will be reassigned to other locations. The MRC has two area offices within reach by the MBTA (Roxbury and Somerville) for temporary assignment of programs.*
- 5. Employee contact lists for re-assignments as may be used as needed. Managers will work with IT staff to assure access for employees at remote locations.*

Auditor's Reply

While the Massachusetts Rehabilitation Commission's addendum to the COOP is a necessary addition, more detailed procedures would enhance the plan to provide guidance on the actions to be taken. A business continuity plan should contain detailed instruction on the actual procedures to be used for the

successful restoration of MRC's business processes. Development and maintenance of a viable business continuity plan would include training and testing of the recovery plan at least annually. The plan should be provided to all employees involved in the restoration and backed up in both electronic media and hard copy to be stored off-site in a secondary location. Until the business continuity plan is finalized and tested, the Massachusetts Rehabilitation Commission remains vulnerable to interruption of services.

COMMONWEALTH OF MASSACHUSETTS

By His Excellency

MICHAEL S. DUKAKIS

Governor

EXECUTIVE ORDER NO. 144

(Revoking and superseding Executive Order No. 25)

WHEREAS, it is the responsibility of the Commonwealth of Massachusetts to preserve the health and welfare of its citizens in the event of emergencies or disasters by insuring the effective deployment of services and resources; and

WHEREAS, such emergencies or disasters may result from enemy attack or by riot or other civil disturbances, or from earthquakes, hurricanes, tornados, floods, fires, and other natural causes; and

WHEREAS, the experience of recent years suggests the inevitability of natural disasters and the increasing capability of potential enemies of the United States to attack this Commonwealth and the United States in greater and ever-growing force; and

WHEREAS, the effects of such emergencies or disasters may be mitigated by effective planning and operations:

NOW, THEREFORE, I, Michael S. Dukakis, Governor of the Commonwealth, acting under the provisions of the Acts of 1950, Chapter 639, and in particular, Sections 4, 8, 16 and 20 thereof, as amended, and all other authority conferred upon me by law, do hereby issue this Order as a necessary preparatory step in advance of actual disaster or catastrophe and as part of the comprehensive plan and program for the Civil Defense of the Commonwealth.

1. The Secretary of Public Safety, through the State Civil Defense Director, shall act as State Coordinating Officer in the event of emergencies and natural disasters and shall be responsible for the coordination for all activities undertaken by the Commonwealth and its political subdivisions in response to the threat or occurrence of emergencies or natural disasters.

2. This coordination shall be carried out through and with the assistance of the Massachusetts Civil Defense Agency and Office of Emergency Preparedness, as provided under the Acts of 1950, Chapter 639, as amended.

3. Each secretariat, independent division, board, commission and authority of the Government of the Commonwealth (hereinafter referred to as agencies) shall 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.

Each agency shall make appropriate plans for carrying out such emergency responsibilities as may be assigned in this Order or by subsequent Order of the Governor and for rendering such additional emergency assistance as the Secretary of Public Safety and the Civil Defense Agency and Office of Emergency Preparedness may require.

4. The responsibility for such planning shall rest with the head of each agency, provided that such agency head may designate a competent person in the service of the agency to be and act as the Emergency Planning Officer of the Agency. It shall be the function of said Emergency Planning Officer to supervise and coordinate such planning by the agency, subject to the direction and control of the head of the agency, and in cooperation with the Secretary of Public Safety and the State Civil Defense Agency and Office of Emergency Preparedness.

5. Each agency designated as an Emergency Response Agency by the Director of Civil Defense shall assign a minimum of two persons to act as liaison officers between such agency and the Civil Defense Agency and Office of Emergency Preparedness for the purpose of coordinating resources, training, and operations within such agency.

To the extent that training and operational requirements dictate, the liaison officer shall be under the direction and authority of the State Civil Defense Director for such periods as may be required.

6. A Comprehensive Emergency Response Plan for the Commonwealth shall be promulgated and issued and shall constitute official guidance for operations for all agencies and political subdivisions of the Commonwealth in the event of an emergency or natural disaster.

Given at the Executive Chamber in Boston this 27th day of September in the Year of Our Lord, one thousand nine hundred and seventy-eight, and of the independence of the United States, the two hundredth and third.

MICHAEL S. DUKAKIS
Governor
Commonwealth of Massachusetts

PAUL GUZZI
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS



MITT ROMNEY
GOVERNOR

KERRY HEALEY
LIEUTENANT GOVERNOR

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE DEPARTMENT
STATE HOUSE • BOSTON 02133
(617) 725-4000

BY HIS EXCELLENCY

MITT ROMNEY
GOVERNOR

EXECUTIVE ORDER NO. 475

**Mandating Continuity of Government and Continuity of Operations Exercises
within the Executive Department**

WHEREAS, the security of the Commonwealth is dependent upon our ability to ensure continuity of government in the event of a terrorist attack, natural disaster, or other emergency;

WHEREAS, effective preparedness planning requires the identification of functions that must be performed during such an emergency, the assignment of responsibility for developing plans for performing those functions, and the assignment of responsibility for developing the capability to implement those plans;

WHEREAS, to accomplish these aims, the Governor directed each secretariat within the executive department to develop a Continuity of Government Plan identifying an official line of succession for vital positions; prioritizing essential functions which should continue under all circumstances; designating an alternate command site; and establishing procedures for safeguarding personnel and resources;

WHEREAS, the Governor also directed each secretariat and agency within the executive department to develop a Continuity of Operations Plan establishing emergency operating procedures; delegating specific emergency authority to key personnel; establishing reliable, interoperable communications; and providing for the safekeeping of critical systems, records, and databases;

WHEREAS, one hundred and two Continuity of Government and Continuity of Operations plans have been developed by the Office of the Governor and every secretariat and agency within the executive department;

WHEREAS, these Continuity of Government and Continuity of Operations plans have been submitted to and remain on file with the Massachusetts Emergency Management Agency and are ready to be put into operation in the event of a terrorist attack, natural disaster, or other emergency;

WHEREAS, to achieve a maximum state of readiness, these plans have been incorporated into the daily operations of every secretariat and agency in the executive department;

WHEREAS, each executive department agency with critical functions has exercised its Continuity of Operations plan and tested its alert and notification procedures, emergency operating procedures, and the interoperability of communications and information systems; and

WHEREAS, each secretariat has exercised its Continuity of Government plan, and tested its ability to prioritize and deliver essential functions, operate at an alternate facility, and implement succession plans and delegations of authority in an emergency; and

WHEREAS, these regular exercises will continue to ensure that vulnerabilities in the Continuity of Government and Continuity of Operations plans are identified, reviewed, and corrected, and will help to secure an effective response by each secretariat and agency in the event of a terrorist attack, natural disaster, or other emergency;

NOW, THEREFORE, I, Mitt Romney, Governor of the Commonwealth of Massachusetts, by virtue of the authority vested in me as Supreme Executive Magistrate, do hereby order as follows:

Section 1: Each secretariat and agency within the executive department shall continue to consider emergency preparedness functions in the conduct of its regular operations, particularly those functions which would be essential in a time of emergency.

Section 2: Each secretariat within the executive department shall conduct activities on a quarterly basis that support the implementation of its Continuity of Government and Continuity of Operations plans and shall submit a quarterly report to the Executive Office of Public Safety detailing the actions taken to implement these plans.

Section 3: Each agency within the executive department shall conduct activities on a quarterly basis that support the implementation of its Continuity of Operations plan and shall submit a quarterly report to the Executive Office of Public Safety detailing the actions taken to implement such plan.

Section 4: 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 submitted Continuity of Government and Continuity of Operations plans.

Section 5: Each agency 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 submitted Continuity of Operations plan.

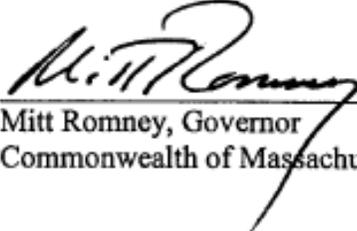
Section 6: These trainings and exercises shall be designed to simulate emergency situations which may arise, and shall be designed to test the effectiveness of the various components of the Continuity of Government and Continuity of Operations plans. These exercises must, at a minimum, include transfer of command functions to an emergency relocation site and the use of emergency communication systems.

Section 7: Each secretariat within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Government and Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these plans. Likewise, each agency within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Operations plan, and based on these findings, shall regularly, and in no event less than once per calendar year, update its Continuity of Operations plan. These plans shall be submitted to and remain on file with the Massachusetts Emergency Management Agency. In addition, the Executive Office for Administration and Finance shall submit a quarterly report to the Executive Office of Public Safety on the status of its review of executive department communication and information systems.

Section 8: The Executive Office of Public Safety shall submit an annual report to the Office of the Governor regarding the status of the Continuity of Government plan of each secretariat within the executive department, and the status of the Continuity of Operations plan of each secretariat and agency within the executive department.



Given at the Executive Chamber in Boston this 3rd day of January in the year of our Lord two thousand and seven and of the Independence of the United States, two hundred and thirty.


Mitt Romney, Governor
Commonwealth of Massachusetts


William Francis Galvin
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS



THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE DEPARTMENT
STATE HOUSE • BOSTON 02133
(617) 725-4000

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

By His Excellency

DEVAL L. PATRICK
GOVERNOR

EXECUTIVE ORDER NO. 490

**Mandating Preparation, Review, Updating, and
Electronic Management of Continuity of Government and
Continuity of Operations Plans**

Revoking and Superseding Executive Order No. 475

WHEREAS, the security and well-being of the people of the Commonwealth depend on our ability to ensure continuity of government;

WHEREAS, effective preparedness planning requires the identification of functions that must be performed during an emergency and the assignment of responsibility for developing and implementing plans for performing those functions;

WHEREAS, to accomplish these aims each secretariat within the executive department was directed to develop a Continuity of Government plan identifying an official line of succession for vital positions, prioritizing essential functions, designating alternate command sites, and establishing procedures for safeguarding personnel and resources; and each secretariat and agency within the executive department was directed to develop a Continuity of Operations Plan establishing emergency operating procedures, delegating specific emergency authority to key personnel, establishing reliable, interoperable communications, and providing for the safekeeping of critical systems, records, and databases;

2007 SEP 27 AM 10:54
OFFICE OF THE GOVERNOR
EXECUTIVE DEPARTMENT

WHEREAS, Continuity of Government and Continuity of Operations plans have been developed by the Office of the Governor and every secretariat and agency within the executive department and all one hundred and two of these plans are currently stored in paper form at the Massachusetts Emergency Management Agency;

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;

WHEREAS, to allow greater access to these plans, ensure their security and sustainability, and encourage more active participation and review by the secretariats and agencies, they should be maintained on a secure online database; and

WHEREAS, the Executive Office of Public Safety and Security and Massachusetts Emergency Management Agency are collaborating with the Information Technology Department to develop an online tool and database to maintain these Continuity of Government and Continuity of Operations plans;

NOW, THEREFORE, I, Deval L. Patrick, Governor of the Commonwealth of Massachusetts, by virtue of the authority vested in me by the Constitution, Part 2, c. 2, § 1, Art. I, do hereby revoke Executive Order 475 and order as follows:

Section 1. Each secretariat and agency within the executive department shall continue to consider emergency preparedness functions in the conduct of its regular operations, particularly those functions which would be critical in a time of emergency.

Section 2. The Secretary of Public Safety and Security (hereinafter, "the Secretary"), in his discretion, shall designate secretariats and agencies as either critical or non-critical for the purpose of determining the detail, frequency of submission, and testing of Continuity of Government and Continuity of Operations plans.

Section 3. The Secretary shall notify all secretariats and agencies of the completion of the online Continuity of Operation / Continuity of Government tool and database (hereinafter, "the online tool"). Within 120 days of notification of completion of the online tool, each secretariat and agency shall submit, via the online tool, the appropriate Continuity of Government plan and/or Continuity of Operations plan based upon its critical or non-critical designation.

Section 4. If the Secretary designates a secretariat or agency as critical, then that secretariat or agency shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice its submitted Continuity of Government and Continuity of Operations plans.

Section 5. These trainings and exercises shall be designed to simulate emergency situations which may arise, and shall be designed to test the effectiveness of the various components of the Continuity of Government and Continuity of Operations plans. These exercises must, at a minimum, include transfer of command functions to an emergency relocation site and the use of emergency communication systems.

Section 6. Each designated critical secretariat within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Government and Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these plans using the online tool. Likewise, each designated critical agency within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Operations plan, and based on these findings, shall regularly, and in no event less than once per calendar year, update its Continuity of Operations plan using the online tool. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security detailing the trainings and exercises conducted and the actions taken to incorporate the findings of such trainings and exercises into updated Continuity of Government and Continuity of Operations plans.

Section 7. Each non-critical agency within the executive department shall conduct activities on an annual basis that support the implementation of its Continuity of Operations plan, including but not limited to ensuring that the plan is current and viable, and shall regularly, and in no event less than once per calendar year, update these plans using the online tool. In addition, each non-critical agency shall submit an annual report to the Executive Office of Public Safety and Security detailing the actions taken to implement such plan.

Section 8. The Executive Office of Public Safety and Security shall submit an annual report to the Office of the Governor regarding the status of the Continuity of Government plan of each secretariat within the executive department, and the status of the Continuity of Operations plan of each secretariat and agency within the executive department.

Section 9. This Executive Order shall continue in effect until amended, superseded, or revoked by subsequent Executive Order.

Given at the Executive Chamber in Boston this 26th day of September in the year of our Lord two thousand and seven, and of the Independence of the United States of America two hundred and thirty-one.



DEVAL L. PATRICK
GOVERNOR
Commonwealth of Massachusetts

WILLIAM FRANCIS GALVIN
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS

Continuity Planning Criteria

The Office of the State Auditor created this document to provide a guideline for planning and establishing a business continuity process to ensure necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercises, rehearsals, tests, training, and maintenance.

Continuity planning efforts will determine an organization's business readiness to recover from an emergency or interruption to normal business processing. These efforts require the creation and maintenance of a documented business continuity plan (BCP) to ensure effective and efficient recovery and restoration of business functions or services – including paper documents, electronic data, technology components, and telecommunications recovery. The BCP must detail all processes, procedures, activities and responsibilities executed during a disaster, or emergency, or an interruption to the organization's products or services.

Our evaluation criteria is a compilation of the above Standards, Guidelines and Objectives developed by the following recognized organizations:

- Contingency Planning & Management (CP&M - National Organization)
<http://www.contingencyplanning.com/>
- DRII Disaster Recovery Institute International (DRII - International Organization)
<http://www.drii.org/DRII>
- IT Governance Institutes' Control Objectives for Information [related] Technology (COBIT); Control Objectives Document, Delivery & Support Section (DS4).
- Department of Homeland Security - Continuity Of Operations Project Guidance documents (COOP).
- [Presidential Decision Directive-67](#) (requires all Federal agencies to have viable COOP capabilities) and Comm. Of Mass. Executive Order No. [144](#) from Governor Michael S. Dukakis in 1978 (requires all state agencies to prepare for emergencies/disasters, and to provide liaisons to Massachusetts Emergency Management Agency for coordinating resources, training, testing and operations), and
- Comm. of Mass. Executive Order No [475](#) from Governor Mitt Romney in 2007, and
- Comm. of Mass. Executive Order No [490](#) from Governor Deval L. Patrick in 2007.

Our criteria is summarized in the following items:

1. Creation of a Business Continuity Plan and Business Continuity Team, comprised of a Business Continuity Manager (BCM), and alternate, for managing the Continuity Program (creation, modifications, updates, test exercises, etc.); Team Leaders, and alternates (from each business unit) to coordinate all continuity aspects for their particular areas of business.

2. Awareness Continuity Training should be given to all employees (minimum of twice annually).
3. Identification and prioritization of all critical/essential business functions (called Risk Analysis, and Business Impact Analysis). A Risk Analysis assigns a criticality level. A Business Impact Analysis identifies the Recovery Time Objective (RTO) - when the applications/systems restoration is needed - most important for critical/essential functions. Analyses should be documented within the BCP. Executive Management must review and sign-off on: analyses, BCP, and test exercise results.
4. Offsite Storage Program - protection of critical data, materials, or media. Document location address and contact name (during business and off hours). Identify authorized individual(s) to retrieve offsite data. Document offsite access procedures.
5. Identify all resources to support critical business functions, alternate site, technology, software, applications, data, personnel, access, transportation, and vendors needed. Workload swaps, split operations, work at home, employee family (need) services.
6. Name(s) authorized to declare a disaster and execution of BCP, and establish. Command Center, Assembly/Holding Areas, Fire/Police/Rescue notification, Site Emergency Personnel (Fire Marshals, security, building evacuations, EMT).
7. Notification Lists and Procedures (employees, legal, Public Relations, support groups, vendors, clients).
8. Establish a strategy for communicating with all affected parties (release of approved and timely information, Senior manager, Officer-in-charge, Media, and company representative).
9. Document a plan for coordinating with interdependent departments (SLA).
10. Implement a plan to recover and restore agency's functions (for RTO, RPO) – at least, yearly test exercises.
11. Document a plan for reestablishing normal business operations (back to original site).

References

803 CMR 3.05 Sections 1 and 2

Chapter 6, Sections 167-178B of the Massachusetts General Laws

Chapter 6, Section 178C-178P, of the Massachusetts General Laws

Chapter 11, Section 12, of the Massachusetts General Laws

Chapter 15A, Section 5, of the Massachusetts General Laws

Chapter 93H of the Massachusetts General Laws

Chapter 82 of the Acts of 2007

Chapter 647 of the Acts of 1989

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Comptroller General of the United States

Control Objectives for Information and Related Technology (version 4.1)

Criminal Offender Record Information (CORI)

EOHHS 101 Code of Massachusetts Regulations (CMR) 15.00-15.16

Executive Orders Nos. 490, 491, and 504

Generally Accepted Government Auditing Standards (GAGAS)

Human Resources Compensation Management System (HR/CMS)

Information Systems Audit and Control Association (ISACA)

Massachusetts Management Accounting and Reporting System (MMARS)

Office of the Secretary of State

Office of the State Auditor

Operational Services Division

State Comptroller-Internal Control Guidelines

U.S. Government Accountability Office