

A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

TEL. (617) 727-6200

No. 2008-1414-4T

**OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY CONTROLS
PERTAINING TO
BUSINESS CONTINUITY PLANNING FOR
THE OPERATIONAL SERVICES DIVISION**

November 1, 2007 through December 14, 2007

**OFFICIAL AUDIT
REPORT
JUNE 30, 2008**

TABLE OF CONTENTS

INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	2
AUDIT CONCLUSION	4
AUDIT RESULTS	5
Business Continuity Planning	5
APPENDIX	
I Executive Order 144	9
II Executive Order 475	11
III Executive Order 490	14
IV Continuity Planning Criteria	18

INTRODUCTION

The Operational Services Division (OSD) operates under Chapter 731 of the Acts of 1989, as amended, and is responsible for the cost-effective purchasing and contracting of equipment, supplies, and certain services for all executive branch departments, agencies, and commissions. OSD was formerly known as the Department of Procurement and General Services until the agency name was changed by Chapter 151 of the Acts and Resolves of 1996. The Division is the largest single purchaser for the executive branch. The agency's mission statement states:

OSD administers the procurement process by establishing statewide contracts for goods and services that ensure best value, provide customer satisfaction and support the socio-economic and environmental goals of the Commonwealth and by providing specific operational services.

In pursuit of its goals, OSD provides through a vendor the Commonwealth's Procurement Access and Solicitation System (COMM-PASS) that provides public access to all interested parties at no cost. COMM-PASS provides a single point of contact for procurement in Massachusetts through the Internet whereby cities, towns, and other public entities can post contract opportunities, and businesses interested in providing commodities or services to the Commonwealth can search over 2500 contracts for free.

OSD has a total of 19 servers that agency data applications are being processed on. There are 14 file servers at One Ashburton Place and five file servers at the Massachusetts Information Technology Center (MITC) in Chelsea. The Uniform Financial Report (UFR eFile) for financial report filings by Human Service Providers' production and training applications are located at MITC, and E-Track, the Office of Vehicle Management's fleet tracking and management system, is located at One Ashburton Place.

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 Operational Services Division (OSD) for the audit period of November 1, 2007 through December 14, 2007. The scope of our audit was to assess the extent to which OSD had addressed business continuity planning for business operations including an assessment of on-site and off-site storage of backup media. Our audit included an assessment of the Information Technology Division's (ITD) efforts to partner with and to support OSD's Business Continuity Plans, and to facilitate the agency's critical applications and systems restoration processes.

Audit Objectives

We sought to evaluate whether an effective business continuity and contingency plan had been implemented to provide reasonable assurance that IT operations could be regained within an acceptable period should a disaster cause computerized operations to become inoperable for an extended period of time. In this regard, our objective was also to assess whether off-site storage for backup copies of LAN and microcomputer-based applications and data files was being created.

Since OSD is dependent upon the Massachusetts Information Technology Center (MITC), we sought to determine the degree of collaboration between OSD and the Information Technology Division (ITD) to support the selection of a second data center to act as an additional processing facility and backup facility for the current primary center located in Chelsea, Massachusetts, and to ensure timely restoration of OSD's data files and systems.

Audit Methodology

To determine the audit scope and objective, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, and reviewing documented disaster recovery and business continuity planning at OSD. We also performed a high-level risk analysis and assessed the strengths and weaknesses of internal controls for ITD's development of a second data center to support OSD's recovery efforts. Upon completion of our pre-audit work, we determined the scope and objectives of this audit.

To determine the audit scope and objective, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review, and documentation concerning business continuity planning. We interviewed senior management to obtain an understanding

of their internal control environment, primary business functions, and stated controls. We obtained an understanding of the Division's mission-critical functions and application systems.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States 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

Regarding system availability, our review indicated that, although OSD had identified an alternate processing site, controls pertaining to disaster recovery and business continuity planning needed to be strengthened. We found that OSD did not have comprehensive documented plans to address disaster recovery and business continuity for automated operations. Planning for a service outage can have many steps or phases in order to minimize the impact on clients. A Continuity of Operations Plan (COOP) is a high level of strategy for executives planning agency continuation of operations. A Business Continuity Plan (BCP) is more detailed and should encompass user area plans and a disaster recovery plan.

Although we found through interviews and a review of OSD's COOP that OSD had certain procedures in place in the event of a major disaster or emergency, OSD had not formally documented these procedures in a business continuity strategy and comprehensive user area plan that would address a loss of IT processing capabilities. Although OSD indicated that they would rely on an alternate processing site starting in 2009 to recover critical information, OSD does not currently have formally documented user area plans that would identify courses of action for staff to follow under various disaster or emergency scenarios. We determined that the procedures regarding the generation of backup copies of magnetic media at a secure off-site location were adequate for mission-critical applications processed through OSD and would aid in recovery efforts. However, in the event of an outage at One Ashburton Place, the 14 OSD servers located there would need to be replaced and replicated. In the event of an outage at the Massachusetts Information Technology Center (MITC), the five OSD servers and their associate applications housed at MITC would not be available until OSD completes working with ITD on disaster recovery planning initiatives. Should the services provided by OSD become unavailable, the Commonwealth may be unable to procure needed services or goods in a disaster situation when time to deliver goods or services would be most critical.

AUDIT RESULTS

Business Continuity Planning

Our audit revealed that although the Operational Services Division (OSD) has a high level Continuity of Operations Plan (COOP) in place, efforts for detailed business continuity plans and disaster recovery plans need to be strengthened to be sufficiently comprehensive to ensure timely restoration of OSD's systems, including the COMM-PASS application. Although the COOP was last updated on October 10, 2007, OSD did not have adequate plans for restoring critical information in the event of a major disaster.

OSD administers the Commonwealth's procurement process by establishing statewide contracts for goods and services that ensure best value, provide customer satisfaction, and support the socio-economic and environmental goals by providing specific operational services. Should the services provided by OSD become unavailable, the Commonwealth could be hampered in procuring needed services or goods in a disaster situation when time to deliver the goods or services would be the most critical.

According to OSD's survey form, OSD has a server room of approximately 600 square feet with backup air conditioning located at One Ashburton Place. However, there is no backup generator for the server room. OSD has a total of 19 servers, 14 of which are located at One Ashburton Place and five of which are located at the Massachusetts Information Technology Center (MITC). The applications located at MITC are UFR, E-Track, and various production and training applications. COMM-PASS is OSD's only vendor-supplied application. Clients would be impacted immediately if COMM-PASS, E-Track, or UFR were rendered inoperable. If IT capabilities were lost, the restoration of Internet access is most important to OSD, followed by security systems, processing systems, and finally phone access.

OSD keeps backup copies of application systems and data files on tapes, which have been used to restore processing capabilities in the past, at Central Reprographics in Charleston, MA. Currently, Central Reprographics also functions as the alternate cold processing site for OSD should One Ashburton Place be rendered inoperable. According to the MIS Director, OSD is also developing an alternate processing site that they hope to complete by 2009, located in Lancaster, MA. This facility is where OSD could relocate if One Ashburton Place were unavailable. In addition, as of July 1, 2008, all tapes will be sent to a vendor's facility, Iron Mountain, for offsite storage. Although OSD is currently working with ITD to develop a Business Continuity Plan, they are not yet working on a Disaster Recovery Plan.

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 make plans for the continuation of government services. In 1978, Executive Order No. 144 mandated the head of each agency within the Commonwealth to "... make appropriate plans for the 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 may be required on an emergency basis. In January 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 plan.” In September 2007, Executive Order No. 490, which superseded Executive Order 475, 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... and... 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 and the time needed to restore computer operations. In addition, an effective plan should provide specific instructions for various courses of action to address different types of disaster scenarios. Specifically, the plan should identify the ways in which essential services would be provided without 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, 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 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 the functions of an 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 and amend the contingency plans accordingly. System modifications, changes to IT equipment configurations, and user requirements should be assessed in terms of their impact to existing business continuity plans (see Appendix IV for other criteria).

Recommendation

We recommend that the Operational Services Division establish a business continuity process to develop and maintain appropriate recovery strategies to regain mission-critical and essential processing within acceptable time periods. We further recommend that OSD develop, document, and test a business continuity plan. Once completed, OSD should develop, document, and test a disaster recovery plan in conjunction with ITD. The business continuity plan should document OSD's recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames. At a minimum, OSD should develop user area plans to continue its operations should the mainframe, file server, or microcomputer systems be unavailable. A copy of these plans should be stored off-site in a secure and accessible location. As part of disaster recovery planning, OSD needs to identify and make viable an alternate processing hot site. The hot site should have a similar operating system so that the system software will be accessible for usage in the case of emergency in order to implement the disaster recovery plan. After the plan has been tested, OSD should evaluate the scope of the tests performed and document the results of the test.

OSD should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans and 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. Further, the completed business continuity and user area plans should be distributed to all appropriate staff members. We recommend OSD's IT personnel be trained in their responsibilities in the event of an emergency or disaster. Also, personnel should be made aware of manual procedures that are to be used when processing is delayed for an extended period of time.

In conjunction with ITD, OSD 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 the OSD's servers in Boston, and the servers at MITC. OSD must also collaborate with ITD to identify and implement an alternate processing site to ensure continuity of operations.

We recommend that OSD adhere to all executive orders for continuity of operations and business continuity planning. We also recommend that OSD continue working with ITD on business continuity and disaster recovery planning.

Auditee's Response

The Operational Services Division (OSD) takes business continuity and disaster recovery seriously, and has already begun to take steps to address the Audit Conclusions in your report. OSD plans to work with the Information Technology Division (ITD) on a long-term Disaster Recovery Plan, and has been working with ITD since the fall of 2007 in preparing Business Impact Analyses, confirming essential functions, critical systems and vital records, and in developing an IT Assessment. OSD is continuing these efforts and is now moving into the Gap and Strategy phase with ITD, to be followed by working sessions and the development of detailed business continuity plans.

At the same time, OSD has contracted with Iron Mountain for Off Site Backup services at their state-of-the-art facility starting July 1, 2008. We believe this will further ensure we can obtain data in the event of a catastrophic event. Along with this, OSD has leased a facility in Lancaster, Massachusetts on the DCAM campus, to act as an Emergency Relocation Site in the event that Ashburton Place or OSD Offices are unavailable. In 2009, we will be working to ready the facility to house emergency systems and staff.

Auditor's Reply

We are pleased that OSD management is reviewing the risks associated with its business continuity objectives and is taking steps to address these risks. In that regard, it is important that the Division conduct adequate business impact analysis for its IT-enabled business processes. Understandably, business continuity planning on the part of the Division should be coordinated with the business continuity planning and disaster recovery efforts of the Information Technology Division.

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.

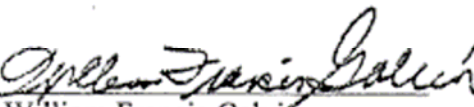
Section 7: Each secretariat within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Government and Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these 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



DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE DEPARTMENT

STATE HOUSE • BOSTON 02133

(617) 725-4000

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;

2008 SEP 27 AM 10:54
OFFICE OF THE
GOVERNOR

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 Office 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.

A handwritten signature in black ink, appearing to read "Deval Patrick", written over a horizontal line.

DEVAL L. PATRICK
GOVERNOR
Commonwealth of Massachusetts

A handwritten signature in black ink, appearing to read "William Francis Galvin", written over a horizontal line.

WILLIAM FRANCIS GALVIN
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS

Continuity Planning Criteria

The goal of this document is 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. 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) authorize 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, Pub. 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).