

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. 2008-0004-4T

**OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY CONTROLS
PERTAINING TO
BUSINESS CONTINUITY PLANNING FOR
THE EXECUTIVE OFFICE OF ELDER AFFAIRS**

October 19, 2007 through November 4, 2008

**OFFICIAL AUDIT
REPORT
MARCH 11, 2009**

TABLE OF CONTENTS

INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	2
AUDIT CONCLUSION	4
AUDIT RESULTS	6
Business Continuity Planning	
APPENDICES	
I. Executive Order 144	11
II. Executive Order 475	13
III. Executive Order 490	16
IV. Continuity Planning Standards	20

INTRODUCTION

The Executive Office of Elder Affairs (EOEA) is an authorized agency under Chapter 19A of the Massachusetts General Laws, which shall be under the supervision and control of a Secretary of Elder Affairs. The Office's mission statement reads as follows:

The Executive Office of Elder Affairs promotes the independence and well being of elders and people needing medical and social supportive services by providing advocacy, leadership, and management expertise to maintain a continuum of services responsive to the needs of our constituents, their families, and caregivers.

EOEA is comprised of four operational divisions - the Office of Finance and Administration, the Office of Program Management, the Office of Policy Development, and the Office of the Secretary. The EOEA has approximately 86 employees and volunteers, and oversees 27 non-profit area and regional agencies, administering 96 elder affairs programs to provide support services to an estimated 225,000 active clientele.

EOEA relies on IT resources located at its offices and at the Massachusetts Information Technology Center (MITC) in Chelsea to assist in carrying out its mission by providing IT processing support. The agency does not have its own data center or server room since EOEA's LAN servers are located at the Executive Office of Health and Human Services. The Information Technology Division (ITD) at MITC, as well as Harmony Information Systems which is located in Vermont, provides application services and support. ITD also supports the Massachusetts Management Accounting and Reporting System (MMARS), MassMail, and Human Resources Compensation Management Systems (HRCMS) applications, and Harmony supports a six-part web-based case management system (SAMS) that provides services to EOEA's Senior Information Management System (SIMS). All client information is contained within the SAMS program, which is available 24 hours a day. Iron Mountain, an off-site backup storage and retrieval service provider, backs up the Harmony data. In addition, Harmony also keeps backup copies of applications and data on-site in Vermont.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, from March 10, 2008 through November 4, 2008, we performed an audit of selected information technology (IT) related controls regarding disaster recovery and business continuity planning at the Executive Office of Elder Affairs (EOEA) for the audit period of October 19, 2007 to November 4, 2008. The scope of our audit was to assess the extent to which EOEA 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's (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 EOEA 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 EOEA 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 EOEA develop viable business continuity plans and to provide alternate processing and backup storage facilities and recovery plans to ensure timely restoration of EOEA's data files and systems supported by MITC.

Audit Methodology

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 contingency and disaster recovery planning at EOEA. 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 their internal control environment, primary business functions, and stated controls. We obtained an understanding of the Department'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 (COOP's), Continuation of Government (COG), Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP). We also interviewed ITD staff that was assigned business continuity planning responsibilities to determine the extent of DRP/BCP services provided to the EOE. In addition, we determined whether EOE was in compliance with Governor Patrick's Executive Order No. 490 issued September 26, 2007.

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 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 Executive Office of Elder Affairs (EOEA), we determined that although documentation of the strategies for recovering information technology (IT) capabilities under EOEA's charge needed to be strengthened, there is a reasonable likelihood that EOEA would be able to resume mission-critical business operations. However, we determined that although EOEA had established a disaster recovery and business continuity framework with documented roles and responsibilities, the Office could experience delays given that business continuity plans for IT resources were undocumented. Although EOEA's main applications are either on the web or at MITC, and since EOEA does not manage their own data center or servers, it appears that EOEA does not need a disaster recovery plan (DRP). However, development of a business continuity plan (BCP) would be advantageous since EOEA is dependant upon service providers for IT support for their applications. A business continuity plan should be developed that would outline how EOEA staff would integrate EOEA's strategies into the DRPs of their service providers or what steps would be undertaken if one or more elements of the DRPs were unable to be completed.

We believe that EOEA could reduce the risk of failing to resume business functions supported by technology under their charge by developing more comprehensive recovery plans, ensuring that all staff having recovery responsibilities are adequately trained, designating an alternative processing site for central office operations, and approving and implementing a business continuity plan. In addition, the disaster recovery plans of EOEA's service provider, Harmony Information Systems, and EOEA's business continuity plans need to be effectively tested to ensure continued viability for the agency. At the time of our review, EOEA was not in compliance with Executive Order 490 that requires annual training and exercises of all recovery plans.

At the time of the audit, EOEA did not have an approved and tested BCP, however EOEA did have a continuity of operations plan (COOP). In addition, the Executive Office of Health and Human Services had developed a continuation of government (COG) plan for the agencies within the executive office, including EOEA. Documentation received from EOEA included a DRP of their service provider, Harmony Information Systems. Included in the plan are steps required of EOEA that have not yet been tested.

In addition, although ITD performs an annual disaster recovery test at the out-of-state Sungard facility in New Jersey, the recovery testing is limited to a portion of the application systems supported at the Massachusetts Information Technology Center (MITC). At the time of the audit, the state did not have

an alternative processing facility owned by the Commonwealth for systems operated at MITC. However, ITD was in the process of attempting to establish a second data center as an alternate processing and backup site in western Massachusetts.

AUDIT RESULTS

Business Continuity Planning

We determined that the Executive Office of Elder Affairs had a continuity of operations plan (COOP), and continuation of government (COG) plan. However, EOEA did not have a formal documented agency-wide recovery plan for restoring information technology (IT) resources should a major event or disaster render IT services inoperable or inaccessible. EOEA is dependant upon Harmony Information Systems, which is located in Vermont, and ITD for providing disaster recovery services for EOEA's applications.

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 continuation of agency operations. A BCP is more detailed and should encompass a disaster recovery plan and user area plans.

EOEA oversees 27 non-profit regional Agency Services Access Points (ASAP) and Area Agencies on Aging (AAA) throughout the state. These ASAPs and AAAs administer a myriad of elder services (home care, health care, transportation, etc.) to 225,000 active clients.

EOEA does not have a data center or server room, or any servers on-site. The Massachusetts Information Technology Center (MITC), Software Technologies, Inc. (STI), and Harmony Information Systems (Harmony) provide application services and support. MITC supports basic statewide applications (MMARS, MassMail, HR/CMS, etc.) and STI supports a six-part module web-based case management system (SAMS) that provides services to EOEA's Senior Information Management System (SIMS). All client information is contained within the case management system. The SAMS/SIMS application is available 24 hours a day. In addition, Harmony also keeps backup copies of applications and data on-site in Vermont.

Since all application support is provided off-site, there is no need for EOEA to provide disaster recovery planning for on-site telecommunications and network functions. However, the agency does have notification contact lists for ASAP representatives in the event of emergencies. Additionally, the SAMS/SIMS application has the capability to broadcast notifications to ASAP personnel.

The service provider, Harmony, has recently completed a continuity plan for systems that it supports, but there have not been any recovery test exercises conducted to date. The service provider's plan is to employ a portable data center that would be delivered from Canada. The expected turnaround time to activate this portable data center is approximately 48 hours. EOEA would need to begin their disaster recovery processing within 24 hours of an emergency.

Recovery processing for the Boston office would deploy employees to their homes, whereby they would begin manual procedures of critically required functions, such as utilizing web applications and telephone communications, with regional offices. The ASAP regional offices have inter-agency agreements for alternate site recovery and continued processing. ASAPs have inter-office email, but no direct connection to the Boston office.

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 the head of each agency within the Commonwealth to “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 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 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 and 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 for 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 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 other criteria.)

Recommendation

We recommend that the Executive Office of Elder Affairs strengthen its 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 EOEA develop and test a comprehensive and formal business continuity plan that incorporates the disaster recovery plans of ITD, EOHHS and Harmony Information Systems. The business continuity plan should document EOEA's recovery strategies with respect to various disaster scenarios. The business continuity plan should contain all pertinent information needed to effectively and efficiently recover critical business operations within the needed time frames. At a minimum, EOEA should develop user area plans to continue business operations to the extent possible should IT resources be unavailable. A copy of these plans, in both hardcopy and electronic media, should be stored off-site in secure and accessible locations. As part of disaster recovery planning, EOEA should test the viability of their alternate processing site. After the plan has been tested, EOEA should document the results of the test and evaluate the scope and results of the tests performed.

EOEA should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans. EOEA 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 EOEA'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, EOEA 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 Harmony's servers and the servers at MITC.

We recommend that the Executive Office follow Executive Order No. 490 for continuity of operations and business continuity planning. Included in this executive 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 EOEa continue working with ITD and Harmony on business continuity and disaster recovery planning.

Auditee's Response

Below please find information pertaining to EOEa's DR plan for the SIMS System and our internal Business Continuity plan. As you may recall during your visit, we discussed the fact that the SIMS application (Senior Information Management System) is essentially EOEa's and its 27 statewide provider networks' system of record for case management of elders receiving services across the Commonwealth. This is an ASP (Active Service Page) web application that is hosted in Burlington VT. in a secure and certified facility. This application can be accessed anywhere with the correct login criteria and a standard internet connection. As part of our DR Agreement with our vendor, Harmony Information Systems, Harmony is required to perform an annual Active System Test Plan and bi-annual Passive System Test Plan (s). (Please note, the details of the actual tasks that will be preformed are listed in the DR plan under Appendix W – Plan Testing. 87. that was given to you along with our COOP and COG plans during our initial visit.

EOEa's SIMS system 1st scheduled Passive test date is January 26th, 2009. This bi-annual exercise will take place at our vendor's site and will result in a detailed accounting of what the results of the testing exercise may have revealed.

Regarding our discussion on Business Continuity, the group that is tasked with putting the finishing touches on ELD's Business Continuity Plan has a scheduled meet on January 22, 2009. The goal of this meeting will be to review and assign a final list of action items that that will allow ELD to put the finishing touches on our Business Continuity plan by April of 2009.

Again, once this final stage of these (2) exercises have been completed we will be happy to share them with you and your team.

Auditor's Reply

We are pleased that EOEA took timely action starting in January 2009 to begin addressing the disaster recovery and business continuity planning. It is important to ensure that security risks are adequately addressed for web-based applications when operating under a recovery scenario, such as EOEA's mission-critical Senior Information Management System. We suggest that EOEA's vendor's January 26, 2009 test results be incorporated into the EOEA disaster recovery and business continuity planning process.

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.

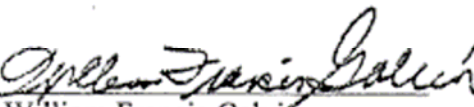
Section 7: Each secretariat within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Government and Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these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

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. Off-site 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 off-site data. Off-site 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).