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. 2008-0236-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY PERTAINING TO BUSINESS CONTINUITY PLANNING FOR THE DEPARTMENT OF MENTAL HEALTH

September 29, 2006 through October 8, 2008

OFFICIAL AUDIT REPORT
DECEMBER 3, 2008

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Department of Mental Health (DMH), established by Chapter 19, Section 1, and operating under Chapter 123, Sections l through 36B, of the Massachusetts General Laws, promotes mental health through early intervention, treatment, education, policy, and regulation so that all residents of the Commonwealth may live full and productive lives. DMH currently serves approximately 27,000 adults, adolescents, and children through an array of inpatient and community-based services, including residential, case management, and rehabilitation support.

The Department is organized into six geographic areas that are managed by Area Directors. Each area is divided into local service sites that provide case management and oversee integrated systems of state and vendor-operated adult and child/adolescent mental health services. In addition to the Commissioner's Office located in Boston, DMH has three other divisions, which include Program Operations, Clinical and Professional Services, and Management and Budget. The Department coordinates planning, sets and monitors attainment of broad policy and standards, and performs certain fiscal, personnel, and legal functions. Some specialized programs, including forensic mental health services, the child and adolescent inpatient units, and intensive residential treatment programs, are managed centrally. The Department's mission statement reads as follows:

> *The Department of Mental Health, as the State Mental Health Authority, assures and provides access to services and supports to meet the mental health needs of individuals of all ages, enabling them to live, work and participate in their communities. The department establishes standards to ensure effective and culturally competent care to promote recovery. The department sets policy, promotes self-determination, protects human rights and supports mental health training and research. This critical mission is accomplished by working in partnership with other state agencies, individuals, families, providers and communities. DMH sets the standards for the operation of mental health facilities and community residential programs and provides clinical, rehabilitative and supportive services for adults with serious mental illness, and children and adolescents with serious mental illness or serious emotional disturbance.*

DMH relies on information technology to manage information and provide services to its clients. DMH's technology includes a wide area network (WAN) that connects their six regional local area networks (LAN) to provide processing for 5,000 employees at 32 sites, including three hospitals and 29 community health centers. In addition, DMH provides electronic access for 25 court clinics. Of the application systems used by DMH, the Department has identified the Meditech system, which is a medical client database, as its mission-critical application for agency operations. The Department also uses the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management Systems (HR/CMS) for financial accounting and human resources

management. Both of these application systems, which are accessed through the Commonwealth's WAN, reside on file servers located at the Massachusetts Information Technology Center (MITC). The Meditech application system consists of a medical client database having system modules that support the functions of referral or the acceptance of inpatient, community, or child adolescents; clinical practice and forensic evaluations; and billing and accounts receivable. Meditech modules also provide management information for community programs, census, medical records, providers, and contract management.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, from February 1, 2008 through October 8, 2008, we performed an audit of selected information technology (IT) related controls regarding disaster recovery and business continuity planning at the Department of Mental Health (DMH) for the audit period of September 29, 2006 through October 8, 2008. The scope of our audit was to assess the extent to which DMH 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 DMH is dependent upon ITD's Massachusetts Information Technology Center (MITC) for operating the Meditech application system and other application systems that support budgetary and human resources functions, we sought to determine whether DMH 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 DMH develop viable business continuity plans and to provide alternate processing and backup storage facilities and recovery plans to ensure timely restoration of DMH'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 as well as performing a preliminary review and documentation concerning business contingency and disaster recovery planning at DMH. We obtained a high-level understanding of the Department's IT environment and identified mission-critical application systems. 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 who support IT functions. Documentation was requested, but not limited to the Department'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 who were assigned business continuity planning responsibilities to determine the extent of DRP and BCP services provided to the DMH. In addition, we determined whether DMH was in compliance with Governor Patrick's Executive Order # 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 Department of Mental Health (DMH), we determined that although documentation of the strategies for recovering information technology (IT) capabilities under DMH's charge needed to be strengthened, there is a reasonable likelihood that DMH would be able to resume mission-critical business operations, but not always within an acceptable time period. We determined that, although DMH had established a disaster recovery and business continuity framework with documented roles and responsibilities, the Department could experience delays because that disaster recovery plans (DRPs) for IT resources needed to be more detailed.

DMH could reduce the risk of not resuming 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 the disaster recovery and business continuity plans. In addition, disaster recovery and business continuity plans need to be effectively tested to ensure continued viability. At the time of our review, DMH was not in compliance with Executive Order 490 that requires annual training and exercises of all recovery plans.

Although DMH has been working with the Information Technology Division (ITD) on developing a business continuity plan (BCP), DMH did not have an approved and tested BCP or DRP. At the time of the audit, DMH had draft versions of various regional office continuity of operations plans (COOP), as well as numerous documents containing multiple characteristics of a business continuity plan, including an enterprise data backup plan specifically for the Meditech application. In addition, The Executive Office of Health and Human Services (EOHHS) had developed a continuation of government (COG) plan for the agencies within the executive office, including the Department of Mental Health.

Regarding backup processing, DMH uses a controlled interagency data-backup program called Backup Executive. Tapes are also used for off-site storage, which are kept securely in fireproof safes. On-site, backup copies of application systems and data files are stored on discs. 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 Department of Mental Health (DMH) had a continuity of operations plan (COOP) for various regional offices, as well as elements of a business continuity plan (BCP), disaster recovery plan (DRP), and continuation of government (COG) plan. However, DMH 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. 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 DRP and user area plans.

Regarding the mission-critical Meditech application residing at the Massachusetts Information Technology Center (MITC) in Chelsea, the Department has a draft version of an Enterprise Data Backup Plan for the restoration of related applications, servers, and email programs. The Meditech backup plan is reviewed and tested by the Information Technology Division (ITD) for its adequacy and effectiveness, and updated on a regular basis. If IT resources were rendered inoperable for a period of time greater than 72 hours, including the Meditech application system, the impact to DMH is that up to 27,000 clients could be effected. Since DMH's Meditech client database supports the functions of referral, acceptance, management, census, medical records, providers, contracts, clinical practice, forensic evaluations, and billing and accounts receivable, any disruption in the electronic Meditech system would force DMH to resort to an older paper system which could hinder or delay services to clients.

DMH uses a data-backup program called Backup Executive for all application systems not operated on servers or mainframe computers at the Massachusetts Information Technology Center (MITC). Tapes are also used for off-site storage, which are kept securely in fireproof safes. Backup copies of application systems and data files that are generated for on-site availability are stored on discs. According to DMH, they have successfully restored processing capabilities in the past using backup copies of application systems and data files.

Although an intra-agency agreement identifies the regional offices as the alternate processing sites, they have not been tested. DMH has been in contact with ITD regarding alternate processing site services and is currently working with the Division to strengthen its business continuity plan. Since ITD has yet to establish a state-owned second data center to support the backup operations and processing of applications residing at MITC, DMH participates annually in a Meditech application test by ITD at the out-of-state Sungard facility in New Jersey.

DMH has 51 Meditech servers located at MITC. Since DMH's Meditech medical client database supports the functions of referral, acceptance, management, census, medical records, providers, contracts, clinical practice, forensic evaluations, and billing and accounts receivable, any disruption in the electronic Meditech system would force DMH to resort to an older paper system which could hinder or delay services to clients. We acknowledge that as part of the Department's planning process, DMH has documented various planning steps needed to restore systems in their information security handbooks.

Agencies are required to perform and document their planning efforts for the continuity of operations 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 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 plan." In September 2007, Executive Order No. 490 mandated "Whereas, to achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly; ….. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security."

BCPs 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 Department of Mental Health strengthen its business continuity planning process by developing and maintaining appropriate recovery strategies to regain mission-critical and essential processing within acceptable time periods. We further recommend that DMH also develop and test a more comprehensive and formal business continuity plan that incorporates a disaster recovery plan in conjunction with ITD. The business continuity plan should document DMH'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, DMH 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, DMH should test the viability of their alternate processing site. After the plan has been tested, DMH should document the results of the test and evaluate the scope and results of the tests performed.

DMH should specify the assigned responsibilities for maintaining the plans and supervising the implementation of the tasks documented in the plans. DMH 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. Further, the completed business continuity and user area plans should be distributed to all appropriate staff members. We recommend that DMH'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, DMH 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 DMH's regional servers, and the servers at MITC. As part of business continuity planning, DMH should incorporate a strategy in which the Department 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.

We recommend that the Department follow the requirements of 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 that DMH continue working with ITD on business continuity and disaster recovery planning.

Auditee Response

IT Backup Environment and Practices:
DMH has refreshed a substantial share of its environment over the past two years. One element is the backup support. The process was reviewed Auditors and was found to be strong and based on sound industry standards with the exception of our off-site storage practices. DMH does rotate its media off site on a weekly basis, but our previous site practices often moved tapes within the same building, or campus on which the tapes were produced. This was found to be insufficient and DMH agrees. DMH now moves all media for all locations on a weekly rotation to a locked location within DMH AIT control at the Hadley building in Westborough. Media produced at the Hadley location are stored in a locked area at the Westborough State Hospital (building separated by public roads and a number of private properties). The final elements of the plan to be completed:

- *An assessment of the locked storage container for fire retardant and heat retardant status*
- *The storage containers to be used during transport of the media between sites*

DMH will finalize these two remaining elements within the financial capabilities of DMH within this fiscal year.

Business Continuity Planning:
Like all Commonwealth agencies, DMH needs to improve its focus on the Business Continuity needs and planning required to support its users and clients under all circumstances within its responsibilities detailed in Executive Order No. 490 for Continuity of Operations and Business Continuity Planning. DMH AIT has negotiated and agreed to a project

scope for AIT's participation in DMH Business Continuity Planning. DMH AIT will assume responsibility for completing a comprehensive Information Technology Service Continuity Management (ITSCM) Plan. This industry standard is an approach, which insures an organization's ability to continue to provide a pre-determined and agreed level of IT Services to support the minimum business requirements, "Service Continuity". The intent is to then use and include the ITSCM in all site Business Continuity Plans and the greater DMH-wide Business Continuity Plans. The following is the basic plan and timeline for the ISCM.

Overall Process Strategy:

Define direction and high-level methods to meet IT service level objectives

- *Establish generic framework and guidelines for a continuity program, including:*
  - *Management structure & responsibilities*
  - *How to conduct business criticality & risk assessments*
  - *How to define and create an IT Service Continuity plan*
  - *How to rehearse an IT Service Continuity plan*
  - *Solution architectures and design considerations*
  - *Document and include in all site response plans to any area of business continuity or disaster recovery*

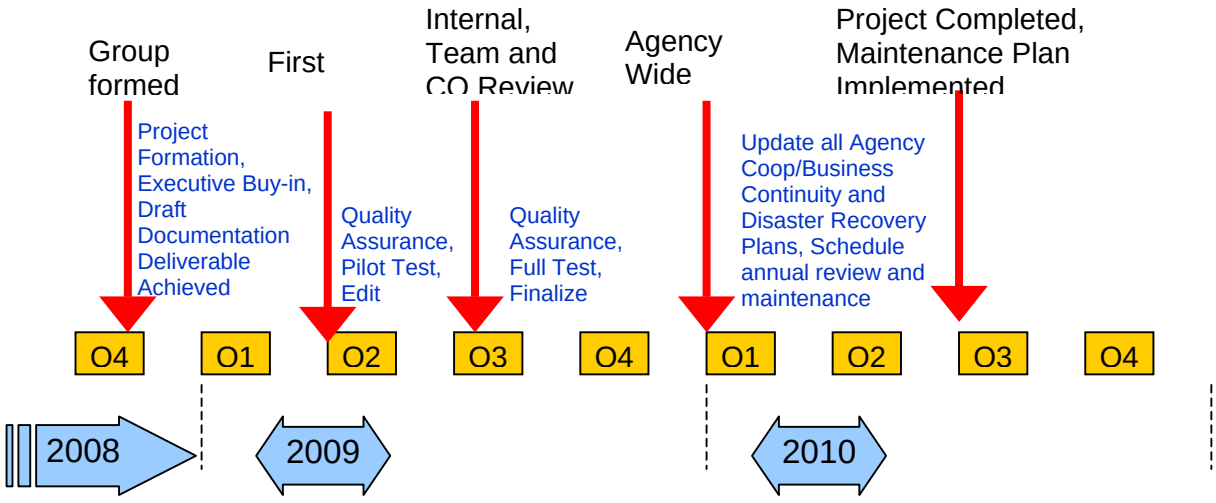
  Agreed at Executive – CO and Area levels

  Needs to consider four stages of major incident
  - *Initial response*
  - *Service recovery*
  - *Service delivery (following incident)*
  - *Normal service resumption*

  Manage and Launch the Process
  - *Identify and document for all of DMH*
  - *Standardize on a state-wide approach*
  - *Build IT disaster recovery and business continuity planning into the design process*
  - *Build incident specific work flows using a standard approach and template*
  - *Standardize all response tasks and documentation requirements*
    - *Detail all services and applications and determine the importance to DMH and a clearly defined order of restoral*
    - *Establish Recovery Objectives (point in them and outage tolerance) for all services and applications*

- *Educate and train – executives, participants and all others at appropriate levels*
  - *Expectations*
  - *Process*
  - *Deliverables*
- *Equip everyone involved appropriately to meet their responsibilities*
- *Build a comprehensive test plan that is exercised to some level quarterly*
- *Test – correct – test again*
- *Deploy the plan for inclusion in ALL Emergency Preparedness/Disaster Recovery/Business Continuity/Area/Site/DMH-wide/Department plans*
- *Participate in non-DMH tests using our tests to gain peer input (example: EOHHS, DPH, ITD testing opportunities*
- *Review and maintain the documentation on a yearly basis (at a minimum)*

Timeline for Information Technology Service Continuity Management Plan



Auditor's Reply

Based on the auditee response above, it appears that DMH has outlined a reasonable process for developing their business continuity and disaster recovery planning framework. While DMH Applied Information Technology will assume responsibility for completing a comprehensive Information Technology Service Continuity Management Plan, final accountability should rest with senior management and business process owners. We acknowledge that two remaining elements have been identified within the IT Backup Environment and Practices section of the auditee response and that a timetable has been established to complete outstanding tasks by the third quarter of 2010. We encourage DMH to ensure that adequate resources are allocated to develop, in a timely manner, viable recovery and contingency strategies.

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 Common wealth (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

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

MITT ROMNEY
GOVERNOR

KERRY HEALEY
LIEUTENANT GOVERNOR

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;

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, § I, 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.

DEVAL L. PATRICK
GOVERNOR
Commonwealth of Massachusetts

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' **C**ontrol **Ob**jectives for **I**nformation [related] **T**echnology (COBiT); Control Objectives Document, Delivery & Support Section (DS4).
- Department of Homeland Security - **C**ontinuity **O**f **O**perations **P**roject 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).