The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DE NUCCI
AUDITOR

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

No. 2010-0064-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS PERTAINING TO BUSINESS CONTINUITY PLANNING FOR THE SOLDIERS' HOME IN HOLYOKE

July 1, 2009 through October 9, 2009

OFFICIAL AUDIT REPORT

FEBRUARY 22, 2010

TABLE OF CONTENTS

INTRODUCTION

Soldiers' Home in Holyoke (SHH) was established under Chapter 6, Sections 70 and 71 of the Massachusetts General Laws and became operational in 1952. The SHH is a state-funded agency under the Executive Office of Health and Human Services and is available to all qualified veterans. SHH has 307 employees and functions as a 305-bed healthcare facility currently housing 285 residents. The Governor has appointed a seven-member board of trustees to oversee the SHH's operational activities to ensure they meet the objectives of their mission statement:

> *The mission of the Soldiers' Home in Holyoke is to provide, with honor and dignity, the highest quality of personal health care services to Massachusetts Veterans. The vision is to be recognized as the health care provider of choice for all Veterans residing in the Commonwealth of Massachusetts.*

The three primary areas of service provided by the Soldiers' Home in Holyoke are acute care, domiciliary care, and long-term care. Other services provided include outpatient care, physical therapy, social services, pharmacy services, spiritual guidance, and dietary services. SHH is fully accredited by The Joint Commission and inspected annually by the Veterans Administration. In addition, SHH in partnership with the Valley Opportunity Council (a local anti-poverty agency), provides case management and marketing of a 14-unit residence for homeless veterans in the City of Holyoke and a six-unit residence in the City of Chicopee. SHH is located on a 17-acre campus consisting of three buildings comprised of 220,000 square feet, including a 275-bed main hospital facility, a 30-bed dormitory residence, and an outside emergency generator building.

SHH's mission-critical application, provided by American Health Care (AHC), enables management and staff to process financial, clinical, and administrative transactions. The AHC application is comprised of six integrated modules that include general ledger, resident census, billing, resident trust, purchasing, and inventory. SHH's local area network (LAN) supports other administrative and patient-related activities including dietary services, medical labs, and the pharmacy. The LAN also provides access to the Massachusetts Management Accounting and Reporting System (MMARS), Human Resources/Compensation Management System (HR/CMS), and the state's information data warehouse.

In fiscal year 2009, SHH received state appropriations in the amount of $20,864,231, and in fiscal year 2010 received an appropriation of $19,803,450.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit at the Soldiers' Home in Holyoke (SHH) for the period of July 1, 2009 through October 9, 2009. The audit was conducted from September 14, 2009 through October 9, 2009 for selected information technology (IT) related controls regarding business continuity and disaster recovery planning.

The scope of our audit was to assess the extent to which SHH had addressed business continuity and disaster recovery planning for business operations supported by IT and if SHH 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 efforts to partner with the Information Technology Division (ITD) with regard to the agency's utilization of business continuity and disaster recovery planning to restore mission-critical applications and related business processes.

Audit Objectives

With respect to the availability of computing system capabilities, we sought to determine whether business continuity and disaster recovery strategies would provide reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible. We also sought to determine whether a business continuity plan (BCP) and disaster recovery plan (DRP) had been tested, reviewed, and approved to provide reasonable assurance of the plans' viability. Our objective was to also assess whether backup copies of computer application systems and data files were being generated and stored at secure on-site and off-site locations. In addition, we sought to determine whether controls were in place and effect to provide reasonable assurance of SHH's compliance with the Department of Homeland Security Headquarters' Continuity of Operations Plan (COOP) and Executive Order No. 490 Electronic Management of Continuity of Government and Continuity of Operations Plans. We also sought to determine whether SHH and ITD had collaborated on identifying IT recovery requirements and had developed appropriate business continuity, disaster recovery, and backup of magnetic media plans with regard to budgetary and human resources application systems that reside at the Massachusetts Information Technology Center (MITC).

Audit Methodology

To determine the audit scope and objective, we conducted pre-audit work that included obtaining and reviewing documentation to gain an understanding of SHH's relevant operations concerning business contingency and disaster recovery planning. 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 SHH's contingency planning concerning its mission-critical functions, application systems, and internal control environment. Documentation was requested but not limited to the agency's plans for the continuation of agency operations, such as its Continuity of Operations Plan (COOP), business continuity plan (BCP), and disaster recovery plan (DRP). In addition, we determined whether SHH was in compliance with Executive Order No. 490, issued September 26, 2007.

Our audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included Executive Orders No. 144, No. 475, and No. 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 Soldiers' Home in Holyoke (SHH), we determined that although documentation of the strategies for recovering information technology (IT) capabilities needed to be strengthened, there is a reasonable likelihood that SHH would be able to resume mission-critical business operations, but possibly not within an acceptable time period. We determined that although SHH had established a disaster recovery and business continuity framework with documented roles and responsibilities, the SHH could experience delays given that business continuity plans (BCP) and disaster recover plans (DRP) for IT resources needed to be more detailed.

Our audit revealed that SHH had in place a Continuity of Operation Plan (COOP) dated July 31, 2009 and other documented control practices requiring an emergency relocation site and emergency notification plans. However, we determined that the individual documents did not provide sufficient recovery strategies to regain business operations in a timely manner should a disaster render computer systems inoperable or unobtainable. To strengthen controls, the agency needs to perform a criticality assessment and risk analysis to develop a strategic comprehensive and tested BCP and DRP that operate in conjunction with the COOP.

Based on the results of our audit, we determined that some internal controls in place at Soldiers' Home in Holyoke provided reasonable assurance that some IT-related activities would be provided in a manner that would meet business objectives. However, our audit revealed that other controls needed to be implemented or strengthened to help ensure that the SHH's IT resources will sufficiently support its computer capabilities, will properly account for software, and provide reasonable assurance that systems will be available when required. In particular, SHH needs to strengthen controls to provide reasonable assurance that critical IT processing operations for administrative functions could be regained quickly and effectively should a disaster render IT systems inoperable. Although we found that SHH had IT policies and procedures and agreements with area facilities, some were found to be outdated and invalid. In addition, we found that SHH could reduce the risk of failing to resume business functions supported by technology within an acceptable time period by ensuring that all staff members having recovery responsibilities are adequately trained.

We found that off-site storage of backup media for the mission-critical American Health Care application was in place and daily/weekly backups of network data are secured in a fireproof vault at an off-site location in the Chiller Building. Although there has been no organized testing for replenishment of IT resources, we determined there is reasonable assurance that SHH could successfully restore losses of files and folders using the backup tapes.

We found that SHH also relies on MITC for access to the Massachusetts Management Accounting and Reporting System (MMARS), MassMail, and the state's wide area network MAGNet. We also determined that with regards to MITC that ITD performs an annual disaster recovery test at the out-of-state vendor-supported SunGard facility in New Jersey; however, the recovery testing is limited to only a portion of the application systems supported at SHH. In addition, the state does not have an alternate state-owned processing and backup facility for the systems operated at MITC. At the time of our audit, ITD is in the process of establishing a second data center as an alternate site in Springfield, Massachusetts, which would greatly benefit the agencies under the Executive Office of Health and Human Services, including SHH.

AUDIT RESULTS

Business Continuity Planning

We determined that the Soldiers' Home in Holyoke (SHH) had a high-level continuity of operations plan (COOP) containing multiple elements of business continuity and disaster recovery planning. However, SHH did not have a formal documented business continuity plan (BCP) or disaster recovery plan (DRP). Planning for a disaster can have many steps or phases in order to minimize its impact on clients. A COOP is a high-level documented strategy for executives planning an agency's continuation of operations. A BCP is more detailed and should encompass a DRP and detailed user area plans. SHH should coordinate with its Secretariat, the Executive Office of Health and Human Services (EOHHS), and the Information Technology Division (ITD) to develop an approved BCP and DRP that is tested at least annually.

SHH's server room is located on the ground floor of the main hospital facility. The server room is approximately 440 square feet, has a single entrance secured by a keypad, and has three servers containing ten non-critical database applications and one mission-critical American Health Care application. We found that the server room had appropriate environmental protection controls in place including fire detection and suppression equipment, backup air conditioning for temperature control, and a backup generator and uninterruptible power supply. We also found physical security controls to be generally adequate. SHH's financial reporting, human resource, and MassMail applications are located at the Massachusetts Information Technology Center (MITC) in Chelsea. At the time of our audit, ITD was engaged in the development of a backup and alternate processing site.

In regards to backup processing, SHH maintains daily/weekly backup copies of applications and data files on media tape stored offsite at the Chiller building, which is located on the SHH campus. The backup tapes are created on a weekly cycle. Although SHH has not restored files and folders using the backup tapes, there is reasonable assurance that backup media would be available as required.

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. Our 2001 audit report and our management letter dated August 10, 1994 to SHH's management included a recommendation that management assess the nature and extent of required disaster recovery and contingency planning. In 1978, Executive Order No. 144 mandated that the head of each agency within

the Commonwealth "make appropriate plans for the protection of its personnel, equipment and supplies (including records and documents) against the effects of enemy attack or natural disaster, and for maintaining or providing services appropriate to the agency which maybe required on an emergency basis." In 2007, Executive Order No. 475 mandated "Each agency within the executive department shall conduct activities on a quarterly basis that support the implementation of its Continuity of Government and Continuity of Operations plan and shall submit a quarterly report…" and "…Each secretariat within the executive department shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice… 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."

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

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

Recommendation:

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

SHH should specify assigned responsibilities for maintaining the plans and identifying the individuals to be trained in the implementation and execution of the plans' tasks under all emergency conditions. Furthermore, the completed business continuity and user area plans should be distributed to all appropriate staff members. We recommend SHH'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 IT processing is delayed for an extended period of time.

In conjunction with EOHHS and ITD, SHH should establish procedures to ensure the criticality of systems are evaluated; business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or computing capabilities; and appropriate business continuity and disaster recovery plans are developed for the applications residing on SHH's servers. As part of business continuity planning, SHH should incorporate a strategy in the event an additional alternate processing site is needed to ensure the continuity of operations.

We recommend that SHH 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.

Auditee Response

The Soldiers' Home in Holyoke substantially agrees with the findings of the OSA and has taken the following steps towards resolving the issues discovered during the audit.

Business Continuity Plan - The IT Department has a good portion of this completed with our current documented policies and procedures. Our agency requires that all approved policies be stored on the "Shared Drive, Everyone, Policies, MIS" for all employees to review. That has been done and is currently updated with new or changed policies. Our shortfall with this is that we currently do not have a "BCP Document" that identifies all of our steps and procedures should they be needed to be put in place. The auditors offered us a website address that has a BCP Format that we could use to develop our document. We will start to develop our BCP getting it reviewed and approved so it can be inserted into the agencies COOP with all of the other departments plans.

Disaster Recovery Plan - As with the BCP our DRP has a good portion in place and operational. The major shortfall cited was because we did not have an off-site location to go to in the event of a disaster. I am going to check with Russ Murray, EHS, CSIO to see what he is planning for in this area for the smaller agencies. With the planning for a second IT Data Center in Springfield, will this site be available in the event of a disaster for the smaller western MASS agencies? With the current and on going budget outlook not too many smaller agencies can afford the cost of an off-site service.

Auditor's Reply

We are pleased that Soldiers' Home in Holyoke is in the process of strengthening and documenting a comprehensive disaster recovery and business continuity plan containing detailed user area procedures. Executive Order No. 490 requires at least annual testing of disaster recovery and business continuity plans and reporting of the test results to the Executive Office of Public Safety and Security. Understandably, testing of the disaster recovery and business continuity plans will provide assurance as to the viability of the plans.

Until such time as the Commonwealth's second data center is online, the Home should identify an alternate processing location to support disaster recovery.

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

MITT ROMNEY
GOVERNOR

KERRY HEALEY
LIEUTENANT GOVERNOR

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

BY HIS EXCELLENCY

MITT ROMNEY
GOVERNOR

EXECUTIVE ORDER NO. 475

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 4: Each secretariat within the executive department shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice its submitted Continuity of Government and Continuity of Operations plans.

Section 5: Each agency within the executive department shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice its submitted Continuity of Operations plan.

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

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

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

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

Mitt Romney, Governor
Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS

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

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

By His Excellency

DEVAL L. PATRICK
GOVERNOR

EXECUTIVE ORDER NO. 490

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

Revoking and Superseding Executive Order No. 475

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

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

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

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. Document offsite access procedures.

5. Identify all resources to support critical business functions, alternate site, technology, software, applications, data, personnel, access, transportation, and vendors needed. Workload swaps, split operations, work at home, employee family (need) services.

6. Name(s) authorized to declare a disaster and execution of BCP, and establish. Command Center, Assembly/Holding Areas, Fire/Police/Rescue notification, Site Emergency Personnel (Fire Marshals, security, building evacuations, EMT).

7. Notification Lists and Procedures (employees, legal, Public Relations, support groups, vendors, clients).

8. Establish a strategy for communicating with all affected parties (release of approved and timely information, Senior manager, Officer-in-charge, Media, and company representative).

9. Document a plan for coordinating with interdependent departments (SLA).

10. Implement a plan to recover and restore agency's functions (for RTO, RPO) – at least, yearly test exercises.

11. Document a plan for reestablishing normal business operations (back to original site).

References

803 CMR 3.05 Sections 1 and 2

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

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

Chapter 11, Section 12, of the Massachusetts General Laws

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

Chapter 93H of the Massachusetts General Laws

Chapter 82 of the Acts of 2007

Chapter 647 of the Acts of 1989

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Comptroller General of the United States

Control Objectives for Information and Related Technology (version 4.1)

Criminal Offender Record Information (CORI)

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

Executive Orders Nos. 490, 491, and 504

Generally Accepted Government Auditing Standards (GAGAS)

Human Resources Compensation Management System (HR/CMS)

Information Systems Audit and Control Association (ISACA)

Massachusetts Management Accounting and Reporting System (MMARS)

Office of the Secretary of State

Office of the State Auditor

Operational Services Division

State Comptroller-Internal Control Guidelines

U.S. Government Accountability Office