OFFICE OF THE GOVERNOR
COMMONWEALTH OF MASSACHUSETTS
STATE HOUSE • BOSTON, MA 02133
(617) 725-4000

DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

By His Excellency

DEVAL L. PATRICK
GOVERNOR

EXECUTIVE ORDER NO. 504

ORDER REGARDING THE SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

(Revoking and Superseding Executive Order 412)

WHEREAS, identity theft is a serious crime that, according to current Federal Trade Commission statistics, affects as many as 9 million Americans each year and costs consumers and businesses approximately $52 billion annually;

WHEREAS, the Commonwealth of Massachusetts has recognized the growing threat of identity theft and taken steps to safeguard the personal information of its residents by, among other things, enacting Massachusetts General Laws Chapter 93H ("Chapter 93H");

WHEREAS, pursuant to Chapter 93H, the Massachusetts Office of Consumer Affairs and Business Regulation has promulgated regulations, effective January 1, 2009, defining security standards that must be met by persons, other than state entities, who own, license, store or maintain personal information about residents of the Commonwealth;

WHEREAS, also pursuant to Chapter 93H, the Secretary of the Commonwealth, through his Supervisor of Public Records, is charged

with establishing rules or regulations designed to safeguard personal information that is owned or licensed by state executive offices and authorities;

WHEREAS, the Executive Department recognizes the importance of developing and implementing uniform policies and standards across state government to safeguard the security, confidentiality and integrity of personal information maintained by state agencies; and

WHEREAS, the implementation of such policies and standards will further the objectives of Chapter 93H and will demonstrate the Commonwealth's commitment to adhere to standards equal to or higher than those that govern the private sector.

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 412 and order as follows:

Section 1. This Executive Order shall apply to all state agencies in the Executive Department. As used in this Order, "state agencies" (or "agencies") shall include all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices, now existing and hereafter established.

Section 2. It shall be the policy of the Executive Department of the Commonwealth of Massachusetts to adopt and implement the maximum feasible measures reasonably needed to ensure the security, confidentiality and integrity of personal information, as defined in Chapter 93H, and personal data, as defined in Massachusetts General Laws Chapter 66A, maintained by state agencies (hereafter, collectively, "personal information"). Each executive officer and agency head serving under the Governor, and all state employees, shall take immediate, affirmative steps to ensure compliance with this policy and with applicable federal and state privacy and information security laws and regulations.

Section 3. All state agencies shall develop, implement and maintain written information security programs governing their collection, use,

dissemination, storage, retention and destruction of personal information. The programs shall ensure that agencies collect the minimum quantity of personal information reasonably needed to accomplish the legitimate purpose for which the information is collected; securely store and protect the information against unauthorized access, destruction, use, modification, disclosure or loss; provide access to and disseminate the information only to those persons and entities who reasonably require the information to perform their duties; and destroy the information as soon as it is no longer needed or required to be maintained by state or federal record retention requirements. The security programs shall address, without limitation, administrative, technical and physical safeguards, and shall comply with all federal and state privacy and information security laws and regulations, including but not limited to all applicable rules and regulations issued by the Secretary of State's Supervisor of Public Records under Chapter 93H.

Section 4. Each agency's written information security program shall include provisions that relate to the protection of information stored or maintained in electronic form (hereafter, "electronic security plans"). The Commonwealth's Chief Information Officer ("CIO") shall have the authority to:

- Issue detailed guidelines, standards, and policies governing agencies' development, implementation and maintenance of electronic security plans;
- Require that agencies submit their electronic security plans to ITD for review, following which ITD shall either approve the plans, return them for amendment, or reject them and mandate the preparation of a new plan;
- Issue guidelines specifying when agencies will be required to prepare and submit supplemental or updated electronic security plans to ITD for approval;
- Establish periodic reporting requirements pursuant to which all agencies shall conduct and submit self-audits to ITD no less than annually, assessing the state of their implementation and compliance with their electronic security plans, with all guidelines, standards, and policies issued by ITD, and with all applicable federal and state privacy and information security laws and regulations;

- Conduct reviews to assess agency compliance with the governing plans, guidelines, standards, policies, laws and regulations. At the discretion of ITD, reviews may be conducted on site or electronically, and may be announced or unannounced;
- Issue policies requiring that incidents involving a breach of security or unauthorized acquisition or use of personal information be immediately reported to ITD and to such other entities as required by the notice provisions of Chapter 93H; and
- Where necessary and appropriate, and with the approval of the Secretary for Administration and Finance, determine and implement remedial courses of action to assist non-compliant agencies in achieving compliance with the governing plans, guidelines, standards, policies, laws and regulations. Such actions may include, without limitation, the imposition of terms and conditions relating to an agency's information technology ("IT")-related expenditures and use of IT capital funding.

Section 5. Each agency shall appoint an Information Security Officer ("ISO"), who may also hold another position within the agency. ISOs shall report directly to their respective Agency heads and shall coordinate their agency's compliance with the requirements of this Order, applicable federal and state laws and regulations, and ITD security standards and policies. All agency security programs, plans, self-audits, and reports required by this Order shall contain certifications signed by the responsible ISO and the responsible agency head attesting to the accuracy and completeness of the submissions.

Section 6. All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided at the time they commence work. Such training shall include, without limitation, guidance to employees regarding how to identify, maintain and safeguard records and data that contain personal information.

Section 7. The Enterprise Security Board ("ESB"), as presently established, shall advise the CIO in developing the guidelines, standards, and policies required by Section 4 of this Order. Consistent with the ESB's current framework, the precise members and make-up of the ESB shall be determined by the CIO, but its membership shall be drawn from state employees across the Executive Department with knowledge and experience in the fields of information technology, privacy and security, together with such additional representatives from the Judicial and Legislative Branches, other constitutional offices, and quasi-public authorities who accept an invitation from the CIO to participate. The ESB shall function as a consultative body to advise the CIO in developing and promulgating guidelines, standards, and policies that reflect best practices to ensure the security, confidentiality and integrity of the electronic personal information collected, stored, used, and disseminated by the Commonwealth's IT resources.

Section 8. The CIO shall develop mandatory standards and procedures for agencies to follow before entering into contracts that will provide third parties with access to electronic personal information or information technology systems containing such information. Such standards must require that appropriate measures be taken to verify the competency and integrity of contractors and subcontractors, minimize the data and systems to which they will be given access, and ensure the security, confidentiality and integrity of such data and systems.

Section 9. All contracts entered into by state agencies after January 1, 2009 shall contain provisions requiring contractors to certify that they have read this Executive Order, that they have reviewed and will comply with all information security programs, plans, guidelines, standards and policies that apply to the work they will be performing for their contracting agency, that they will communicate these provisions to and enforce them against their subcontractors, and that they will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information to which they are given access as part of the contract from unauthorized access, destruction, use, modification, disclosure or loss. The foregoing contractual provisions shall be drafted by ITD, the Office of the Comptroller, and the Operational

Services Division, which shall develop and implement uniform language to be incorporated into all contracts that are executed by state agencies. The provisions shall be enforced through the contracting agency and the Operational Services Division. Any breach shall be regarded as a material breach of the contract that may subject the contractor to appropriate sanctions.

Section 10. In performing their responsibilities under this Order, ITD, the CIO and the Operational Services Division shall have the full cooperation of all state agencies, including compliance with all requests for information.

Section 11. This Executive Order shall take effect immediately and shall continue in effect until amended, superseded or revoked by subsequent Executive Order.

Given at the Executive Chamber in Boston this 19th day of September in the year of our Lord two thousand and eight, and of the Independence of the United States of America two hundred and thirty-two.

DEVAL L. PATRICK
GOVERNOR
Commonwealth of Massachusetts

WILLIAM FRANCIS GALVIN
Secretary of the Commonwealth

GOD SAVE THE COMMONWEALTH OF MASSACHUSETTS