Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report-Issued September 14, 2012

Executive Order 504 Compliance Review Regarding the Security and Confidentiality of Personal Information at Executive Department Agencies

For the period January 1, 2009 through June 30, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

On September 19, 2008, Executive Order 504 (EO504) was issued regarding the security and confidentiality of personal information of residents of the Commonwealth. EO504 requires Executive Department agencies to develop, implement, and maintain written information security plans that govern the collection, use, distribution, storage, retention, and destruction of personal information, including provisions for protecting personal information in both hardcopy and electronic form.

In accordance with Chapter 11, Section 12, of the General Laws, we conducted a performance audit of the progress made by Executive Department agencies in implementing EO504 during the period January 1, 2009 through June 30, 2011. Our audit scope was to assess whether Executive Department agencies adequately addressed the security and reporting requirements of EO504 to ensure the security, confidentiality, and integrity of personal information.

Based on our audit, we have concluded that, except as noted in the Audit Results section, the Commonwealth's Information Technology Division (ITD) made significant progress in addressing the key requirements of EO504 and that Executive Department agencies assigned Information Security Officers (ISOs); provided security training to their staff; developed written information security plans to govern the protection of personal information; and provided reports on the existence and security of personal information under their charge. However, our review found that improvements could be made in state agencies' compliance with EO504 requirements and that an adequate process was not in place to assess the controls that state agencies have established over the safeguarding of personal information.

Our audit indicated that significant progress has been made by Executive Department agencies to meet EO504 reporting requirements. Specifically, we found that ITD provided EO504-related training to agencies, designated reporting requirements, and tracked the submission of agency report filings. Moreover, we noted that most Executive Department agencies designated ISOs, trained agency personnel, inserted terms and conditions in vendor contracts for protecting personal information, identified the existence of personal information in their systems, and submitted required reports and some self-audit questionnaires (SAQs). However, we noted that improvements were needed in several areas, including (a) SAQ filings, (b) communication of management's responsibilities under EO504, (c) the security of hardcopy personal information, (d) consistency in data entry, (e) ITD review of annual agency submissions, (f) identification of personal information use, (g) appointment of ISOs, (h) data classification, (i) security training, (j) vendor contract management, and (k) addressing the impact of Executive Order 510.

Our audit found that although ITD has provided guidance to state agencies for EO504 compliance and has established a central collection point for agency submissions of personal information-related reports and self-audits, adequate internal controls were not in place to provide ITD with reasonable assurance that the personal information being maintained at the state agencies subject to the requirements of EO504 was being adequately protected. As a result, ITD management lacks (1) reliable feedback on the existence and performance of an operational process, activity, or combination of controls and (2) independent review processes to validate agency reports and verify the existence of controls necessary to protect personal information.

INTRODUCTION

Background

Executive Order 504 (EO504), which was issued on September 19, 2008, pertains to an "Order Regarding the Security and Confidentiality of Personal Information" for Massachusetts residents. Section 2 of EO504 states that 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 Law Chapter 66A, maintained by state agencies. 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."

EO504 requires all Executive Department agencies to develop, implement, and maintain written information security plans that govern the collection, use, distribution, storage, retention, and destruction of personal information. Each agency's written information security plan should include provisions for protecting personal information in both hardcopy and electronic form. The security and confidentiality goals of EO504 include improving security awareness and strengthening responsibilities and controls for safeguarding personal information. Based on our audit work, it appears that EO504 has increased the level of awareness of the need to safeguard personal information from unauthorized access and disclosure. Further, it appears that EO504 has focused attention on the need for Executive Department agencies to establish incident response procedures for addressing security breaches regarding the protection of personal information.

Agency responsibilities under EO504 include appointing Information Security Officers (ISOs) who should report directly to their agency heads. ISOs are responsible for coordinating agency compliance with EO504, including adherence to federal and state laws and regulations for privacy and security, Information Technology Division (ITD) enterprise security policies and standards, and contractual security and privacy obligations. The agency head and the ISO are required to certify and submit to ITD an Information Security Program (ISP), an Electronic Security Plan (ESP), and a Self-Audit Questionnaire (SAQ) annually on September 19th.

In addition, EO504 requires all agency heads, managers, supervisors, and employees (including contract employees) to attend mandatory information security training within one year of the effective date of EO504 and states: "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."

EO504 also requires that all contracts dated after January 1, 2009, contain provisions requiring contractors to certify that they have read EO504 and that the "CIO [Chief Information Officer] 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 [IT] systems containing such information." Agencies are required to manage vendors and contractors by verifying that contractors have acceptable security controls to prevent data breaches. In doing so, the agencies are required to follow ITD's mandatory standards for verifying competence and integrity of contractors and subcontractors and to ensure that certifications are incorporated into contracts.

EO504 authorizes the Commonwealth's CIO, who is the agency head of ITD, to issue policies, standards, and detailed guidelines governing agencies' development, implementation, and maintenance of ESPs. The CIO requires agencies to submit their ISPs, ESPs, and SAQs to ITD, which shall approve them, return them for amendment, or reject them and require that new ones be prepared. The CIO is also authorized to establish periodic reporting requirements pursuant to which all agencies shall conduct and submit self-audits no less than annually to ITD, which is responsible for conducting reviews to assess agency compliance with EO504 and applicable federal and state privacy and information security laws and regulations. The CIO is required to 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 other entities as required by the notice provisions of Chapter 93H of the General Laws. In addition, the CIO, where necessary and appropriate and with the approval of the Secretary for Administration and Finance, is required to determine and implement remedial courses of action to assist noncompliant agencies in achieving compliance with the governing policies, standards, guidelines, laws, and regulations.

Audit Scope, Objectives, and Methodology

Our audit scope was to assess whether Executive Department agencies adequately addressed the security and reporting requirements of EO504 to ensure the security, confidentiality and integrity of personal information. The audit covered the period January 1, 2009 through June 30, 2011.

We conducted this performance audit in accordance with applicable generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of our audit were to assess:

- ITD compliance with the requirements that the CIO develop guidelines and standards to direct agencies to identify and evaluate efforts to protect personal information, assign ISOs, conduct self-audits, include appropriate contract language, and report annually on EO504 compliance.
- Agency compliance with filing requirements for ISPs, ESPs, and SAQs; designating ISOs; and training agency management and staff regarding personal information privacy requirements and security measures.
- The extent to which EO504 has assisted state government in implementing and exercising appropriate controls to provide reasonable assurance that personal information as defined under Chapter 93H of the General Laws is safeguarded from unauthorized access and disclosure.

To meet our audit objectives, we reviewed relevant laws, rules, and regulations, as well as instructions issued by ITD for completion and submission of ISPs, ESPs, and SAQs. Specifically, we reviewed EO504 to obtain an understanding of measures that agencies are required to implement to ensure the security, confidentiality, and integrity of personal information. In addition, we reviewed Chapters 66A and 93H of the General Laws, Chapter 647 of the Acts of 1989, 201 Code of Massachusetts Regulations (CMR) 17.00, and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT 4.1) issued by the Information Systems Audit and Control Association in July 2007. To aid in the identification and evaluation of IT controls, we also referred to the Enterprise Information Security Policy and the Enterprise Data Classification Standard from ITD, Information Systems Audit and Control Association's (ISACA's) Guidance to

Achieve Control Objectives for Successful IT Governance, and the International Standards Organization's ISO/IEC 27002 on IT Security Management.

We attended EO504-related training for the on-line database application to support agency submissions for the September 19, 2011 filing date. We reviewed training documentation provided by ITD designed to assist agencies in addressing the requirements of EO504 and for submitting agency documentation on the status of personal information security. Through interviews, documentation, and reviews, we obtained information regarding the status of agency submissions of EO504 documents for the September 19, 2009 and 2010 and filing dates. We obtained filing status information as of the end of the audit period on June 30, 2011 pertaining to the September 19, 2010 filing submissions. Subsequent to the audit period, we obtained filing statistics from ITD regarding the September 19, 2011 filing date.

We interviewed the Commonwealth's CIO, who oversees ITD, Secretariat-level CIOs, state agency level ISOs, and ITD personnel responsible for EO504 support and monitoring. Moreover, we reviewed the steps taken by Executive Department agencies to identify personal information in hardcopy and electronic form, assess the need for personal information for agency operations and business processes, conduct risk assessments of personal information security and the impact of unauthorized disclosure, evaluate the adequacy of controls (policy, procedures, organizational, assurance mechanisms) to protect personal information from unauthorized access and disclosure, and report on the status of personal information data and related controls. We assessed whether agencies had appointed ISOs and whether they reported directly to the agency heads.

Our audit found that the ITD had substantively met EO504 requirements to issue policies, standards, and detailed guidelines for agencies to develop, maintain, and annually report their ISPs and ESPs and to conduct and annually report the results of self-audits of the protection of personal information. To assist agencies, ITD conducted EO504 training sessions and developed a standardized SAQ that incorporated requirements from the Commonwealth's Enterprise Security Policy and generally accepted security practices. Furthermore, ITD established a process to review and approve agency submissions of ISPs, ESPs, and SAQs and to monitor and track agency reporting compliance. ITD also developed an Enterprise Incident Response Policy to be followed by Executive Department agencies and assigned staff with specific responsibilities to support the EO504 compliance process. Some of the tasks completed by ITD include establishing a website;

developing reporting templates and the SAQ; and providing training to address legal requirements, background information, security, and preparation and filing of ISPs, ESPs and SAQs. ITD also established a process to review and track agency submissions of ISPs, ESPs, and SAQs.

However, as discussed in the Audit Results section, our review found that improvements could be made in agency compliance with EO504 requirements and that an adequate process was not in place to assess the controls that state agencies have established over the safeguarding of personal information.

AUDIT RESULTS

1. IMPROVEMENTS NEEDED IN COMPLIANCE WITH EXECUTIVE ORDER 504 REQUIREMENTS FOR THE SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

Our audit indicated that significant progress has been made by Executive Department agencies to meet Executive Order 504 (EO504) reporting requirements. Specifically, we found that the Commonwealth's Information Technology Division (ITD) had provided EO504-related training to agencies, designated reporting requirements, and tracked the submission of agency report filings. Moreover, we noted that most Executive Department agencies designated Information Security Officers (ISOs), trained agency personnel, inserted terms and conditions in vendor contracts for protecting personal information, identified the existence of personal information, and submitted required reports and some self-audit questionnaires (SAQs). However, we noted that improvements were needed in several areas, including (a) SAQ filings, (b) communication of management's responsibilities under EO504, (c) the security of hardcopy personal information, (d) consistency in data entry, (e) ITD review of annual agency submissions, (f) identification of personal information use, (g) appointment of ISOs, (h) data classification, (i) security training, (j) vendor contract management, and (k) addressing the impact of Executive Order 510, as discussed below.

a. SAQ Filings

We found that, for the first-year filing, 79 of the 81 agencies that were being tracked by ITD submitted the required Information Security Programs (ISPs) and Electronic Security Plans (ESPs) and that all but six submitted SAQs by the first year filing deadline of September 19, 2009. However, during the next fiscal year, 40 agencies did not file SAQs by the filing deadline of September 19, 2010. Moreover, we found that, subsequent to our audit period, 35 agencies had not submitted SAQs by the third-year filing deadline of September 19, 2011. (See Appendix I for agency listings.)

b. Communication of Responsibilities

Some agency officials interviewed indicated that they did not know whether the protection of personal information and compliance with EO504 was the responsibility of agency management or ITD. In fact, some such officials indicated that they were concerned that not all management personnel sufficiently understood that the protection of personal information and compliance with EO504 reporting was a management responsibility.

c. Hardcopy Documentation

Although EO504 and the ISPs require protection and reporting of personal information in hardcopy form, the increased emphasis on the role of IT to protect personal information stored electronically may have overshadowed the importance of strong physical security controls over hardcopy documents. For example, agency personnel raised concerns that documents containing personal information are sometimes stored in unlocked file cabinets or boxes, or are left unattended on desks or work spaces within unsecured office areas.

d. Data Entry

We noted that, with respect to the annual submission of EO504 reports, agencies were initially required to submit their ISPs and ESPs within spreadsheets that had been pre-established by ITD. However, ITD and the agencies soon recognized that the initial filings could be very time-consuming and that data input and review of the spreadsheets were cumbersome. As a result, ITD developed an on-line database application that was available in January 2011 for data entry and submitting of EO504 reports and SAQs. The new database application eliminates the data entry and review problems encountered with the large spreadsheets that had been used for the first- and second-year filings. According to ITD staff, although the application system has a reporting capability, including a high-level dashboard for Secretariat level reporting, further enhancement is needed to provide detailed analysis capabilities for security and compliance reporting.

e. ITD Review of Annual Agency Submissions

ITD has established a formal process to track the submission of agency ISP, ESP, and SAQ reports and to conduct desktop reviews to determine whether all required information has been submitted. ITD is authorized under EO504 to review agency-submitted reports for approval, or return them for amendment or rejection. However, our review found that this review process does not include an in-depth analysis or verification of the information contained in the agency reports, including agency statements of compliance with security provisions. In addition, ITD had not determined how the data collected can best be used to monitor compliance and evaluate agency control assessments.

f. Identification of Personal Information Use

EO504 requires agencies to identify their requirements for protecting personal information, report on the use of personal information, and provide controls to safeguard personal information from unauthorized disclosure. The last requirement is achieved by having agencies conduct self-audits and complete an SAQ that is submitted along with the identification of application systems that contain personal information and their related security requirements. However, our interviews with Secretariat Chief Information Officers (SCIOs) revealed that state agencies under their control used different methods of identifying application systems that contained personal information, increasing the possibility that some systems containing personal information may not have been identified. Specifically, we found that, depending on the secretariat and the extent of its IT systems and resources, different data-gathering techniques were employed to identify the use of personal information. For example, some agencies scanned all systems for data that could be personal information, whereas other agencies relied on requesting agency personnel to identify the systems that used personal information. Accordingly, there is inadequate evidence to conclude that effective efforts had been made by Executive Department agencies to properly identify all systems that contained personal data so that these systems could be properly safeguarded against unauthorized disclosure of this information.

g. Appointment of ISOs

Our audit found that, for the first year's September 19, 2009 reporting period, Executive Department agencies complied with the requirement that an ISO be designated for each agency. However, in a limited number of instances, the same person was designated as an ISO for more than one agency. Specifically, five individuals were ISOs of 14 of the 82 Executive Department agencies. We also found that, during the second and third years, there was a significant turnover in ISOs. Although some of the changes in staff assigned as ISOs may have been caused by normal staff reassignments, our interviews with ISOs indicated that many such changes resulted from the consolidation and relocation of IT staff from the agency level to the secretariat level.

Our audit indicated that the appointment of replacement ISOs largely occurred in the absence of a formal transition process, resulting in some of the newly appointed ISOs not being fully aware of the actions taken by prior ISOs or having a sufficient understanding of their EO504 responsibilities. EO504 indicates that the ISO, who is to report directly to the agency head, is responsible for coordinating the agency's compliance with EO504, federal and state laws and

regulations for privacy and security, ITD's enterprise security policies and standards, and contractual security and privacy obligations. Newly appointed ISOs would benefit from a formal transition and training process, since both reporting and compliance requirements require a working understanding of how and where personal information is stored and used, security and confidentiality requirements, breach notification procedures, controls to adequately safeguard hardcopy and electronically based information, and compliance assessment techniques. (Summary results of our interviews with 34 of the 40 agency ISOs for agencies that were delayed in submitting SAQs for the September 19, 2010 filing date are shown in Appendix III.)

h. Data Classification

Data classification is an integral part of data management that provides a foundation for ensuring that appropriate levels of security are established to protect information from unauthorized access and use. It is through data classification that the type and level of sensitivity of individual data elements are defined so that appropriate security schemes can be developed and implemented. Our audit found that although data classification is referenced in the ISP, ESP, and SAQ, there is no guarantee that a uniform methodology would be used by agencies to classify their data. In addition, agency responses to our audit questionnaire (see Appendix III) indicated that 26 of 34 agencies had not completed data classification as required by ITD's data classification standard. Given the importance of the proper management and security of data, increased efforts are needed to implement appropriate data classification methodologies and to ensure that data residing in Commonwealth systems and used by state agencies are uniformly and appropriately classified.

i. Security Training

According to agency documentation, agencies had complied with EO504 requirements that management and staff receive security-related training by September 19, 2009. Although EO504 requires that new hires receive training in the security of personal information, agency responses to the audit questionnaire (see Appendix III) indicated that staff hired after September 2009 had not received this security-related training at 30 of 34 agencies. Effective security training programs ensure that employees clearly understand the responsibilities for securing and maintaining confidentiality of personal information and what must be done to limit, if possible, further exposure should a breach of confidentiality be identified. Because of the size and

complexity of the manual and electronic operations at state agencies containing personal information, training programs are a critical first step in safeguarding personal information.

j. Vendor Contract Management

Under EO504, agencies are required to ensure that agreements with vendors that have access to personal information include terms and conditions to protect this personal information. Agencies are also required to manage vendors and contractors by verifying that the contractors have acceptable security controls to prevent data breaches. In compliance with EO504, ITD, in conjunction with the Office of the State Comptroller and the Operational Services Division, drafted contract language to be included in contracts regarding the protection of personal information. Agencies are to follow ITD's mandatory standards for verifying competence and integrity of contractors and subcontractors and ensure that requirements for certifications are incorporated into contracts. In addition, contractors and subcontractors are required to comply with 201 Code of Massachusetts Regulations (CMR) 17.00 as promulgated by the Office of Consumer Affairs and Business Regulations regarding the protection of personal information.

However, our audit found that the process of ensuring that adequate controls are in place to protect personal information in the custody of state agency contractors and subcontractors relies almost entirely on the contract language designed to address the security over this information and that no actual verification or review of a vendor's administrative, technical, and physical controls over its personal information is performed by state agencies. Although there is merit in requiring that vendor agreements specify the responsibilities to safeguard personal information and to have certifications submitted, neither adequately verifies that adequate controls are in effect.

k. Impact of Executive Order 510

On February 19, 2009, Executive Order 510 (EO510) was issued, which changed the lines of reporting for state agency IT personnel and impacted certain points of accountability. Specifically, EO510 required that IT personnel be transferred from their individual agencies and consolidated to one of the seven executive level offices (e.g., the Executive Office of Health and Human Services, the Executive Office for Administration and Finance). Many of the state agencies that we surveyed indicated that this transfer impacted the degree to which they were able to retain and direct the actions of their staff members who were knowledgeable about their

particular technical controls to protect personal information. They also indicated that the most immediate impact was an initial loss of knowledge at the agency level regarding the specific IT controls that were in place and the degree of their effectiveness, and that the impact was also noticeable where there was a large turnover of ISO positions after the first-year period. Moreover, our survey of agencies that were late in filing their EO504 reports for the second-year filing indicated that some newly appointed ISOs appeared to lack an adequate understanding of EO504 responsibilities (see Appendix III).

Recommendation

In order to improve agency compliance with the requirements of EO504, we recommend the following:

- All agencies delinquent in filing an annual report on personal information security and/or their SAQ should immediately take appropriate action to file the reports with ITD. Given that, as of the end of our audit period, five agencies had not filed any annual SAQs, we recommend that the Commonwealth's CIO consider whether remedial courses of action should be required to assist these non-compliant agencies in fully meeting their EO504 reporting responsibilities.

- ITD should consider modifying the filing requirements under certain circumstances in which the operational responsibility, including IT security, has been transferred outside of the agency; the expertise to assess the effectiveness of IT controls is no longer at the agency; or some of the systems relied upon by the agency are enterprise-based systems used by multiple agencies. In such cases, we recommend that the filing of the agency's ISP, ESP and SAQ be handled as a combined secretariat and agency filing, retaining the required sign-offs by the agency head and agency ISO, but including the Secretary of the respective secretariat and the SCIO.

- ITD should continue to provide an underlying foundation for IT security and the protection of personal information through the development of IT security policies and standards. The information obtained by state agencies that have implemented EO504 in terms of the controls over personal information should be shared with other branches of government and independent authorities to assist them in addressing Chapters 93H and 93I of the General Laws and to help coordinate the protection of personal information across state government.

- Agencies should develop a coordinated security training curriculum to be used as a baseline. Each agency can then tailor its training requirements to reflect its operational environment and technology. At a minimum, the training program should address use of controls; data classification as a means to identify sensitive information; and annual verification of data use, classification, and protection. Annual security awareness training should address compliance with EO504 in support of Chapters 66A, 93H, and 93I of the General Laws and enterprise security policies promulgated by ITD.

- Responsibility and points of accountability for implementing, exercising, and evaluating internal controls to identify and protect personal information and comply with EO504 should be evaluated on an agency and secretariat level, identifying assigned responsibilities, points of accountability, and levels of communication. Further, oversight tasks should be performed to ensure that all personnel having roles and responsibilities for protecting personal information are identified and that appropriate communication and input requirements are established.

- State agencies should establish a formal transition/training process to ensure that individuals being assigned as an agency's ISO understand the knowledge requirements and the role and responsibilities of the position.

- ITD should develop programs that continue to provide guidance to agencies on security methods, controls, and procedures to follow in order to ensure full compliance with EO504.

Auditee's Response:

ITD is in general agreement with the recommendations made by the SAO. Below are specific responses to each recommendation.

ITD will review current filing requirements, and make appropriate changes to address changes in operational responsibility or systems that are used by multiple agencies within a Secretariat. Target Date: August 2012.

EO504 specifically calls out the agency head and the agency ISO as the individuals with the requirement of signing/attesting to any required EO504 submissions. Changing the reporting requirements could require modification of the EO504 document itself.

ITD will continue to evolve IT Security policies and standards in support of the protection of personal information. ITD is committed to share information and collaborate with other branches of government, independent authorities, and municipalities to promote best practices for the protection of personal information. Target Date: Ongoing.

ITD will develop a remedial process to assist non-compliant agencies in meeting their EO504 reporting requirements. Target Date: May 2012.

ITD will make recommended changes to training programs as recommended by SAO. Target Date: June 2012.

ITD will review current practices for assigned roles and responsibilities related to the implementing, exercising and evaluating internal controls related to identification and protection of personal information and compliance with EO504. ITD will develop a formal training protocol for newly assigned agency Information Security Officers. Target Date: To be determined.

2. LACK OF ADEQUATE ASSURANCE PROGRAM TO VERIFY CONTROLS FOR SAFEGUARDING PERSONAL INFORMATION

Our audit found that although ITD has provided guidance to state agencies for EO504 compliance and has established a central collection point for agency submissions of personal information-related

reports and self-audits, adequate internal controls were not in place to provide ITD with reasonable assurance that the personal information being maintained at the state agencies subject to the requirements of EO504 was being adequately protected. As a result, ITD management lacks (1) reliable feedback on the existence and performance of an operational process, activity, or combination of controls and (2) independent review processes to validate agency reports and verify the existence of controls necessary to protect personal information.

The overall objective of an effective EO504 assurance function is to assess the degree to which agencies comply with Executive Order 504 and Chapters 93H and 93I of the General Laws regarding the protection of personal information. Assurance refers to a process that is designed to provide the user of all reports submitted to ITD in accordance with EO504 with a level of comfort over the accuracy and reliability of the information contained in these reports. The EO504 assurance function would evaluate the adequacy of controls to safeguard personal information from unauthorized access, modification, use, and disclosure. Consistent exercise of security, monitoring, and reporting controls are achieved through process management and regular assurance programs.

Effective EO504 assurance programs should:

- Determine whether agencies have taken sufficient steps to identify and document the operational processes and IT systems that contain personal information and the statutory, regulatory and other legal requirements requiring protection of personal information.

- Verify that agencies have conducted a risk assessment regarding security over personal information.

- Determine whether agencies have performed data classification regarding the sensitivity and protection requirements of data (degree to which the agency has complied with ITD's data classification standard).

- Verify the validity of agency statements in ISPs, ESPs and SAQs regarding the existence of and controls over personal information.

- Confirm that agencies can demonstrate compliance with Chapters 93H and 93I of the General Laws and Executive Order 504, including designating ISOs and meeting reporting requirements.

- Determine whether agencies have appropriate breach notification procedures that are in place and likely to be followed should a breach in confidentiality for personal information occur.

- Confirm the extent to which personal information is captured, stored, reported, or transmitted to other parties or systems.
- Review agencies' policies and procedures regarding the protection of personal information and related breach notification procedures.
- Review the appropriateness of stated controls for safeguarding personal information.

Comprehensive assurance programs typically include on-site assessments of the adequacy of agency policies; procedures; control self-assessments; and administrative, technical, and physical controls established by the state agency to protect personal information and ensure that appropriate incident response procedures will be followed should a data breach occur. However, although ITD is authorized under EO504 to conduct reviews to assess agency compliance with EO504 and applicable federal and state privacy and information security laws and regulations, ITD officials told us that, due to resource and staffing constraints, ITD conducts only limited "desk reviews" of the various required reports and SAQs submitted by state agencies rather than comprehensive, on-site control examinations. These officials further stated that, although a diligent effort has been made to monitor submission of reports and SAQs, ITD reviews have focused primarily upon the degree of completion of agency submissions regarding the identification of processes and systems containing personal information and related requirements to protect personal information. In this regard, although ITD has been able to review the extent to which agencies have identified federal and state privacy and information security laws and regulations, its current review process does not provide sufficient assurance for assessing compliance with laws, regulations, and legal agreements. In addition, the emphasis on the reporting process without adequate verification that appropriate security controls are in effect may result in a false sense of security that personal information is adequately protected.

Recommendation

ITD should establish an adequate assurance program framework to independently assess compliance with the requirements of EO504 and Chapter 93H and 93I of the General Laws, including the adequacy of controls to safeguard personal information. The assurance program should also address the review requirements of Executive Order 532, "Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems," issued May 9, 2011.

The assurance program should:

- Obtain a documented understanding of an agency's business processes and supporting systems and the degree of compliance in filing the required ISPs, ESPs, and SAQs.
- Obtain evidence of compliance with Chapter 93H and 93I of the General Laws and Executive Order 504.
- Assess an agency's risk management processes.
- Assess the extent to which agencies have adopted and implemented control practices outlined in ITD's enterprise IT policies and standards and obtain evidence of the degree to which appropriate IT security measures are in place and in effect.
- Assess compliance with relevant policies, standards, and guidelines, and evaluate facilities' security, risk management, and oversight processes.
- Determine, where applicable, whether changes to IT systems are performed in a controlled manner that maintains adequate safeguards over personal information, such as data masking.
- Summarize IT security and agency compliance with EO504 and Chapter 93H and 93I of the General Laws.
- Prepare assurance review reports for agency and appropriate oversight body review.

The assessment of data integrity of EO504 reporting should include an evaluation of controls pertaining to the collection and entry of source data; accuracy, completeness, and authenticity checks; processing integrity; error handling; and output review.

We further recommend that risk assessments be used to identify and evaluate agencies and select those areas for review that have the greatest risk exposure. A suggested risk analysis approach would include identification and valuation of assets, vulnerability and threat analysis, impact analysis, and identification and evaluation of control design for vulnerability scenarios. High-level assessments of security controls should be conducted to support assurance planning.

ITD's EO504 assurance program should also assess whether agencies have verified the competency and integrity of contractors and subcontractors; minimized the data and systems to which contractors will be given access; and ensure the security, confidentiality, and integrity of such data and systems. In addition, a framework should be developed for assisting agencies to address their responsibility to verify that vendors have appropriate controls in effect to protect personal information. The assurance program should assess the extent to which ISOs are involved in the

EO504 process and with coordinating compliance with all security requirements for protecting personal information.

Finally, we recommend that agencies be provided with additional guidance on conducting self-audits. Agencies should have available a documented methodology that provides a stronger basis for gathering, analyzing, and documenting control evidence to support agency responses to the SAQ.

Auditee's Response:

ITD is in general agreement with the recommendations made by the SAO. Below are specific responses to each recommendation

ITD is in the process of creating an Assurance/Compliance function within the organization. The function will most likely not be limited to securing personal information and compliance with EO504, but we will take all recommendations above into consideration as we develop the Assurance/Compliance function. Target Date: August 2012

ITD will work with agencies to provide additional guidance on conducting self-audits. Target Date: Ongoing

APPENDIX I

EO504 Self-Audit Questionnaire Approval Status

September 19, 2009 through September 19, 2011

	Filing Status as of 6/30/11			Filing Status as of 9/19/11
Agency Name**	09/19/09 Filing Date Fiscal Year 2010	09/19/10 Filing Date Fiscal Year 2011	06/30/11 Audit Period Fiscal Year 2011	09/19/11 Filing Status Fiscal Year 2012
Appellate Tax Board	Approved	Approved	Approved	Not Received
Board of Library Commissioners	Approved	Approved	Approved	Approved
Board of Registration in Medicine	Approved	Not Received	Not Received	Not Received
Bureau of State Office Buildings	Approved	Approved	Approved	Approved
Chief Medical Examiner	Approved	Approved	Approved	Not Received
Children's Trust Fund	Approved	Not Received	Not Received	Approved
Civil Service Commission	Approved	Approved	Approved	Not Received
Department of Agricultural Resources	Approved	Approved	Approved	Not Received
Department of Business Development	Approved	Not Received	Not Received	Approved
Department of Children and Families	Approved	Not Received	Not Received	Not Received
Department of Conservation and Recreation	Not Received	Not Received	Not Received	Not Received
Department of Correction	Approved	Approved	Approved	Approved
Department of Criminal Justice Information Services	Approved	Not Received	Approved	Not Received
Department of Developmental Services	Approved	Not Received	Approved	Approved
Department of Early Education and Care	Approved	Not Received	Not Received	Not Received
Department of Elementary and Secondary Education	Approved	Not Received	Not Received	Not Received
Department of Energy Resources	Approved	Approved	Approved	Approved
Department of Environmental Protection	Approved	Not Received	Remediation Required	Not Received
Department of Fire Services	Approved	Remediation Required	Approved	Approved
Department of Fish and Game	Approved	Approved	Approved	Approved
Department of Higher Education	Approved	Not Received	Not Received	Approved
Department of Housing and Community Development	Approved	Approved	Approved	Approved
Department of Industrial Accidents	Approved	Approved	Approved	Approved
Department of Labor Relations	Approved	Remediation Required	Remediation Required	Approved
Department of Mental Health	Approved	Remediation Required	Remediation Required	Not Received
Department of Public Health	Approved	Under Review	Under Review	Not Received
Department of Public Safety	Approved	Remediation Required	Remediation Required	Not Received
Department of Public Utilities	Not Received	Not Received	Not Received	Not Received
Department of Revenue	Approved	Approved	Approved	Not Received

Agency Name	09/19/09 Filing Date Fiscal Year 2010	09/19/10 Filing Date Fiscal Year 2011	06/30/11 Audit Period Fiscal Year 2011	09/19/11 Filing Status Fiscal Year 2012
Department of State Police	Approved	Not Received	Not Received	Approved
Department of Transitional Assistance	Approved	Not Received	Approved	Not Received
Department of Veterans' Services	Not Received	Not Received	Not Received	Not Received
Department of Workforce Development*	Approved	Approved	Approved	(See Exec. Office of Labor & Workforce Development)
Department of Youth Services	Approved	Approved	Approved	Approved
Department of Telecommunications and Cable	Approved	Not Received	Not Received	Approved
Developmental Disabilities Council	Approved	Not Received	Approved	Approved
Division of Administrative Law Appeals	Approved	Not Received	Not Received	Approved
Division of Apprentice Training*	Approved	Not Received	Approved	(see Division of Labor Standards)
Division of Banks	Approved	Approved	Approved	Approved
Division of Capital Asset Management	Approved	Remediation Required	Remediation Required	Approved
Division of Career Services	Approved	Not Received	Approved	Approved
Division of Health Care Finance and Policy	Approved	Approved	Approved	Approved
Division of Insurance	Approved	Remediation Required	Remediation Required	Approved
Division of Medical Assistance (MassHealth)*	Approved	Approved	Not Received	(See Exec. Office of Health & Human Services)
Division of Labor Standards	------	------	------	Approved
Division of Occupational Safety*	Approved	Approved	Approved	(see Division of Labor Standards)
Division of Professional Licensure	Approved	Approved	Approved	Approved
Division of Standards	Approved	Not Received	Not Received	Not Received
Division of Unemployment Assistance	Approved	Not Received	Approved	Approved
Executive Office for Administration and Finance	Not Received	Not Received	Not Received	Not Received
Executive Office of Education	Approved	Not Received	Not Received	Approved
Executive Office of Elder Affairs	Approved	Not Received	Not Received	Approved
Executive Office of Environmental Affairs	Not Received	Not Received	Not Received	Not Received
Executive Office of Health and Human Services	Approved	Not Received	Not Received	Not Received
Executive Office of Housing and Economic Development	Approved	Not Received	Not Received	Not Received
Executive Office of Labor & Workforce Development	Approved	Approved	Approved	Approved
Executive Office of Public Safety and Security	Approved	Not Received	Approved	Not Received
George Feingold Library	Approved	Approved	Approved	Not Received
Governor`s Office	Approved	Approved	Approved	Not Received
Group Insurance Commission	Approved	Approved	Approved	Approved
Human Resources Division	Approved	Not Received	Not Received	Not Received

Agency Name	09/19/09 Filing Date Fiscal Year 2010	09/19/10 Filing Date Fiscal Year 2011	06/30/11 Audit Period Fiscal Year 2011	09/19/11 Filing Status Fiscal Year 2012
Information Technology Division	**Approved**	**Approved**	**Approved**	**Not Received**
Massachusetts Commission for the Blind	**Approved**	**Approved**	**Approved**	**Not Received**
Massachusetts Commission for the Deaf and Hard of Hearing	**Approved**	**Not Received**	**Not Received**	**Not Received**
Massachusetts Emergency Management Agency	**Approved**	**Approved**	**Approved**	**Not Received**
Massachusetts Rehabilitation Commission	**Approved**	**Not Received**	**Not Received**	**Not Received**
Massachusetts Office On Disability	**Approved**	**Not Received**	**Not Received**	**Approved**
Merit Rating Board*	**Approved**	**Approved**	**Approved**	**(see Department of Transportation)**
Military Division	**Approved**	**Approved**	**Approved**	**Not Received**
Municipal Police Training Committee	**Approved**	**Not Received**	**Remediation Required**	**Approved**
Office for Refugees and Immigrants	**Approved**	**Not Received**	**Not Received**	**Not Received**
Office of Consumer Affairs & Business Regulation	**Approved**	**Not Received**	**Not Received**	**Approved**
Operational Services Division	**Approved**	**Approved**	**Approved**	**Approved**
Parole Board	**Approved**	**Not Received**	**Not Received**	**Approved**
Public Employee Retirement Administration Commission	**Approved**	**Approved**	**Approved**	**Approved**
Sex Offender Registry Board	**Approved**	**Approved**	**Approved**	**Approved**
Soldiers` Home In Chelsea	**Not Received**	**Not Received**	**Not Received**	**Approved**
Soldiers` Home In Holyoke	**Approved**	**Approved**	**Approved**	**Approved**
State 911 Department	**Approved**	**Not Received**	**Under Review**	**Approved**
State Racing Commission*	**Approved**	**Approved**	**Approved**	**(see Office of Consumer Affairs & Business Regulation)**
State Reclamation Board	**Approved**	**Not Received**	**Not Received**	**Not Received**
Teachers' Retirement Board	**Approved**	**Approved**	**Approved**	**Approved**
	09/19/09 Filing Date Fiscal Year 2010	**09/19/10 Filing Date Fiscal Year 2011**	**06/30/11 Audit Period Fiscal Year 2011**	**09/19/11 Filing Status Fiscal Year 2012**
Total Agencies That Had Not Filed SAQs:	**6**	**40**	**30**	**35**

Source: Information Technology Division

* Six agencies that submitted individual reports in 2009 had reports combined with a merged or parent agency in 2011.

** Chapter 25 of the Acts of 2009 consolidated the Commonwealth's transportation agencies and authorities into a new, streamlined secretariat, the Massachusetts Department of Transportation (MassDOT). As the timing and implementation of this transportation reform legislation overlapped with the implementation of Executive Order 504, ITD did not oversee the transportation secretariat's compliance with EO504 during the transitional period, and MassDOT was therefore not included in the scope of the OSA review covering the period ended June 30, 2011.

APPENDIX II

EO504 Selected Agency Survey Results

OSA staff interviewed 34 of the 40 state agencies that were delayed in submitting their Self-Audit Questionnaires (SAQs) by the September 19, 2010 filing date and obtained the following information:

- 30 agencies indicated that they have performed information security training regarding the protection of personal information.
- 30 agencies indicated that they believe that adequate controls are in place and in effect to provide reasonable assurance that personal information is protected against unauthorized access, use, modification, and disclosure.
- 28 Information Security Officers (ISOs) indicated that they hold other positions within their agencies.
- 28 agencies indicated that they have a documented information security policy (ISP) readily available.
- 26 agencies indicated that they have performed data classification for all automated systems since 2009.
- 25 agencies indicated that they believe sufficient procedures are in place to ensure timely notification to data owners should a breach of confidentiality of personal information occur.
- 11 agencies indicated that they have previously notified data owners regarding an actual or perceived breach of confidentiality of personal information.
- Various reasons for not submitting an ISP, Electronic Security Program (ESP), or SAQ for fiscal year 2011 included: no changes in documents; new Chief Security Officers (CSOs), ISOs, and Secretariat Chief Information Officers (SCIOs); and documents that were not ready for submission.

APPENDIX III

Glossary of Terms

Definition of Personal Information per Chapter 93H of the General Laws

"Personal information:" A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security Number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Definition of Personal Data per Chapter 66A of the General Laws

"Personal data:" Any information concerning an individual which, because of name, identifying number, mark, or description can be readily associated with a particular individual; provided, however, that such information is not contained in a public record, as defined in clause 26 of Section seven of Chapter four and shall not include intelligence information, evaluative information, or criminal offender record information as defined in Section 167 of Chapter six.

APPENDIX IV

Executive Order 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