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

Official Audit Report – Issued June 11, 2015

Controls over Confidential Information Stored on Electronic Equipment by Certain State Agencies

For the period July 1, 2012 through June 30, 2014

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

June 11, 2015

Dear Auditees:

I am pleased to provide this performance audit of controls over confidential information stored on electronic equipment by certain state agencies. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2012 through June 30, 2014. My audit staff discussed the contents of this report with management of each audited agency. We included full agency written responses in Appendix A of this report and incorporated excerpts of agency responses into the applicable sections of the report.

I would also like to express my appreciation to the audited agencies for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CMR	Code of Massachusetts Regulations
DAA	District Attorneys Association
DIA	Department of Industrial Accidents
DMH	Department of Mental Health
DOT	Department of Transportation
DSP	Department of State Police
EOAF	Executive Office for Administration and Finance
EOHHS	Executive Office of Health and Human Services
EOLWD	Executive Office of Labor and Workforce Development
EOPSS	Executive Office of Public Safety and Security
IT	information technology
MassIT	Massachusetts Office of Information Technology
OCME	Office of the Chief Medical Examiner
OSC	Office of the State Comptroller
OSD	Operational Services Division
OTIS	Office of Technology and Information Services
PII	personally identifiable information
SLC	State Lottery Commission
TRS	Teachers' Retirement System

EXECUTIVE SUMMARY

In carrying out their various missions, Commonwealth agencies must often use and store data such as names, Social Security numbers, and other identifying information that the state defines as "personal information" under Chapter 93H, Section 1, of the Massachusetts General Laws. As the overseers of citizen data, agencies are responsible for removing data from electronic equipment when that equipment leaves their control, whether to be transferred to another state agency or to be destroyed. Unfortunately, some common methods of removing data—such as reformatting hard drives—leave residual data that can still be retrieved, and therefore they are not completely effective in preventing inappropriate access to, and disclosure of, confidential information, which can lead to identity fraud. Recognizing this risk and the sensitivity of citizens' personal data, the Commonwealth has promulgated numerous requirements for their protection in laws, regulations, policies, and executive orders. In addition to ensuring proper security over confidential data while equipment is being used, state agencies are responsible for removing data from electronic equipment that is either being returned at the end of a lease or being transferred after it has been designated surplus or worthless.

We undertook this audit to determine whether various state agencies were taking the measures necessary to comply with applicable laws, regulations, and other authoritative guidance. Specifically, we sought to determine whether the agencies were ensuring that any confidential information maintained on state-owned or state-leased electronic equipment was properly removed once it had been determined that the equipment would be disposed of or returned to a vendor.

This audit covered the period July 1, 2012 through June 30, 2014 and involved audit work at the following executive departments and agencies: the Massachusetts Department of Transportation (DOT), Office of the Chief Medical Examiner (OCME), Department of Public Health, Department of Youth Services, Department of Mental Health, Department of Industrial Accidents, Department of Revenue, Teachers' Retirement System (TRS), Department of State Police (DSP), District Attorneys Association, and State Lottery Commission (SLC), as well as the Hampden County Registry of Deeds.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 6**	None of the 12 agencies included in our audit fully complied with state requirements regarding the removal of confidential information from electronic equipment.
Recommendations **Page 8**	1. Agencies should establish formal policies and procedures that align with the requirements of the Massachusetts Office of Information Technology (MassIT) for removing confidential information from electronic equipment. 2. Agency management should collaborate with MassIT to ensure that all individuals associated with the protection of confidential information have adequate knowledge of MassIT policies and procedures regarding the protection of confidential data. 3. Agencies should submit self-audits in accordance with MassIT requirements.
Finding 2 **Page 10**	OCME stored electronic equipment that might have contained confidential information in areas easily accessible to people who were not associated with its Information Technology (IT) department.
Recommendations **Page 11**	1. OCME should reexamine the risk of unauthorized access to stored electronic equipment and implement effective physical security controls over areas used to store equipment that may contain confidential information. At a minimum, the controls should fulfill the requirements of MassIT's Enterprise Physical and Environmental Security Policy; depending on the volume and sensitivity of stored information, management could also consider using security cameras and access logs as added controls for these areas. 2. OCME should ensure that senior IT personnel responsible for handling this equipment are properly trained and are aware of MassIT's security guidance.
Finding 3 **Page 12**	Four agencies did not have adequate inventory controls over stored electronic equipment that may have contained confidential information.
Recommendations **Page 13**	1. Agencies should maintain an inventory of surplus and worthless electronic equipment, including hard drives, and reconcile the inventory at least once a year. 2. Agencies should develop and implement a training program and provide additional supervision to personnel responsible for managing the storage, accounting, and protection of surplus or worthless equipment that may contain confidential information. 3. Agencies should develop necessary inventory control policies and procedures for surplus, worthless, and off-lease electronic equipment that, at a minimum, align with the guidelines of MassIT and the state's Operational Services Division.
Finding 4 **Page 15**	Six agencies did not properly classify the level of sensitivity of data on their electronic equipment as low, medium, or high.
Recommendations **Page 16**	1. Agencies should classify their data as having low, medium, or high sensitivity. 2. Agencies should consult with MassIT, if necessary, for guidance on developing policies and procedures regarding data classification. In addition, they should update their policies periodically to ensure compliance with MassIT requirements.

Post-Audit Action

- OCME has indicated that it will remove all confidential information from electronic equipment before transporting it to DSP, where it is destroyed.
- TRS has indicated that it has implemented written policies for wiping (deleting data from) equipment and disposing of it.
- SLC has taken action to reduce the risk of transporting unwiped equipment to its vendor for destruction by purchasing a new hard-drive tool that will remove confidential information from the equipment.
- DOT is in the process of updating its policies and procedures regarding the protection of confidential information.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain state agencies' internal controls over confidential data stored on state-owned or state-leased electronic equipment for the period July 1, 2012 through June 30, 2014. We extended our audit period through December 31, 2014 to accommodate our audit test of agencies' compliance with the requirement of Executive Order 504 to perform a self-assessment, which is completed on a calendar-year cycle.

We conducted this performance audit in accordance with 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The table below lists our objective and our conclusion and provides links to the findings where they are discussed.

Objective	Conclusion
Did the audited state agencies have adequate controls to ensure that confidential information had been removed from electronic equipment that they stored or had designated as surplus, worthless, or coming off lease, in accordance with established laws, regulations, and other requirements?	**No; see Findings 1, 2, 3, and 4**

To accomplish our audit objective, we performed the following audit procedures:

- We reviewed applicable state laws,[1] regulations, executive orders,[2] policies,[3] and procedures, as well as industry standards relevant to data security.
- We reviewed various records related to surplus and leased electronic equipment that would routinely be used to store confidential data and judgmentally selected 12 state agencies to audit.
- We reviewed the internal controls each agency had implemented for the protection of confidential information residing on its electronic equipment.

1. See Appendix B for Chapter 93H, Sections 2 and 3, of the General Laws.
2. See Appendices D and E for Executive Orders 504 and 532.
3. See Appendix C for MassIT policies.

- We interviewed the agency personnel responsible for protecting confidential information to gain an understanding of their policies and procedures for wiping (deleting information from), disposing of, transferring, and returning leased electronic equipment.

- We compared the policies and procedures developed and implemented at each agency with the requirements of applicable state laws, regulations, executive orders, policies, and procedures, as well as industry standards relevant to data security.

- We selected a non-statistical sample of 41 hard drives from a total of 361 available at the 12 selected agencies. We purchased and used R Studio, a forensic software tool, to assess the contents of these drives while taking steps to ensure that our testing did not affect the actual data. Because non-statistical sampling was used, we cannot project the results of our testing in this area to the entire population.

- To evaluate agency oversight, safeguards, and monitoring of electronic equipment, we examined inventory controls and relevant documentation, including e-mails, forms, certificates, and lease agreements. Our review verified the authorization steps required for approval from the state's Operational Services Division (OSD), as well as agency procedures to wipe equipment and verify that all data have been removed from it before disposal, transfer, or lease end.

- To determine whether physical security controls were in place and in effect to protect surplus, worthless, and off-lease equipment, we observed the storage locations of the equipment and attempted to verify the existence of controls such as door locks, security cameras, intrusion alarms, and physical access logs.

- To determine whether the agencies were using state-approved vendors to remove personally identifiable information or dispose of equipment, we compared the names of the vendors to a list of approved statewide contractors maintained by OSD and verified that each vendor was registered with the Secretary of the Commonwealth.

- We reviewed agency policies, procedures, and practices and interviewed senior information-technology personnel to determine whether agencies were complying with Section 1 of the Massachusetts Office of Information Technology's Enterprise Information Security Standards. These standards require agencies to classify data as low sensitivity (general use), medium sensitivity (internal use), or high sensitivity (confidential use).

- To determine whether the agencies had reported storing personal and sensitive data electronically, we reviewed the annual Internal Control Questionnaires submitted to the Office of the State Comptroller by each agency.

After we finished our audit fieldwork, we sent a copy of our draft report to each of the 12 audited agencies for review and comment. Each of the agencies provided written comments, which are included as Appendix A to this report. In addition, after each finding, we present a summary and/or excerpts from the agency-submitted comments on that finding and, as applicable, our replies to those comments.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. None of the agencies reviewed complied with all state requirements for information security.

None of the 12 agencies included in our audit fully complied with Executive Order 504 and certain Massachusetts Office of Information Technology (MassIT) policies and procedures regarding the removal of confidential information stored on electronic equipment. Unless agencies ensure that all confidential information is removed from electronic equipment before disposal, there is a higher-than-acceptable risk that unauthorized individuals will obtain access to this information and use it for malicious purposes. The instances of noncompliance are as follows:

- Only 1 of the 12 agencies had developed formal written policies and procedures regarding removing confidential information from electronic equipment before disposing of it or returning it to a lessor. Six agencies had inadequate written policies and procedures. The remaining 5 agencies did not have any policies and procedures.

- We asked all 12 agencies for copies of lease agreements specifying which party—the agency or the leasing vendor—was responsible for removing confidential information from equipment at the end of the lease. Two agencies did not have leased equipment, and 2 provided contracts stating specifically which party was responsible. In the latter 2 cases, we were able to verify that the information had been removed by the responsible party in compliance with state requirements. However, the other 8 agencies did not provide lease agreements even after repeated requests. In these 8 cases, because we could not determine which party was responsible for the data removal, we could not determine whether that party had done so in compliance with state requirements.

- Five of the 12 agencies relied on third-party vendors to dispose of their surplus and worthless electronic equipment. However, confidential information was not removed from this equipment before it was transported off site. For example, the Office of the Chief Medical Examiner (OCME) returned a leased copy machine to the lessor without removing any confidential information that may have resided on its hard drive.

- Six of the 12 agencies physically destroyed equipment without checking for, and removing, any confidential and personal information that might have resided on hard drives.

- Two agencies did not submit a self-audit of their electronic security plan to MassIT for calendar year 2014 by the required deadline.

Areas of Noncompliance by Agency

Name of Agency	Inadequate/Nonexistent Policies and Procedures for Removal of Confidential Information	No Documentation of Removal of Confidential Information Before Return to Vendor	Confidential Information Not Removed Before Transportation	Confidential Information Not Removed Before Destruction	2014 Self-Audit Not Submitted to MassIT by Required Deadline
Department of Industrial Accidents	✓		✓	✓	
Department of Mental Health	✓	✓		✓	
Department of Public Health	✓	✓		✓	✓
Department of Revenue	✓	✓			
Department of State Police	✓	✓	✓		✓
Department of Youth Services	✓	✓		✓	
Hampden County Registry of Deeds		✓			
Department of Transportation	✓	✓	✓	✓	
State Lottery Commission	✓		✓	✓	
Office of the Chief Medical Examiner	✓	✓	✓		
Teachers' Retirement System	✓				
District Attorneys Association	✓				

Authoritative Guidance

MassIT's Enterprise Physical and Environmental Security Policy requires the removal of sensitive information from equipment before it is transported off site or disposed of:

6. Agencies must have maintenance procedures in place to accomplish the following . . .

6.4. Ensuring adequate controls are implemented for off-site equipment prior to sending the equipment off-site for any reason. At a minimum, Agencies must:

6.4.1. Securely remove any sensitive data that does not need to reside on the equipment . . .

7.3. Ensure all equipment containing storage media, e.g., fixed hard drives are checked to verify that any licensed software or information classified as having medium or high sensitivity are removed or overwritten prior to disposal.

Regarding documentation of removal of confidential information by vendors, Chapter 93I, Section 2, of the Massachusetts General Laws states,

> *Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.*

Regarding self-audits and the establishment of policies and procedures, Massachusetts Executive Order 504 requires agencies to develop a written information security program that addresses the collection and safeguarding of personally identifiable information (PII). It also requires them to submit self-audits to MassIT at least once a year, reporting on their compliance with their own policies and with state and federal requirements.

Reasons for Noncompliance

We learned through interviews and observations that key personnel at some agencies were not aware of the specific requirements of MassIT's Enterprise Physical and Environmental Security Policy and Executive Order 504. In addition, most of the agencies we reviewed did not have policies or procedures, or had policies and procedures that were not adequate, to ensure that PII was removed when necessary. Where policies and procedures were in place, they did not always conform to MassIT policies and procedures for the safeguarding of PII.

Recommendations

1. Agencies should establish formal policies and procedures that align with MassIT requirements for removing confidential information from electronic equipment.

2. Agency management should collaborate with MassIT to ensure that all individuals associated with the protection of confidential information have adequate knowledge of MassIT policies and procedures regarding the protection of confidential data.

3. Agencies should submit self-audits in accordance with MassIT requirements.

Auditees' Responses

In their written comments, with the exception of the Department of Mental Health (DMH), the agencies concurred with our conclusions and recommendations and described corrective actions they were taking to address our concerns, as indicated in the excerpts below.

State Lottery Commission

> *The MSLC is in the process of updating its security policy regarding confidential information as well as taking steps to ensure compliance with the Commonwealth's procedures for the removal of confidential information from surplus electronic equipment, on-site destruction, and documentation of the same for all electronic equipment before disposing of as surplus equipment. We now use equipment that has passed National Security Administration (NSA) evaluation criteria as part of our surplus procedure, to perform this on-site destruction.*

Hampden County Registry of Deeds

> *The Registry was made aware that electronic equipment with informational storage required a certification of destruction. This ensures how and when the information on the equipment was destroyed. Unaware of the policy, the Registry was wiping the computer informational storage using military standards and documenting the process. At that point, the equipment was disposed of and the Registry received documentation that the equipment was removed from the premises. We now understand that the documentation we obtained was not satisfactory for the Office of the State Auditor. With this new information we immediately obtained vendors that could provide this type of certification.*

Executive Office of Health and Human Services

The Executive Office of Health and Human Services (EOHHS) responded on behalf of DMH, the Department of Public Health, and the Department of Youth Services. With regard to DMH, EOHHS stated,

> *As reflected in its 504 Self Audit and its policies and procedures . . . DMH's written policies and procedures for the removal of confidential information from electronic equipment and the documentation of same, conform to all applicable requirements.*

EOHHS also stated that it would work with each of these three departments to create a Media Sanitization policy based on MassIT requirements and would modify its own procedures to

document the revised requirements. EOHHS estimated that agency-wide implementation would take one to three months.

Department of State Police

The Department of State Police (DSP) referred in its response to policies developed by the Office of Technology and Information Services (OTIS) within DSP's oversight agency, the Executive Office of Public Safety (EOPSS):

> *EOPSS/OTIS has developed draft security policies based on the MassIT security policies that are currently in review. Upon dissemination, these policies will apply to all EOPSS agencies including the Massachusetts State Police.*

DSP also stated that it believed it had procedures in place to ensure the security of data stored on equipment that requires transportation.

Auditor's Reply

Based on the auditee responses, we believe that agencies are taking appropriate measures to address concerns we identified.

In its response, EOHHS indicated that DMH had developed written policies and procedures for the removal of confidential information for stored electronic equipment. However, during our audit, DMH only provided us with PII procedures that had not been updated since 2008 and that did not take into account the removal of confidential information from stored electronic equipment. It was only after we had completed our audit fieldwork that DMH explained that new policies and procedures had been drafted. Therefore, we did not have the opportunity to assess these procedures and perform testing to determine whether they were being adhered to.

2. One agency did not maintain adequate physical security controls over storage of electronic equipment.

OCME stored electronic equipment that may have contained confidential information in areas that were easily accessible to people who were not associated with OCME's Information Technology (IT) department. Specifically, 40 hard drives that had been designated as worthless and possibly containing confidential information were stored in an open, unsecured area. The absence of adequate physical security controls over areas containing electronic equipment increases the risk of equipment being lost,

stolen, or damaged and exposes agencies to the risks of unauthorized access, use, and disclosure of confidential information and PII.

Authoritative Guidance

MassIT's Enterprise Physical and Environmental Security Policy requires agencies to implement procedures that address, among other things, "helping to ensure that agency access points (entrances/exits) in work areas remain secure." According to this policy, acceptable controls include items such as locks and keys, video monitoring, and access logs.

Reasons for Security Issues

During our interviews with OCME's IT personnel, we found a general lack of awareness of MassIT security guidance. Management was aware of the policies, but communication of the requirements appears to be lacking.

Recommendations

1. OCME should reexamine the risk of unauthorized access to stored electronic equipment and implement effective physical security controls over areas used to store equipment that may contain confidential information. At a minimum, the controls should fulfill the requirements of MassIT's Enterprise Physical and Environmental Security Policy; depending on the volume and sensitivity of stored information, management could also consider using security cameras and access logs as added controls for these areas.

2. OCME should ensure that senior IT personnel responsible for handling this equipment are properly trained and are aware of MassIT's security guidance.

Auditee's Response

The OCME in conjunction with the EOPSS OTIS will address these recommendations through new procedures and protocols regarding storage, transportation or destruction of equipment. Security awareness training will be provided to local IT and business staff.

Auditor's Reply

Based on its response, we believe OCME is taking appropriate measures to address the concerns we identified.

3. Some agencies did not maintain adequate inventory controls over stored equipment.

Four agencies—the Department of Industrial Accidents (DIA), OCME, the State Lottery Commission (SLC), and DSP—did not have adequate inventory controls over electronic equipment that was stored (for periods varying from a few months to years) and may have contained confidential information, as detailed in the sections below. The absence of adequate inventory controls and related policies and procedures increases the risk of loss, theft, or misuse of PII and the equipment containing it.

- DIA is responsible for processing data related to citizens' medical and financial information. DIA could not provide an inventory record for hard drives designated as surplus property. After we initially requested this information, DIA provided a list of 109 hard drives that it had designated as surplus. We randomly selected a non-statistical sample of 8 of the 109 hard drives to determine whether they contained sensitive information. Using forensic audit software, we found that 1 of the drives contained confidential information. This hard drive had not been accounted for during our initial request for DIA's system of record for inventory. This indicates that, had this drive become lost or stolen, DIA might not have been aware that potential confidential and personal information was at risk of being exposed.

- OCME is responsible for processing and maintaining highly sensitive personal and medical information. OCME was not maintaining an inventory record for approximately 200 hard drives designated as worthless. We randomly selected a non-statistical sample of 4 of these drives to determine whether they contained sensitive information. Using forensic audit software, we found that one of the hard drives contained a deceased person's name, age, medical record number, cause of death, and medical history.

- SLC could not provide a current inventory record for stored electronic equipment including each device's model number, serial number, type, date of transfer to the warehouse, and date of designation as surplus/worthless.

- DSP could not provide an inventory record for several hundred pieces of stored electronic equipment. According to DSP personnel, this equipment contained confidential and personal information and had been offline and out of service for as long as four years.

Authoritative Guidance

For IT assets (including hardware such as personal computers, notebook computers, and hard drives), Section 1.1 of MassIT's Enterprise IT Asset and Risk Management Policy states,

> *Secretariats and their respective Agencies must maintain an inventory of IT assets which consist of physical IT assets (hardware, network devices, etc.) and logical IT assets (data, software, licensing, and applications).*

Section 1.1.7 requires that agencies maintain an inventory and review it regularly:

> *Annually conduct a physical audit of IT assets and reconcile the audit with the IT asset inventory. Agencies must investigate and resolve discrepancies between the physical audit of IT assets and the IT asset inventory.*

The Office of the State Comptroller's (OSC's) Fixed Assets—Accounting and Management Policy also requires an annual inventory of fixed assets (this requirement also applies to equipment designated as surplus or worthless):

> *There shall be an **annual inventory** taken of fixed assets owned by every Department. This inventory shall include, at a minimum, a verification of the existence and location of fixed assets owned by a Department. This inventory shall be done on or about June 30th of each year.*

Conducting an annual inventory of stored electronic equipment and recording accountability will help reduce risks to agencies' IT assets and PII.

Regular inventories based on an inventory record are also required by Chapter 647, Section F, of the Acts of 1989, which states,

> *Periodic comparison shall be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts.*

In addition, according to 802 Code of Massachusetts Regulations (CMR) 3.05(1),

> *All agencies must examine their inventories of equipment, supplies and materials and periodically report property that is no longer needed to the State Surplus Property Officer. The disposal of all surplus, salvage, scrap, and worthless property must be coordinated through the State Surplus Property Officer. State agencies may not transfer, donate, destroy or otherwise dispose of property without following these procedures.*

Reasons for Noncompliance

The above agencies did not provide adequate guidance, such as training and supervision, to personnel responsible for managing the storage, accounting, and protection of stored equipment. In addition, they had not developed policies, procedures, and related inventory controls in accordance with 802 CMR 3 and with OSC and MassIT guidelines.

Recommendations

1. Agencies should maintain an inventory of surplus and worthless electronic equipment, including hard drives, and reconcile the inventory at least once a year.

2. Agencies should develop and implement a training program and provide additional supervision to personnel responsible for managing the storage, accounting, and protection of surplus or worthless equipment that may contain confidential information.

3. Agencies should develop necessary inventory control policies and procedures for surplus, worthless, and off-lease electronic equipment that, at a minimum, align with the guidelines of MassIT and the state's Operational Services Division.

Auditees' Responses

In written comments, with the exception of DSP, agencies concurred with our conclusions and recommendations. Some agencies described corrective actions being taken, as follows.

DIA

The Executive Office of Labor and Workforce Development (EOLWD) responded on behalf of DIA:

> *The EOLWD Inventory Management Team maintains the agency's Asset Inventory System (ASAP). The ASAP application maintains description and tracks physical location of all office equipment, PC desktops and laptops. The Procedure for Receiving, Storing and Tagging Equipment that governs the use of the ASAP application includes guidelines for the Disposal of IT Hardware. The procedure is in the process of being finalized by Finance, Facilities, Internal Control and IT staff.*

OCME

> *EOPSS–OTIS has draft enterprise IT policy (compliant with MassIT) under review that will be provided to all EOPSS agencies, including the OCME. The OCME will ensure agency policies will be updated to reflect EOPSS and MassIT directives. An updated enterprise security awareness program will be implemented.*

SLC

> *The MSLC will develop and document inventory control policies and procedures for surplus, worthless, and off-lease electronic equipment and complete a reconciliation annually. Inventory tracking of stored equipment will log the model number, serial number, equipment type, date of transfer to warehouse, and date of designation (surplus/worthless).*
>
> *The MSLC will establish a policy for informing and training staff when necessary in handling electronic equipment in the event it may contain confidential information. MSLC personnel will annually review the documented policy and provide signature of receipt.*

DSP

The Massachusetts State Police takes great care in tracking and disposing of assets. All items (PCs, laptops, printers, etc.) are inventoried and secured until the surplus process and disposal are complete.

Auditor's Reply

Based on the auditee responses, we believe that agencies are taking appropriate measures to address the concerns we identified. With regard to DSP, although we were provided with inventory records of various IT-related assets (such as personal computers, notebook computers, and monitors), the department's inventory records did not account for hard drives that had been removed and that potentially contained confidential and personal information. For this reason, we suggest that once hard drives are removed from electronic equipment and stored separately, as is done at DSP, the department should maintain inventory records of the hard drives, including serial and model numbers. We maintain that without a record of its hard drives, DSP cannot be certain that all the drives are properly accounted for and that any PII they contain is protected from unauthorized access.

4. Some agencies did not comply with MassIT's data-classification policy.

Six agencies—the Department of Transportation (DOT), OCME, DIA, the Teachers' Retirement System (TRS), DSP, and the District Attorneys Association (DAA)—did not properly classify the level of sensitivity of the data residing on their electronic equipment as low, medium, or high. Without these classifications, agencies may not be identifying which equipment contains high-sensitivity data.

From the time information is recorded to the time it is deleted, it should be labeled with a classification designation so that agencies can ensure that it is appropriately protected, stored, and managed.

Authoritative Guidance

Section 1 of MassIT's Enterprise Data Classification Security Standards states,

> *Agencies must classify their data into at least one of the following three levels of classification:* ***Low Sensitivity*** *(General Use);* ***Medium Sensitivity*** *(Internal Use); and* ***High Sensitivity*** *(Confidential Use).*

Section 7 of MassIT's Enterprise Physical and Environmental Security Policy states,

> ***Secure disposal, removal, or reuse of equipment:*** *Agencies must document and implement procedures to reasonably ensure secure handling and disposal of IT-related equipment, particularly hardware that contains data classified as having high or medium sensitivity. Procedures must, at a minimum, accomplish the following . . .*
>
> *7.3 Ensure all equipment containing storage media, e.g., fixed hard drives are checked to verify that any licensed software or information classified as having medium or high sensitivity are removed or overwritten prior to disposal.*

To fulfill the intent of this policy, agencies must know which equipment contains particularly sensitive data in order to develop appropriate procedures and controls.

Reasons for Noncompliance

The aforementioned agencies were unaware of the requirements in MassIT's Enterprise Data Classification Security Standards and Enterprise Physical and Environmental Security Policy and had not implemented classification policies or procedures.

Recommendations

1. Agencies should classify their data as having low, medium, or high sensitivity.
2. Agencies should consult with MassIT, if necessary, for guidance on developing policies and procedures regarding data classification. In addition, they should update their policies periodically to ensure compliance with MassIT requirements.

Auditees' Responses

In written comments, agencies concurred with our conclusions and recommendations. DOT stated that it was improving its procedures in this area, and OCME stated that it was working to address our recommendations. Other agencies provided further descriptions of their corrective actions:

DIA

EOLWD IT will work with DIA to classify the data and continue consultations with MassIT for guidance on developing policies and procedures.

TRS

At the time the audit was being conducted, the MTRS Data Classification Policy was being worked on in accordance with MassIT's Enterprise Data Classification Standards. We plan to finalize our policy by June 30th and forward it to MassIT for review and comment.

DAA

While MDAA strives to comply with, if not institute more stringent policies and procedures than that of all state, federal and industry standard policies and procedures, we will review and strengthen our existing policies and procedures or draft new ones in order to comply with the audit's findings, Executive Order 504 and MassIT policies.

Auditor's Reply

Based on the auditee responses (with the exception of DSP, which did not respond to this matter), we believe that the audited agencies are taking appropriate measures to address the concerns we identified. With regard to DSP, we again encourage the agency to implement the above recommendations.

OTHER MATTERS

The Commonwealth's policies and procedures for protecting confidential information stored on electronic equipment could be improved.

The Commonwealth could improve its policies for the removal of data from electronic equipment that is being disposed of because it has been deemed surplus or worthless or because its lease is ending. Specifically, MassIT does not have a policy regarding when this removal should occur. As a result, equipment that contains confidential information could be stored in unsecured locations for extended periods, making this information more susceptible to unauthorized access and use. In addition, there were no policies requiring agencies to properly document that all confidential data have been removed before the equipment leaves the agency.

MassIT should consider developing policies that (1) establish specific timeframes for removing confidential data from equipment being disposed of or returned to a lessor and (2) require agencies to maintain proper documentation, such as the National Institute of Standards and Technology's 800-88 Certificate of Sanitization Form, confirming that confidential data have been deleted from hard drives or destroyed using industry-standard techniques. Further, the Operational Services Division should consider requiring all agencies to submit a certification verifying that all data have been removed from surplus and worthless electronic equipment before it grants the transfer authorization[4] and approves equipment for destruction. This would include hard drives, memory cards, subscriber identity module cards, cell phones, fax machines, printers, scanners, tablets, and laptop and desktop computers.

4. Written approval by the State Surplus Property Officer (in accordance with 802 Code of Massachusetts Regulations 3.06) of a request to transfer equipment from one agency to another.

APPENDIX A

Full Auditee Responses to Detailed Audit Findings

District Attorneys Association

Massachusetts District Attorneys Association
MDAA
Supporting Commonwealth Prosecutors

To: Mr. James Moriarty, Office of the State Auditor

From: Ms. Tara Maguire, Executive Director, MDAA

RE: Statewide Review of Controls over Stored Information On Electronic Equipment

Date: April 29, 2015

Dear Mr. Moriarty:

Thank you for the opportunity to review and respond to the draft audit report on the Statewide Review of Controls over Stored Information on Electronic Equipment, covering the period July 1, 2012 through June 30, 2014. Having reviewed the draft report, MDAA recognizes that the report makes notice that we are not fully compliant with Executive Order 504, certain MassIT policies and procedures regarding the removal of confidential information stored on certain equipment and having not properly classified the level of sensitivity of the data residing on electronic equipment. It is our understanding that these areas were generally represented by the table titled "Areas of Noncompliance by Agency" found on Page 7 of the draft report. Within this table, MDAA was "checked" as having "Inadequate/Nonexistent Policies and Procedures for Removal of Confidential Information".

While MDAA strives to comply with, if not institute more stringent policies and procedures than that of all state, federal and industry standard policies and procedures, we will review and strengthen our existing policies and procedures or draft new ones in order to comply with the audit's findings, Executive Order 504 and MassIT policies.

To that end, MDAA will seek from the Office of the State Auditor the specific policies or procedures that were found lacking so that we can begin to remedy the general finding of "Inadequate/Nonexistent Policies and Procedures for Removal of Confidential Information".

Thank you,

Tara Maguire
Executive Director

MDAA One Bulfinch Place, Suite 202 Boston, MA 02114 617.723.0642
www.mass.gov/mdaa

Teachers' Retirement System

MTRS
MASSACHUSETTS TEACHERS' RETIREMENT SYSTEM

Main Office
One Charles Park
Cambridge, MA 02142-1206
Phone 617-679-MTRS (6877)
Fax 617-679-1661

Western Regional Office
One Monarch Place, Suite 510
Springfield, MA 01144-4028
Phone 413-784-1711
Fax 413-784-1707

Online mass.gov/mtrs

April 21, 2015

Office of the State Auditor
Attn: James M. Moriarty, CFS, Audit Manager
One Winter Street, 9th floor
Boston, MA 02108

RE: Statewide Review of Controls of Stored Information on Electronic Equipment

Dear Mr. Moriarty:

Thank you for the opportunity to comment on the draft audit report covering the Statewide Review over Stored Information on Electronic Equipment from July 1, 2012 through June 30, 2014. We understand that the Massachusetts Teachers' Retirement System (MTRS) was one of twelve entities audited. My staff and I have reviewed the audit report and offer the following responses to the findings for your consideration.

Finding 1: ***"None of the 12 agencies included in our audit fully complied with Executive Order 504 and certain Massachusetts Office of Information Technology (MassIT) policies and procedures regarding the removal of confidential information stored on electronic equipment."***

MTRS Response:
MTRS has standard procedures in place to remove all confidential data from equipment scheduled for disposal or transport. During the audit, SAO auditors investigated our equipment and found that it was properly wiped of all confidential data and that we were compliant in four out of five areas pertaining to this requirement. The one area in which we were not compliant was to have a written policy in place to document our standard procedures. That policy was finalized last August, shortly after the auditors' visit to our office, and is attached.

Finding 4: ***"Six agencies did not properly classify the level of sensitivity of data on their electronic equipment as having low, medium, or high sensitivity."***

MTRS Response:
At the time the audit was being conducted, the MTRS Data Classification Policy was being worked on in accordance with MassIT's Enterprise Data Classification Standards. We plan to finalize our policy by June 30th and forward it to MassIT for review and comment.

1

MTRS
MASSACHUSETTS TEACHERS' RETIREMENT SYSTEM

In closing, I would like to thank you and your audit team for the cooperation and guidance provided to my staff during the audit process. If you have any questions or would like to discuss any of the feedback above, please be in touch.

Sincerely,

Erika M. Glaster
Executive Director
617-679-6859
Erika.glaster@trb.state.ma.us

2

Office of the Chief Medical Examiner

The Commonwealth of Massachusetts
Executive Office of Public Safety and Security
Office of the Chief Medical Examiner

Charles D. Baker
Governor

Karyn E. Polito
Lieutenant Governor

Daniel Bennett
Secretary

Headquarters

720 Albany Street
Boston, MA 02118-2518

Henry M. Nields, MD, Ph
Chief Medical Examiner

General Office Numbers
Tel: (617) 267-6767
Tel: (800) 962-7877
Fax: (617) 266-6763

April 22, 2015

Office of the State Auditor
One Winter Street
Boston, MA 02108

Attn: James M. Moriarty, CFS
Audit Manager

Dear Mr. Moriarty,

This letter contains the Agency's written responses to the Statewide Review of Controls over Stored Information on Electronic Equipment that was conducted last year.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. None of the agencies reviewed complied with all state requirements for information security.

Recommendations

1. Agencies should establish formal policies and procedures for removing confidential information from electronic equipment that align with MassIT requirements.
2. Agency management should collaborate with MassIT to ensure that all individuals associated with the protection of confidential information have adequate knowledge of MassIT policies and procedures regarding the protection of confidential data.
3. Agencies should submit self-audits in accordance with MassIT requirements.

Auditee's Response

The Office of the Chief Medical Examiner (OCME) is working with the Executive Office of Public Safety and Security's Office of Technology and Information Services (OTIS) to ensure compliance with above recommendations. OTIS provides IT services to the OCME under the state IT consolidation model. Agency management will prioritize actions to ensure compliance to state IT policies.

2. Two[1] agencies reviewed did not maintain adequate physical security controls over storage of electronic equipment.

Recommendations

1. OCME and DMH should reexamine the risk of unauthorized access to stored electronic equipment and ensure that effective physical security controls are in place over storage areas that may contain equipment with confidential information. At a

[1] Subsequent to our audit fieldwork, we determined that only one agency did not maintain adequate physical security controls over storage of electronic equipment.

minimum, the controls should fulfill the requirements of MassIT's Enterprise Physical and Environmental Security Policy; depending on the volume and sensitivity of stored information, management could also consider using security cameras and access logs as added controls for these areas.

2. OCME and DMH should ensure that senior IT personnel responsible for handling this equipment are properly trained and aware of MassIT's security guidance.

Auditee's Response

The OCME in conjunction with the EOPSS OTIS will address these recommendations through new procedures and protocols regarding storage, transportation or destruction of equipment. Security awareness training will be provided to local IT and business staff.

3. Some agencies reviewed did not maintain adequate inventory controls over stored equipment.

Recommendations

1. Agencies should maintain an inventory of surplus and worthless equipment and reconcile the inventory at least once a year.
2. Agencies should develop and implement a training program and provide additional supervision to personnel responsible for managing the storage, accounting, and protection of surplus or worthless equipment that may contain confidential information.
3. Agencies should develop necessary inventory control policies and procedures for surplus, worthless, and off-lease electronic equipment that, at a minimum, align with the guidelines of MassIT and the state's Operational Services Division (OSD).

Auditee's Response

EOPSS – OTIS has draft enterprise IT policy (compliant with Mass IT) under review that will be provided to all EOPSS agencies, including the OCME. The OCME will ensure agency policies will be updated to reflect EOPSS and Mass IT directives. An updated enterprise security awareness program will be implemented.

4. Some agencies did not comply with Mass IT's data-classification policy.

Recommendations

1. Agencies should classify their data as having low, medium, or high sensitivity.
2. Agencies should consult with MassIT, if necessary, for guidance on developing policies and procedures regarding data classification. In addition, they should update their policies periodically to ensure compliance with MassIT requirements.

Auditee's Response

The OCME is working with then EOPSS OTIS to address this recommendation.

Sincerely,

Deborah Mendoza-Lochrie

Deborah Mendoza-Lochrie, MSW, LICSW
Chief of Staff
Office of the Chief Medical Examiner's Office
720 Albany Street
Boston, MA 02118

Department of Transportation

Charles D. Baker, Governor
Karyn E. Polito, Lieutenant Governor
Stephanie Pollack, MassDOT Secretary & CEO

massDOT
Massachusetts Department of Transportation

May 1, 2015

James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

Dear Mr. Moriarty

Please find responses to draft audit concerning "Stored Information on Electronic Equipment" dated April 6, 2015.

Auditee's Response to Question 1

1. MassDOT has formal policies and procedures for removing confidential information from electronic equipment.
2. The policies and procedures have been disseminated to all MassDOT IT personnel.
3. MassDOT is currently concluding the annual PCI/DSS Report on Compliance. Over 300 security controls have been reviewed. All documentation has been accepted and approved. MassDOT is awaiting a final report.

Auditee's Response to Question 2

None

Leading the Nation in Transportation Excellence

Ten Park Plaza, Suite 4160, Boston, MA 02116
Tel: 857-368-4636, TTY: 857-368-0655
www.mass.gov/massdot

Auditee's Response to Question 3

None

Auditee's Response to Question 4

MassDOT is actively improving asset and data management processes and procedures

If you have any further issues or concerns regarding MassDOT" s response, please call me at 617-222-1905.

Regards:

Gary S. Foster
Secretariat Chief Information's Officer MBTA/MassDOT

Executive Office of Health and Human Services (representing the Department of Youth Services, Department of Mental Health, and Department of Public Health)

The Commonwealth of Massachusetts
Executive Office of Health and Human Services
One Ashburton Place, Room 1109
Boston, Massachusetts 02108

CHARLES D. BAKER
Governor

KARYN E. POLITO
Lieutenant Governor

MARYLOU SUDDERS
Secretary

Tel: (617) 573-1600
Fax: (617) 573-1891
www.mass.gov/eohhs

May 14, 2015

Mr. James M. Moriarty, CFS, Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

Re: Statewide Review of Controls over Stored Information on Electronic Equipment

Dear Mr. Moriarty:

Thank you for sharing your draft report and findings from your audit of the Statewide Review of Controls over Stored Information on Electronic Equipment. As always, we appreciate the opportunity to work with the State Auditor's Office (SAO) to identify opportunities to strengthen the integrity and operation of our processes and systems. As a result of this audit process, the Executive Office of Health and Human Services (EOHHS) will begin implementing changes to the processes and systems to address issues raised in the SAO's review, as described further below.

EOHHS is committed to protecting the privacy of the Commonwealth's citizens' stored personal data. We recognize the importance of removal of this data from electronic equipment before the equipment leaves our control. The SAO's report highlights key areas in which EOHHS can improve its processes to ensure that personal data is removed on electronic equipment before it is either transferred to another state agency or to be destroyed.

Attached we have provided a detailed response to the SAO's finding associated with EOHHS. We would welcome the opportunity to discuss these issues further with you and your staff should you desire.

Sincerely,

Marylou Sudders

Finding 1: None of the 12 agencies included in our audit fully complied with Executive Order 504 and certain Massachusetts Office of Information Technology (MassIT) policies and procedures regarding the removal of confidential information stored on electronic equipment.

Recommendations:
Recommendation 1. Agencies should establish formal policies and procedures for removing confidential information from electronic equipment that align with MassIT requirements

EOHHS Department of Mental Health (DMH) Response:

As reflected in its 504 Self Audit and its policies and procedures (in its Privacy and Security Handbook, available on its intranet site), DMH's written policies and procedures for the removal of confidential information from electronic equipment and the documentation of same, conform to all applicable requirements (The DMH Privacy and Security Handbook can be found at: http://eohhs-web.ehs.govt.state.ma.us/DMH%20Site/compliance/handbook.asp). When removal of confidential information is entrusted to a vendor, DMH's contracts require the vendor to comply with all such requirements, including the signing of Business Associates Agreements required under HIPAA. To the best of our knowledge in accordance with DMH procedures, confidential data is in fact removed or destroyed prior to return of electronic equipment to vendors. DMH has in place training requirements in these policies and procedures for staff involved in these activities, and through its MOU with EOHHS concerning IT services, require EOHHS IT personnel working on DMH's behalf to be similarly trained. EOHHS and DMH would welcome specific information found by the Auditor to the contrary so that it can target any necessary corrective action to deficiencies found. Otherwise EOHHS respectfully requests the Auditor's findings and recommendations as to DMH are corrected and or modified. EOHHS currently follows Mass IT policy. EOHHS in collaboration with DMH will create its own Media Sanitization policy based on Mass IT requirements and will coordinate with DMH to ensure that relevant policies, procedures and trainings are consistent and compliant. EOHHS currently has procedures in place that will be modified to formally document the revised requirements. EOHHS estimates that it will take one to three months to implement the new process across EOHHS. DMH will keep its policies and procedures in place unless a decision is made that EOHHS policies supersede DMH policies.

EOHHS Department of Public Health (DPH) Response:

EOHHS currently follows Mass IT policy. EOHHS in collaboration with DPH will create its own Media Sanitization policy based on Mass IT requirements. EOHHS currently has procedures in place that will be modified to formally document the revised requirements. EOHHS estimates that it will take one to three months to implement the new process across EOHHS.

EOHHS Department of Youth Services (DYS) Response:

EOHHS currently follows Mass IT policy. EOHHS in collaboration with DYS will create its own Media Sanitization policy based on Mass IT requirements. EOHHS currently has procedures in place that will be modified to formally document the revised requirements. EOHHS estimates that it will take one to three months to implement the new process across EOHHS.

Recommendation 2. Agency management should collaborate with MassIT to ensure that all individuals associated with the protection of confidential information have adequate knowledge of MassIT policies and procedures regarding the protection of confidential data.

EOHHS Department of Mental Health (DMH) Response:

EOHHS's Media Sanitization policy at DMH will encompass the MassIT policies, procedures and standards. The EOHHS policy will be disseminated to appropriate personnel throughout the Secretariat and in collaboration with DMH will ensure that current personnel are appropriately trained. The policy and necessary training will be incorporated into all new hire orientation materials. Again DMH will continue to train on existing DMH policies and procedures unless a decision is made that EOHHS policies supersede DMH policies.

EOHHS Department of Public Health (DPH) Response:

EOHHS's Media Sanitization policy at DPH will encompass the MassIT policies, procedures and standards. The EOHHS policy will be disseminated to appropriate personnel throughout the Secretariat and will be incorporated into all new hire orientation materials.

EOHHS Department of Youth Services (DYS) Response:

EOHHS's Media Sanitization policy at DYS will encompass the MassIT policies, procedures and standards. The EOHHS policy will be disseminated to appropriate personnel throughout the Secretariat and will be incorporated into all new hire orientation materials.

Recommendation 3. Agencies should submit self-audits in accordance with MassIT requirements

EOHHS Department of Mental Health (DMH) Response:

EOHHS has reviewed the EO504 self-audit submissions and has confirmed that DMH has submitted the EO504 self-audit on 12/5/2013 and 12/19/2014.

EOHHS Department of Public Health (DPH) Response:

EOHHS has reviewed the EO504 self-audit submissions and has confirmed that DPH has submitted the EO504 self –audit on 12/31/203 and 1/29/2015.

EOHHS Department of Youth Services (DYS) Response:

EOHHS has reviewed the EO504 self-audit submissions and has confirmed that DYS has submitted the EO504 self-audit on 12/2/2013 and 12/17/2014.

3

Executive Office of Labor and Workforce Development (representing the Department of Industrial Accidents)

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF LABOR AND WORKFORCE DEVELOPMENT

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LT. GOVERNOR

RONALD L. WALKER, II
SECRETARY

April 27, 2015

Dear Mr. Moriarty:

Please find Below EOLWD/DIA response to the performance audit of controls over confidential information stored in the electronic equipment by certain agencies.

Please do not hesitate to contact me in case of any questions.

Male Kamya

Internal Audit Director

Executive Office of labor and workforce Development.

CHARLES F. HURLEY BUILDING • 19 STANIFORD STREET • BOSTON, MA 02114
www.mass.gov/eolwd

Response to Finding 1:

EOLWD IT is in the process of drafting an Electronic Media Sanitation and Destruction Policy to address the responsibilities and actions required to ensure electronic media (i.e., PC desktop and laptop hard drives, copier memory cards and magnetic tapes) is sanitized prior to destruction. EOLWD will consult with MassIT to confirm the policy aligns with their requirements and conduct self-reviews annually to ensure compliance.

EOLWD initiated procurement of a government certified degausser, as degaussing electronic media is a highly effective means of sanitization by destroying the magnetic signature of stored data. The EOLWD IT will manage the degaussing activities in line with EOLWD's Electronic Media Sanitation and Destruction Policy.

EOLWD will continue to contract with a third party data shredding service supervised by EOLWD IT's Desktop Engineering.

To ensure safe and secure movement of electronic media between EOLWD office buildings, Desktop Engineering and Facilities will involve contracted Security Staff during transfers.

Response to Finding 2:

No response needed.

Response to Finding 3:

The EOLWD Inventory Management Team maintains the agency's Asset Inventory System (ASAP). The ASAP application maintains description and tracks physical location of all office equipment, PC desktops and laptops. The Procedure for Receiving, Storing and Tagging Equipment that governs the use of the ASAP application includes guidelines for the Disposal of IT Hardware. The procedure is in the process of being finalized by Finance, Facilities, Internal Control and IT staff

EOLWD IT routinely reviews all inventory deemed surplus, obsolete, or uneconomically repairable; the items are disposed of under the authorization of the Operational Services Division Surplus Property guidelines. The asset tag on an item deemed ready for disposal is scanned by Inventory Management Team to record the disposal date in ASAP. Electronic media from items ready for disposal will be degaussed in the future and shredded per commonwealth guidelines.

EOLWD IT and Facilities staff who have responsibility for maintaining the tracking process are trained.

Response to Finding 4:

EOLWD IT will work with DIA to classify the data and continue consultations with MassIT for guidance on developing policies and procedures regarding data classification.

State Lottery Commission

THE LOTTERY Massachusetts State Lottery Commission

DEBORAH B. GOLDBERG
Treasurer and Receiver General

BETH BRESNAHAN
Executive Director

May 7, 2015

James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

RE: MSLC Response, Draft Audit Report, Statewide Review of Controls over Electronic Equipment

Dear Mr. Moriarty:

Attached are the Massachusetts State Lottery Commission's responses to the relevant findings in the draft audit report on the Statewide Review of Controls over Stored Information on Electronic Equipment.

We extracted the relevant sections of the report and incorporated our responses directly into each section.

If you have any questions, please do not hesitate to contact me directly at: 781-849-5500.

Sincerely,

Beth Bresnahan
Beth Bresnahan
Executive Director

Supporting the 351 Cities and Towns of Massachusetts

Columbian Street • Braintree • Massachusetts • 02184-1738 • *Tel:* 781-849-5555 • *Fax:* 781-849-5547 • *TTY:* 781-849-5678 • www.masslottery.com

THE LOTTERY **Massachusetts State Lottery Commission**

DEBORAH B. GOLDBERG
Treasurer and Receiver General

BETH BRESNAHAN
Executive Director

May 8, 2015

James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

RE: MSLC Response, Draft Audit Report, Statewide Review of Controls over Electronic Equipment

Dear Mr. Moriarty:

I am forwarding the Massachusetts State Lottery Commission's responses to the relevant findings in the draft audit report on the Statewide Review of Controls over Stored Information on Electronic Equipment.

We extracted the relevant sections of the report and drafted responses to each section. The responses are as follows:

Finding 1 **Page Error! Bookmark not defined.** **Recommendations** **Page 9**	**As referenced in the Auditor's report under Post Audit Action (page 3), the MSLC is in the process of updating its security policy regarding confidential information as well as taking steps to ensure compliance with the Commonwealth's procedures for the removal of confidential information from surplus electronic equipment, on-site destruction, and documentation of the same for all electronic equipment before disposing of as surplus equipment. We now use equipment that has passed National Security Administration (NSA) evaluation criteria as part of our surplus procedure, to perform this on-site destruction.** **The MSLC will take appropriate steps to inform and train staff where necessary regarding the protection of confidential data.**
Finding 3 **Page** Error! Bookmark not defined. **Recommendations** **Page** Error! Bookmark not defined.	**The MSLC will develop and document inventory control policies and procedures for surplus, worthless, and off-lease electronic equipment and complete a reconciliation annually. Inventory tracking of stored equipment will log the model number, serial number, equipment type, date of transfer to warehouse, and date of designation (surplus/worthless).** **The MSLC will establish a policy for informing and training staff when necessary in handling electronic equipment in the event it may contain confidential information. MSLC personnel will annually review the documented policy and provide signature of receipt.**

Supporting the 351 Cities and Towns of Massachusetts
Columbian Street • Braintree • Massachusetts • 02184-1738 • *Tel:* 781-849-5555 • *Fax:* 781-849-5547 • *TTY:* 781-849-5678 • www.masslottery.com

If you have any questions, please do not hesitate to contact me directly at: 781-849-5500.

Sincerely,

Beth Bresnahan
Executive Director

Supporting the 351 Cities and Towns of Massachusetts
60 Columbian Street • Braintree • Massachusetts • 02184-1738 • *Tel:* 781-849-5555 • *Fax:* 781-849-5547 • *TTY:* 781-849-5678 • www.masslottery.com

Executive Office for Administration and Finance (representing the Department of Revenue)

The Commonwealth of Massachusetts
Executive Office for Administration and Finance

Charles D. Baker
Governor

Kristin Lepore
Secretary

Marcie Desmond
Secretariat CIO
ANF

Vincent A. Piccinni
Deputy
Secretariat, CIO
ANF

James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

May 12, 2015

James

The Audit report was well done; the report makes some excellent points and recommendations which we have or are in the process of implementing. The IT staff at ANF-IT/Dept. of Revenue is very conscious of data security and we treat all data on hard drives at the highest level on sensitivity.

The challenge for IT departments is having enough resources to meet the IT demands of the agencies we support, as well as ensuring all other IT related responsibilities - like what is noted in the Audit report- are preformed to specification.

In regards to the Audit report as it pertains to DOR, ANF-IT is committed to ensure hard drives on desktops, laptops, tablets and other mobile devices that leave our secured location are wiped of all data. We wipe and destroy hard drives on unusable devices; we wipe drives 7-times on devices for surplus & devices to be returned to a leasing company.

Thank You

Vincent A.Piccinni
Deputy Secretariat CIO, ANF

Department of State Police

The Commonwealth of Massachusetts
Department of State Police

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

DANIEL BENNETT
SECRETARY

COLONEL TIMOTHY P. ALBEN
SUPERINTENDENT

Office of the Superintendent
470 Worcester Road
Framingham, MA 01702
(508)820-2300

April 21, 2015

Mr. James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street
Boston, MA 02108

RE: Audit No. 2013-5154-35 | Controls over Confidential Information Stored on Electronic Equipment by Certain State Agencies

Dear Mr. Moriarty:

Per your letter of April 6, 2015, enclosed is a written response from the Massachusetts State Police to the draft copy of Audit No. 2013-5154-35 forwarded by the Office of the State Auditor for review by the Massachusetts State Police. The comments that follow relate only the Massachusetts State Police audit findings:

SECTION: DETAILED AUDIT FINDINGS

Finding #1 -- None of the agencies reviewed complied with all state requirements for information security.

The following were noted as deficiencies:

1. Lack of Written Security Policies

RESPONSE: EOPSS/OTIS has developed draft security policies based on the MassIT security policies that are currently in review. Upon dissemination, these policies will apply to all EOPSS agencies including the Massachusetts State Police.

2. Confidential Information Not Removed Before Transportation
RESPONSE: Upon request by the Massachusetts State Police for the rationale for this finding, the Office of the Auditor cited two MassIT policies: The 'Enterprise Physical & Environmental

M:\EOFiles\JohnFlynn\2015 Memos\Audit Report 2013-5154-3S_Review of Draft.doc 1

Excellence In Service Through Quality Policing

Security Policy' Sections 6.4, 6.4.1, 6.4.2 and the 'Enterprise Communications & Operations Management Policy' Sections 14.2.1.

a) The 'Enterprise Physical & Environmental Security Policy' Sections 6.4, 6.4.1, 6.4.2, addresses the movement of equipment offsite. The Massachusetts State Police interprets 'off site' to mean locations other than Massachusetts State Police facilities and that the 'party responsible for the equipment while off site' to reference vendors and/or consultants as opposed to Commonwealth employees.

DSP has 63 locations throughout the Commonwealth with assigned IT assets. Equipment is reassigned and/or moved regularly, not only for disposal purposes, but also in the normal course of business. The transportation of equipment occurs between Commonwealth facilities and is performed by Commonwealth employees. The personnel who transport equipment are aware of the security requirements relative to IT assets and follow specific protocols during transport.

Further, the Massachusetts State Police sees benefit to the oversight that occurs through the centralized management of the disposal/destruction of Massachusetts State Police data and assets. It allows for a thorough review of the asset prior to disposal; the segregation of duties during the disposition process; and preservation of data that may be identified during the iterative review of the asset that occurs prior to disposal. These measures would not be possible in a local setting.

b) The Massachusetts State Police interprets the 'Enterprise Communications & Operations Management Policy' Section 14 as applicable to the exchange of data through electronic means. Section 14.2.1 speaks to insuring that procedures are in place to protect physical media while in transit. The Massachusetts State Police believes that procedures are in place to insure the security of data that requires movement/transit. As previously stated, the transportation of equipment occurs between Commonwealth facilities and is performed by Commonwealth employees. The personnel who transport equipment are aware of the security requirements relative to IT assets and follow specific protocols during transport.

3. 2014 Self Audit not submitted

RESPONSE: The Massachusetts State Police has submitted the 2014 Self Audit to MassIT.

SECTION: DETAILED AUDIT FINDINGS

Finding #3 - Some agencies reviewed did not maintain adequate inventory controls over stored equipment.

The following were noted as deficiencies:

1. DSP could not provide an inventory record for several hundred pieces of stored electronic equipment.

RESPONSE: The Massachusetts State Police believes that it has provided the requested inventory information via email during the audit period and the subsequent review of the draft audit.

2. DSP did not provide adequate guidance, such as training and supervision, to personnel responsible for managing the storage, accounting and protected of stored equipment.

RESPONSE: The Massachusetts State Police takes great care in the tracking and disposing of assets. All items (PCs, laptops, printers, etc.) are inventoried and secured until the surplus process and disposal are complete. There is significant oversight and supervision during the disposal process. Specific procedures are followed by the analysts. Multiple analysts review the assets and inventory records iteratively throughout the disposal process to insure accuracy. Each step in the disposal process is managed by a supervisor who works with the analysts to assess

adherence to proper practices during disposal of assets. This includes visual confirmation of the destruction process of hard drives, smart phones and cameras that occurs on site at State Police Headquarters.
All analysts work on the inventory and disposition efforts. The importance of these efforts is reinforced through the employee review process; all analysts are rated on their adherence to inventory requirements.

3. DSP has not developed policies, procedures, and related inventory controls in accordance with 802 CRM 3 and with OSC and MassIT guidelines.
RESPONSE: The Massachusetts State Police adheres to the Operational Services Division's regulations relative to the inventory and disposal of assets and has a written policy that mandates compliance with 802 CMR 3 (attached). As stated above, EOPSS/OTIS has developed draft security policies based on the MassIT security policies that are currently in review. Upon dissemination, these policies will apply to all EOPSS agencies including the Massachusetts State Police.

Thank you for providing a draft copy of the audit report and the opportunity to comment/respond. Please do not hesitate to follow-up with any questions you may have relative to the above information.

Sincerely,

Colonel Timothy P. Alben
Superintendent

Hampden County Registry of Deeds

The Commonwealth of Massachusetts
COUNTY OF HAMPDEN
REGISTER OF DEEDS
DONALD E. ASHE

HALL OF JUSTICE
50 STATE STREET
SPRINGFIELD, MA 01103-2021
PH: (413) 755-1722 / 784-0479
FAX: (413) 731-8190

WESTFIELD SATELLITE OFFICE
59 COURT STREET
WESTFIELD, MA 01085
(413) 568-2290

April 8, 2015

James M. Moriarty, CFS
Audit Manager
Office of the State Auditor
One Winter Street – 9th Floor
Boston, MA 02108

Dear Mr. Moriarty:

The following is a written response to the one audit finding in the report dated April 6, 2015 on the Statewide Review of Controls over stored information on electronic equipment, covering the period of July 1, 2012 through June 30, 2014.

After reviewing the audit report it is our understanding that the Hampden County Registry of Deeds was going above and beyond all known necessary standards in regards to how confidential information is stored and then completely removed from electronic equipment that had been submitted and removed through the state surplus program. During the audit review, the Registry was made aware that electronic equipment with informational storage required a certification of destruction. This ensures how and when the information on the equipment was destroyed. Unaware of the policy, the Registry was wiping the computer informational storage using military standards and documenting the process. At that point, the equipment was disposed of and the Registry received documentation that the equipment was removed from the premises. We now understand that the documentation we obtained was not satisfactory for the Office of the State Auditor. With this new information we immediately obtained vendors that could provide this type of certification.

Moving forward, all electronic equipment with informational storage will continue to be wiped to military standards before leaving the Registry. Once the equipment is disposed of with the proper vendors, the proper documentation will be available certifying when and how the informational storage was physically destroyed.

Sincerely,

Donald E. Ashe
Register of Deeds

e-mail: hampden@sec.state.ma.us
website: www.registryofdeeds.co.hampden.ma.us

APPENDIX B

Excerpt from Chapter 93H of the Massachusetts General Laws: Security Breaches

Section 2.(a) *The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.*

(b) *The supervisor of records, with the advice and consent of the information technology division [now the Office of Information Technology] to the extent of its jurisdiction to set information technology standards under paragraph (d) of section 4A of chapter 7, shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.*

(c) *The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives*

of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

Section 3.(a) *A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.*

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) *If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.*

APPENDIX C

Requirements from MassIT Policies

Required for All Equipment

1. Classify data on equipment based on agency mission
2. Document data classification
3. Determine methods for removing data (based on data classification)
4. Determine whether device is surplus or worthless

Surplus Equipment	Worthless Equipment	Off-Lease Equipment
1. Fill out required forms for surplus 2. Contact Operational Services Division (OSD) for approval 3. List equipment on OSD website 4. Determine receivers 5. Fill out transfer form 6. Remove data internally or use vendor 7. Perform verification 8. Reconcile inventory	1. Obtain three department management signatures for approval of worthless designation 2. Contact OSD for approval 3. Remove data from hard drive and destroy hard drive internally or use vendor 4. If vendor is used, obtain certificate of destruction 5. Perform verification 6. Reconcile inventory with certificate of destruction	1. Review contract terms to determine responsibility for data removal 2. Remove the data with software or remove the hard drive from the equipment 3. Perform verification 4. Reconcile inventory

Excerpt from MassIT's Enterprise Physical and Environmental Security Policy

7. ***Secure disposal, removal, or reuse of equipment:*** *Agencies must document and implement procedures to reasonably ensure secure handling and disposal of IT-related equipment, particularly hardware that contains data classified as having high or medium sensitivity. Procedures must, at a minimum, accomplish the following:*

    7.1. Secure removal or overwriting of licensed software prior to disposal

    7.2. Effective and permanent removal of the contents/data on the storage device of computing equipment using industry standard techniques or tools to make the original information non-retrievable

Note: *Using the standard delete or format function is an unacceptable method of achieving this goal*

    7.3. Ensure all equipment containing storage media, e.g., fixed hard drives are checked to verify that any licensed software or information classified as having medium or high sensitivity are removed or overwritten prior to disposal

    7.4. Specify whether damaged storage devices, particularly those containing information classified as having high or medium sensitivity, must be repaired or destroyed. Procedures may require that a risk assessment be performed to determine how the device will need to be handled. For example, does the content of the device indicate

that the device should be physically destroyed rather than sent out for repair or discarded?

Excerpt from MassIT's Enterprise Data Classification Security Standards

1. Classification Scheme

Agencies must classify their data into at least one of the following three levels of classification: Low Sensitivity (General Use); Medium Sensitivity (Internal Use); and High Sensitivity (Confidential Use). For each of the three classification levels, the following information is provided:

Classification Title: Classification Level/Type

Definition: Description of Classification

Examples: Types of data that may fall under defined classification. Agencies may choose to classify data that is cited in an example below at a different sensitivity level.

1.1. Low Sensitivity (General Use)

Definition: Data classified as having low sensitivity should be thought of as being for general use and is approved by the agency as available for routine public disclosure and use. Security at this level is the minimum required by the agency to protect the integrity and availability of this data.

Examples: This may include, but is not limited to, data routinely distributed to the public regardless of whether the agency has received a public records request, such as: annual reports, publicly accessible web pages, marketing materials and press statements.

1.2. Medium Sensitivity (Internal Use)

Definition: Data classified as having medium sensitivity should be treated as internal, the release of which must be approved prior to dissemination outside the agency. Its compromise may inconvenience the agency, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. The agency will define the level of protection required for this classification.

Examples: Data in this category is not routinely distributed outside the agency. It may include, but is not limited to non-confidential data contained within: internal communications, minutes of meetings and internal project reports.

1.3. High Sensitivity (Confidential Use)

Definition: Data classified as having high sensitivity is considered confidential. Such data should not be copied or removed from the agency's operational control without authorized permission. High sensitivity data is subject to the most restricted distribution and must be protected at all times. Compromise of high sensitivity data could seriously damage the

mission, safety or integrity of an agency, its staff or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Examples: High Sensitivity data may include, but is not limited to, personally identifiable, legally mandated, or sensitive data associated with: investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, test questions and answers, constituent records, health records, academic records, contracts during negotiation and risk or vulnerability assessments.

APPENDIX D

Executive Order 504: Order Regarding the Security and Confidentiality of Personal Information

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 [now called the Office of Information Technology] 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

APPENDIX E

Executive Order 532: Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems

WHEREAS, the national economy, the financial system on which the economy relies, and the state budget are now under significant stress;

WHEREAS, state government must strive to achieve every possible efficiency in its operations and in its delivery of services to the people of the Commonwealth; and

WHEREAS, one mechanism for achieving greater efficiency and cost-effectiveness is by further coordinating and centralizing the management and operation of the Executive Department's information technology systems;

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 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. *By March 1, 2009, the secretary of each executive office ("secretariat") in the Executive Department shall appoint a Secretariat Chief Information Officer ("SCIO"). Such appointments shall be made following consultation with and approval by the Assistant Secretary for Information Technology (the "Commonwealth Chief Information Officer" (or "CIO"). Each SCIO shall report both to the Secretary of the SCIO's respective secretariat and, through a dotted line relationship, to the Commonwealth CIO. Where operationally warranted, SCIOs shall have the authority, following consultation with agency heads, to appoint chief information officers for agencies within their secretariats ("Agency CIOs"). Each Agency CIO shall report to the SCIO of his or her secretariat. All agency information technology ("IT") personnel shall report to the Agency CIO or to his or her designee, or where no Agency CIO is appointed, to the SCIO for the agency's secretariat.*

Section 3. *By July 1, 2009, with the approval of the Legislature, agency budgets for IT shall be aggregated at the secretariat level and managed by each secretariat's SCIO.*

Section 4. *By July 1, 2009, each SCIO shall submit to the Commonwealth CIO for review and approval a secretariat consolidation plan ("Secretariat Consolidation Plan") demonstrating how the Secretariat will, no later than September 30, 2009, migrate to the most efficient model for the delivery of IT services. Each Secretariat Consolidation Plan shall address, among other things, how the SCIO will manage and consolidate (or, at the SCIO's discretion, retain at the agency level or regionalize):*

- *helpdesk services;*

- *desktop and local area network (LAN) services;*
- *web site information architecture; and*
- *application services which the SCIO proposes to provide at the Secretariat level.*

Plans shall require SCIO approval for all secretariat and agency IT expenditures regardless of funding source. Subject to such approval, plans may provide for the acquisition and maintenance of agency-specific applications to remain at the agency level. Following the Commonwealth CIO's approval of their respective Secretariat Consolidation Plans, and no later than September 30, 2009, each SCIO shall manage IT for his or her secretariat based on that approved plan.

Pursuant to reporting requirements established by the Commonwealth CIO, each SCIO shall prepare and submit periodic IT plans to the Commonwealth CIO for the CIO's review and approval. Each plan shall address: (a) IT operational and project priorities that are consistent with the secretariat's strategic business goals, (b) IT budgets, (c) major IT procurements planned for the year, (d) strategies for enhancing the efficiency, effectiveness and security of IT services at the secretariat level, and (e) IT staffing plans.

Section 5. *By May 30, 2009, the Commonwealth CIO shall issue a high level description of his or her plans for completing the migration of Infrastructure Services for all Executive Department agencies to the Information Technology Division ("ITD") [now called the Office of Information Technology], except those services, if any, that the Commonwealth CIO determines cannot be centralized at ITD due to restrictions imposed by state or federal law. By September 30, 2009, the Commonwealth CIO shall finalize a detailed plan for completing the migration of Infrastructure Services for all Executive Department agencies to ITD. By December 30, 2010, ITD must substantially complete the consolidation of Infrastructure Services for the Executive Department at ITD. Consolidated Infrastructure Services provided by ITD shall, at a minimum, meet the same service levels as those received by Executive Department agencies prior to consolidation. The Commonwealth CIO may, at his or her discretion and through a written delegation, authorize certain Secretariats to operate specific Infrastructure Services.*

Section 6. *There shall be an Infrastructure Services Board ("ISB") which shall advise the Commonwealth CIO regarding service levels for the Infrastructure Services provided by ITD. The precise members and make-up of the Infrastructure Services Board shall be determined by the Commonwealth CIO, but its membership shall be drawn from state employees across the Executive Department with knowledge and experience in the field of IT, with additional representatives from the Judicial and Legislative Branches, other constitutional offices, and quasi-public authorities whose entities are or become customers of ITD's Infrastructure Services and who accept an invitation from the Commonwealth CIO to participate. The ISB shall have no decision making authority; its sole function shall be to provide information and advice, as requested, to the Commonwealth CIO.*

Section 7. *Annually, each SCIO, the cabinet Secretary for the respective Secretariat served by them, and the Commonwealth CIO will collaborate on the drafting and publication of an annual Business Innovation Plan for the Secretariat that:*

- *describes strategies that the Secretariat will implement in order to use information technology to transform the business of government;*

- *identifies specific business cost savings and efficiencies that will be generated through strategic use of information technology within each Secretariat; and*

- *identifies any necessary one-time or ongoing Information Technology investment needed to realize such business cost savings or efficiencies.*

Section 8. *Annually, the Commonwealth CIO shall, for the purpose of protecting Commonwealth programs, data and information technology, conduct compliance reviews across the executive department to ensure full compliance with statutes, regulations, policies, standards and contractual obligations related to information security and information technology and report annually on the results of such reviews to Cabinet Secretaries and the Governor.*

Section 9. *The Commonwealth CIO shall have the authority to coordinate Executive Department IT planning by:*

- *Reviewing and approving Secretariat Consolidation Plans and periodic Secretariat IT plans, and setting timeframes for both secretariat and infrastructure consolidation;*

- *Reviewing and approving secretariat IT budget requests and establishing IT budget priorities, including for all major IT projects regardless of funding source;*

- *Developing a comprehensive multi-year strategic plan for IT for the Executive Department, which addresses the acquisition, management and use of IT and specific projects that implement the strategic plan;*

- *Issuing policies, standards and guidelines governing IT procurement, development and maintenance;*

- *Identifying opportunities for cost savings based on standardization, cross-agency collaboration, use of shared services and centralization of resources; and*

- *Collaborating with SCIOs and Secretariats on the creation of annual Business Innovation Plans for each Secretariat.*

Section 10. *Where appropriate, and with the approval of the Secretary of Administration and Finance, the Commonwealth CIO shall have the authority to enforce this Executive Order by determining and imposing remedial courses of action in instances of secretariat or agency non-compliance with this Order's requirements. Such actions may include, without limitation, a freeze on the non-compliant secretariat's or agency's authority to make IT-related expenditures, as well as a loss of eligibility for IT capital funding.*

Section 11. *The Commonwealth CIO shall report annually to the Executive Office for Administration and Finance concerning: (a) progress made by the Executive Department towards secretariat and infrastructure consolidation; (b) the results of such consolidation; (c) service levels for the consolidated infrastructure services provided to the Executive Department; (d) the cost of such services; (e) Secretariat Business Innovation Plans; and (f) the results of compliance*

reviews of executive department compliance with information security and technology related laws, regulations, policies, standards and contractual obligations.

Section 12. *As used in this Executive Order:*

"Information technology" means hardware, software, and telecommunications equipment, including but not limited to personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, handheld devices, public safety radio services, facsimile machines, technology facilities including but not limited to data centers, dedicated training facilities, switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology;

"Infrastructure Services" shall mean data and telecommunications networks, data center services, web site hosting and portal services (except the provision of website information architecture and content), and shared enterprise services such as email and directory services; and

"Telecommunications" means any origination, transmission, emission, or reception of signs, signals, writings, images, and sounds or intelligence of any nature, by wire, radio, television, optical, or other electromagnetic systems.

Section 13. *Nothing in this Executive Order shall be construed to require action inconsistent with any applicable state or federal law.*

Section 14. *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 9th day of May in the year of our Lord two thousand and eleven, and of the Independence of the United States of America two hundred and thirty-five.

DEVAL L. PATRICK, GOVERNOR

Commonwealth of Massachusetts

WILLIAM FRANCIS GALVIN

Secretary of the Commonwealth

APPENDIX F

Description of Audited Agencies[5]

Executive Office for Administration and Finance (EOAF). EOAF "manages the state's administrative agencies, including revenue collection, information technology, human resources, procurement, and state facilities."

Our examination of EOAF consisted of the following agencies:

- **Department of Revenue**. "The mission of the Massachusetts Department of Revenue is to achieve maximum compliance with the tax, child support and municipal finance laws of the Commonwealth. In meeting its mission, the Department is dedicated to enforcing these laws in a fair, impartial and consistent manner by providing professional and courteous service to all its customers."
- **Teachers' Retirement System.** The system's mission is "to ensure that members . . . achieve and maintain a successful and secure retirement through responsible benefits administration, financial integrity and the provision of outstanding services."

Executive Office of Public Safety and Security (EOPSS). "The Secretary of Public Safety and Security is responsible for the policy development and budgetary oversight of secretariat agencies, independent programs and several boards which aid in crime prevention, homeland security preparedness and ensuring the safety of residents and visitors in the Commonwealth."

Our examination of EOPSS consisted of the following agencies:

- **Office of the Chief Medical Examiner.** "The Office of the Chief Medical Examiner is responsible for investigating the cause and manner of death in violent, suspicious or unexplained deaths."
- **Department of State Police.** "The Massachusetts State Police provide administrative, field, and investigative services as well as standards and training and most wanted information."

Department of Transportation. The department's mission is to "deliver excellent customer service to people who travel in the Commonwealth, and to provide our nation's safest and most reliable transportation system in a way that strengthens our economy and quality of life."

5. Each agency's mission statement is quoted from its webpage at www.mass.gov.

Executive Office of Health and Human Services (EOHHS). EOHHS is the principal agency for managing health and human-service operations throughout the Commonwealth. Our examination of EOHHS consisted of the following agencies:

- **Department of Mental Health.** "The Department of Mental Health, as the State Mental Health Authority, assures and provides access to services and supports to meet the mental health needs of individuals of all ages, enabling them to live, work and participate in their communities. The Department establishes standards to ensure effective and culturally competent care to promote recovery. The Department sets policy, promotes self-determination, protects human rights and supports mental health training and research. This critical mission is accomplished by working in partnership with other state agencies, individuals, families, providers and communities."

- **Department of Youth Services.** "As the juvenile justice agency for the Commonwealth of Massachusetts, the Department of Youth Services promotes positive change in the youth in our care and custody. Our mission is to make communities safer by improving the life outcomes for youth in our care."

Executive Office of Labor and Workforce Development. This office "is committed to building upon our successes in creating jobs and assisting residents in finding employment opportunities in every community within the Commonwealth."

- **Department of Industrial Accidents.** "The Department of Industrial Accidents (DIA) is responsible for overseeing the Workers' Compensation system in Massachusetts."

Independent Agencies: Our examination included the following non-executive-branch agencies:

- **Hampden County Registry of Deeds.** The registry's mission is "to maintain a quality, state-of-the-art recording system that is accurate, all while providing exceptional customer service with the highest level of professionalism."

- **State Lottery Commission.** The commission works "to operate in a manner that secures the integrity of the Lottery's games and protects the well-being of its customers while maximizing revenues returned to the Commonwealth for the benefit of its cities and towns."

- **District Attorneys Association.** "MDAA is an independent state agency whose mission is to support the eleven elected Massachusetts District Attorneys and their combined staff of 1500 employees, including 700 prosecutors and 250 victim-witness advocates. The District Attorneys prosecute approximately 300,000 cases annually. MDAA supports the District Attorneys by managing statewide business technology services and administering grants in the areas of Violence Against Women, Motor Vehicle Crimes, and federal technology grants. MDAA also produces publications for prosecutors and victim-witness advocates, hosts dozens of prosecutor trainings annually, and provides information on budgetary, criminal justice and public safety issues to the executive and legislative branches."