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

Official Audit Report – Issued October 11, 2019

Executive Office of Education—Information Technology Contracts

For the period July 1, 2016 through June 30, 2018

State House Room 230 ■ Boston, MA 02133 ■ auditor@sao.state.ma.us ■ www.mass.gov/auditor

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

October 11, 2019

Mr. James Peyser, Secretary
Executive Office of Education
1 Ashburton Place, Room 1401
Boston, MA 02108

Dear Secretary Peyser:

I am pleased to provide this performance audit of the Executive Office of Education. This report details the audit objective, scope, methodology, findings, and recommendations for the audit period, July 1, 2016 through June 30, 2018. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Executive Office of Education for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Curtis Wood, Secretary, Executive Office of Technology Services and Security

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

COBIT	Control Objectives for Information and Related Technology
DESE	Department of Elementary and Secondary Education
DHE	Department of Higher Education
EEC	Department of Early Education and Care
EOE	Executive Office of Education
EOTSS	Executive Office of Technology Services and Security
ISACA	Information Systems Audit and Control Association
IT	information technology
NIST	National Institute of Standards and Technology
OSA	Office of the State Auditor
OSD	Operational Services Division
RFR	Request for Response

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an audit of the Executive Office of Education (EOE). The purpose of this audit was to determine whether EOE effectively monitored its information technology (IT) contracts during the period July 1, 2016 through June 30, 2018.

In this performance audit, we examined EOE's processes for managing its IT contracts to ensure that the terms of the contracts were met.

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

Finding 1 **Page 5**	EOE did not always establish performance metrics or effectively measure the performance of its IT vendors.
Recommendations **Page 6**	1. EOE should establish key performance indicators for future IT contracts. 2. EOE should develop and implement a process to measure and monitor IT vendors' performance. 3. EOE should develop and implement metrics to ensure that IT vendors' performance requirements, such as project milestones and time and expense budgets, are met.
Finding 2 **Page 9**	EOE did not ensure that all of its third-party contracts contained essential security provisions.
Recommendation **Page 9**	EOE should establish policies and procedures that require that all IT contracts it negotiates with IT vendors comply with the Executive Office of Technology Services and Security's "Third-Party Information Security Standard."

Post-Audit Action

After we completed our audit work, EOE officials informed us that the agency had added a "Third-Party Information Security Standard" to its internal control plan.

OVERVIEW OF AUDITED ENTITY

The Executive Office of Education (EOE) was established under Section 14A of Chapter 6A of the Massachusetts General Laws as the secretariat that oversees the Commonwealth's public education agencies, boards, and commissions, including the Department of Early Education and Care (EEC), the Department of Elementary and Secondary Education (DESE), and the Department of Higher Education (DHE).

According to EOE's fiscal year 2018 internal control plan, the agency's mission is as follows:

> *[EOE] is committed to ensuring that all Massachusetts students not only remain at the head of the class nationally but are also positioned to successfully compete internationally. We will work towards that goal by implementing evidence-based strategies and programs, raising standards and accountability, improving assessments, increasing the quality of teaching, promoting innovation, enhancing student supports, and rewarding excellence.*

EOE manages information technology (IT) services on behalf of EEC, DESE, and DHE and relies on the Operational Services Division (OSD) to select and procure IT vendors that it and other state agencies can use under a master service agreement.[1] If a service is not on the OSD list of available services, EOE can negotiate directly with a vendor for that service. During the audit period, EOE was in the process of transitioning the administration of its IT services to the Executive Office of Technology Services and Security.

1. These contracts set the foundation for future business between parties, allowing them to quickly approve new transactions or agreements without having to renegotiate the terms.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Executive Office of Education (EOE) for the period July 1, 2016 through June 30, 2018.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below are the question we intended our audit to answer, the conclusion we reached regarding our objective, and where the objective is discussed in the audit findings.

Objective	Conclusion
1. Does EOE effectively monitor its information technology (IT) contracts?	**No; see Findings 1 and 2**

We conducted this performance audit by using criteria from policies issued by EOE, the "Enterprise Information Security Policies and Standards" issued by the Executive Office of Technology Services and Security (EOTSS); the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations*; and the Information Systems Audit and Control Association's (ISACA's) document *Control Objectives for Information and Related Technology [COBIT] 4.1*. The EOTSS policies we used as criteria are also derived from NIST's Special Publication 800-53, Revision 4.

According to ISACA's website,

> *COBIT helps bridge the gaps amongst business requirements, control needs and technical issues. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems.*

We gained an understanding of the internal controls over the monitoring process through interviews and observations.

To achieve our objective, we obtained a list of all 22 EOE IT contracts that were ongoing during our audit period and performed the following audit procedures:

- We selected a judgmental nonstatistical sample of 6 of the 22 contracts and reviewed them to ensure that their terms and conditions complied with EOTSS's "Third-Party Information Security Standard."
- We reviewed the same judgmental nonstatistical sample and asked EOE for evidence of monitoring activities related to these contracts to assess its monitoring of IT vendors.
- We further reviewed the same sample and held discussions with EOE officials to determine whether EOE had established performance measures to be used to assess vendor performance.

We used nonstatistical sampling and therefore did not project the results of our testing to the population.

To assess the completeness and accuracy of the contract list, we interviewed knowledgeable employees at EOE and searched COMMBUYS[2] for EOE IT contracts in effect during the audit period. We obtained the list of contracts from COMMBUYS and then compared that to the list we received from EOE's budget director, whom we also observed obtaining a list of contracts from the Commonwealth Information Warehouse. We determined that the list of IT contracts was complete and sufficiently reliable for the purposes of this audit.

2. According to the Operational Services Division's website, COMMBUYS, which is managed by that division, "is the only official procurement record system for the Commonwealth of Massachusetts' Executive Departments [and] offers free internet-based access to all public procurement information."

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Executive Office of Education did not always establish performance metrics or effectively measure the performance of its information technology vendors.

The Executive Office of Education (EOE) did not ensure that performance metrics (i.e., key performance indicators) were measured for its information technology (IT) vendors. Specifically, for five of the six IT contracts in our sample, EOE did not provide performance measurement reports. For the other contract, although EOE did establish performance measures and said that it had evaluated the vendor's performance, it could not show objective metrics to support this assertion. Without establishing measures and objectively monitoring vendor performance, EOE cannot hold its IT vendors accountable for contractual noncompliance and/or poor performance, which could affect its operations.

Authoritative Guidance

Section DS2 ("Manage Third-Party Services") of the Information Systems Audit and Control Association's (ISACA's) document *Control Objectives for Information and Related Technology 4.1* states,

> *The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimizes the business risk associated with non-performing suppliers.*
>
> ***Control Objectives. . . .***
>
> *Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and [service-level agreements].*

Although EOE is not specifically required to follow ISACA requirements, we believe they represent best practices that should be followed.

Reasons for Noncompliance

EOE officials stated that they believe that the agency's contract documents identify expected outcomes and deliverables and that EOE effectively measures performance over the course of a contract. According to EOE management, the agency has been in the process of transitioning the administration

of its IT services to the Executive Office of Technology Services and Security (EOTSS). EOTSS is responsible for IT contract management, but EOE and EOTSS did not have clearly defined roles, responsibilities, and expectations or a process for EOE's IT contract performance monitoring.

Recommendations

1. EOE should establish key performance indicators for future IT contracts.
2. EOE should develop and implement a process to measure and monitor IT vendors' performance.
3. EOE should develop and implement metrics to ensure that IT vendors' performance requirements, such as project milestones and time and expense budgets, are met.

Auditee's Response

EOE prides itself on managing vendor relationships with processes and procedures that ensure it receives the services and products for which it contracts. Executed contract documents identify expected outcomes and deliverables, and EOE effectively measures performance over the course of a contract. . . .

EOE measures performance throughout a contract cycle. Contract documentation, such as the Scope of Work, includes language identifying the procured deliverables. During a contract period, IT staff oversee processes that include daily coordination meetings, weekly reports, required signoffs on deliverables, and overarching project plans and timelines. EOE does not submit payment to vendors until user acceptance testing occurs, if warranted, or the deliverable meets the expectations identified at the outset of the contract—e.g., in the Scope of Work. For IT staff augmentation contracts, job descriptions serve to establish performance expectations, and individuals are terminated if they do not meet these expectations. Additionally, two of the contracts reviewed by the [audit team]—one for phone services and one lease agreement for desktop computers—function essentially as a purchase; the "performance metric" for these contracts simply is whether EOE received the services/goods.

The following table identifies the methods by which EOE established contract expectations and assesses vendor performance for the six contracts reviewed by the [audit team]:

Table 2.

Contract	***Contract Expectations***	***Assessment of Vendor Performance***
ITT46—Network Statewide Services	*Telecommunications/phone contract*	*Monthly review of performance/invoices*
ITC49—IT Asset Lease Services	*Purchase of Network equipment* *Printer Lease* *Desktop Lease*	*Sign off on shipment/receipt of equipment*

Table 2.		
ITS55—IBM Software, Appliances, Maintenance, and Technical Support Statewide Contract	*Hardware, software & support for DESE & DHE data systems*	*Sign off on shipment/receipt of equipment* *Daily performance metrics using Tivoli monitoring software*
ITS53— IT Staff Augmentation Full Service and Niche Statewide Contract	*Staff Augmentation Services*	*Scope of Work / Job Descriptions* *Daily time reporting* *Weekly time sign off using [Human Resource Compensation Management System].* *Weekly status reports of project plan*
18ITSMS1—SIF Maintenance and Support	*Contract for maintaining the data collection system for DESE—3 times a year data collection for all school districts.*	*Application Up-time* *System Performance stats nightly* *Weekly status metrics*
18ESEEK1—Adult Ed Data System	*Purchase and licensing for Adult Ed software system*	*Scope of Work* *Required functionality* *Assigned Project Manager to manage the implementation.* *User acceptance testing and sign off on deliverables.*

. . .

EOE constantly strives to improve practice and identify opportunities for standardization, where appropriate and will continue to work with both EOTSS and other secretariat partners to adopt best practices.

Auditor's Reply

We acknowledge that EOE does perform some monitoring of its contractors' activities. However, the assessment activities detailed in the table above appear to focus primarily on assessing contract compliance and the provision of deliverables and do not address other important aspects of performance, such as the quality of work provided. For example, in the table, EOE indicates that it uses Tivoli software to monitor the performance of the contractor it hired to provide hardware, software, and support for the DESE and DHE data systems. Although this software may allow EOE to monitor the

contractor's activities, EOE does not use the data to assess the vendor's performance. In another example, in the table, EOE indicates that it evaluates the performance of its staff augmentation service contractor by simply monitoring the progress of the project and various attendance metrics rather than the quality of services provided by the contractor (e.g., software developers are not evaluated on coding error rates and timeliness of error resolution). Moreover, it is important to note that although in some instances EOE indicates that it assesses the performance of these contractors, EOE never gave the Office of the State Auditor (OSA) any documentation to substantiate either that it had established metrics it could use to assess their performance or that it had performed any formal assessments.

In its response, EOE asserts that two of the contracts in our sample (one for phone services and one lease agreement for desktop computers) are essentially purchases and that therefore the performance metric for these contracts is simply whether EOE received the services/goods in question. However, in OSA's opinion, performance metrics and measures can and should be established for every contract. For example, on these two contracts, EOE could have established performance metrics such as the timeliness of responses to any service requests or the quality of the products received. In support of this, the "State Finance Law and General Contract Requirements" policy issued jointly by the Comptroller of the Commonwealth and the Operational Services Division (OSD) states,

> *The Commonwealth has a responsibility to conduct monitoring and evaluation of the commodities and services it purchases. These activities can assist in identifying and reducing fiscal and programmatic risk as early as possible, thus protecting both public funds and clients being served.*

As an example of a state agency that meets this requirement, the Commonwealth's Division of Capital Asset Management and Maintenance requires government awarding authorities to complete a standard Contractor Evaluation Form for Building Projects where they rate contractors on such criteria as quality of work, timeliness, and quality of customer service. This type of evaluation provides valuable information for determining whom to hire on future contracts.

In OSA's opinion, to properly assess the quality and effectiveness of the services provided by its contractors, EOE should establish quantifiable performance metrics and should regularly assess vendors' compliance with those metrics.

Based on its response, EOE will take measures to address our concerns in this area.

2. EOE did not ensure that all of its third-party contracts contained essential security provisions.

We selected 6 of 22 IT contracts that were ongoing during our audit period to determine whether they contained all of the required EOTSS security policies and found that none of the 6 contracts fully addressed EOTSS's "Third-Party Information Security Standard." Specifically, none contained all 16 of the IT-security-related contract provisions that this standard requires to be included in all IT contracts, such as the IT contractor's obligation to periodically deliver an independent report to EOE on the effectiveness of its IT security controls. As a result, there is a higher-than-acceptable risk that EOE may experience security issues, such as misuse of confidential information, with some of its IT vendors.

Authoritative Guidance

On October 1, 2017, EOTSS published on its website the preliminary policy "Third-Party Information Security Standard," which established the following best practices for the Commonwealth:

> *Commonwealth Offices and Agencies must ensure that Information Security policies and requirements are addressed and documented in any contract with the* ***third party****.*

Reasons for Noncompliance

EOE management stated that they relied on OSD to ensure that these requirements were contained in master service agreements[3] that OSD established for these services. However, although EOE selected some of these vendors (four out of six) from a master service agreement, it ultimately negotiated separate contracts with all six vendors and therefore was responsible for ensuring that the contracts complied with EOTSS's "Third-Party Information Security Standard." EOE lacked the controls (i.e., policies and procedures) necessary to ensure compliance with these requirements.

Recommendation

EOE should establish policies and procedures that require that all IT contracts it negotiates with IT vendors comply with EOTSS's "Third-Party Information Security Standard."

Auditee's Response

> *EOE ensures that each third-party contract contains required security policies. . . . IT vendors commit to compliance with security policies when they enter a contractual relationship with EOE,*

3. These contracts set the foundation for future business between parties, allowing them to quickly approve new transactions or agreements without having to renegotiate the terms.

whether through use of a statewide contract or in response to an agency-issued [Request for Response, or RFR]. As discussed above, whether EOE uses a statewide contract or an agency-issued RFR to procure IT deliverables or services, vendors commit to abiding by a variety of information security requirements—found, e.g., in the Standard Contract, the Commonwealth Terms and Conditions, the provisions of the statewide contract or RFR, the Executive Order 504 attestation, etc.

EOE also has identified internal policies, including our Procurement Policy and the half-dozen IT-related policies incorporated in our Internal Control Plan that establish security-related requirements and responsibilities, framing and orienting our ongoing work. The [audit team] cites a single policy—EOTSS's Third-Party Information Security Standard—to which it proposes EOE comply. As previously noted, that Standard already applies to EOE by its terms, but EOE has added it as of July 2, 2019, to its Internal Control Plan policy list as EOE-IT-7 Third-Party Information Security Standard, providing an EOE cover memorandum followed by the EOTSS Standard in its entirety. Moving forward, EOE will provide each vendor with a copy of EOE-IT-7 upon bid award.

EOE also submitted supplemental information (contract provisions), presented in the Appendix to this report.

Auditor's Reply

OSA acknowledges that EOE's contracts with these six vendors contain various important provisions related to the management and protection of Commonwealth data that the vendors may obtain and/or access when providing goods or services. However, these standard contract provisions do not address all of the security provisions in the EOTSS standards, such as the IT contractor's obligation to periodically deliver an independent report to EOE on the effectiveness of its IT security controls and the Commonwealth's right to audit the performance of information security and other contractual responsibilities. Therefore, we again urge EOE to implement our recommendation.

APPENDIX

As part of its response to the Office of the State Auditor's audit findings, the Executive Office of Education (EOE) submitted supplemental information.

EOE indicated that every vendor must agree to certain provisions from the Commonwealth's Standard Contract Form, which it quoted as follows:

> ***Protection of Personal Data and Information.*** *The Contractor certifies that all steps will be taken to ensure the security and confidentiality of all Commonwealth data for which the Contractor becomes a holder, either as part of performance or inadvertently during performance, with special attention to restricting access, use and disbursement of personal data and information under G.L. c. 93H and c. 66A and [Executive Order, or EO] 504. The Contractor is required to comply with G.L. c. 93I for the proper disposal of all paper and electronic media, backups or systems containing personal data and information, provided further that the Contractor is required to ensure that any personal data or information transmitted electronically or through a portable device be properly encrypted using (at a minimum) Information Technology Division (ITD) [now the Executive Office of Technology Services and Security, or EOTSS] Protection of Sensitive Information, provided further that any Contractor having access to credit card or banking information of Commonwealth customers certifies that the Contractor is . . . compliant . . . with the Payment Card Industry Council Standards and shall provide confirmation compliance during the Contract, provided further that the Contractor shall immediately notify the Department in the event of any security breach including the unauthorized access, disbursement, use or disposal of personal data or information, and in the event of a security breach, the Contractor shall cooperate fully with the Commonwealth and provide access to any information necessary for the Commonwealth to respond to the security breach and shall be fully responsible for any damages associated with the Contractor's breach including but not limited to G.L. c. 214, s. 3B.*
>
> ***Executive Order 504.*** *Regarding the Security and Confidentiality of Personal Information. For all Contracts involving the Contractor's access to personal information, as defined in G.L. c. 93H, and personal data, as defined in G.L. c. 66A, owned or controlled by Executive Department agencies, or access to agency systems containing such information or data (herein collectively "personal information"), Contractor certifies under the pains and penalties of perjury that the Contractor (1) has read Commonwealth of Massachusetts Executive Order 504 and agrees to protect any and all personal information; and (2) has reviewed all of the Commonwealth* ***Information Technology Division's*** *[now EOTSS's]* ***Security Policies****. Notwithstanding any contractual provision to the contrary, in connection with the Contractor's performance under this Contract, for all state agencies in the Executive Department, including all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices, now existing and hereafter established, the Contractor shall: (1) obtain a copy, review, and comply with the contracting agency's Information Security Program (ISP) and any pertinent security guidelines, standards, and policies; (2) comply with all of the Commonwealth of Massachusetts Information Technology Division's [now EOTSS's] "Security Policies") (3) communicate and*

enforce the contracting agency's ISP and such Security Policies against all employees (whether such employees are direct or contracted) and subcontractors; (4) implement and maintain any other reasonable appropriate security procedures and practices necessary to protect personal information to which the Contractor is given access by the contracting agency from the unauthorized access, destruction, use, modification, disclosure or loss; (5) be responsible for the full or partial breach of any of these terms by its employees (whether such employees are direct or contracted) or subcontractors during or after the term of this Contract, and any breach of these terms may be regarded as a material breach of this Contract; (6) in the event of any unauthorized access, destruction, use, modification, disclosure or loss of the personal information (collectively referred to as the "unauthorized use"): (a) immediately notify the contracting agency if the Contractor becomes aware of the unauthorized use; (b) provide full cooperation and access to information necessary for the contracting agency to determine the scope of the unauthorized use; and (c) provide full cooperation and access to information necessary for the contracting agency and the Contractor to fulfill any notification requirements.

EOE also submitted the following excerpt from the Commonwealth Terms and Conditions, to which vendors must also agree:

***Confidentiality**. The Contractor shall comply with M.G.L. C. 66A if the Contractor becomes a "holder" of "personal data." The Contractor shall also protect the physical security and restrict any access to personal or other Department data in the Contractor's possession, or used by the Contractor in the performance of a Contract, which shall include, but is not limited to the Department's public records, documents, files, software, equipment or systems.*

According to EOE, the following provisions are examples of security requirements included in some statewide contracts:

- ***ITS 55 (IBM Software, Appliances, Maintenance, and Technical Support)—3.7 Security and Privacy Requirement:** Contractor shall comply with all standards, laws and regulations as designated below, provided that an Eligible Entity will designate in its applicable Transaction Documents whether (i) any of the listed standards, laws, and regulations are inapplicable to its use of the Software, Appliances or Services ordered therein; or (ii) any additional standards, laws, regulations or policy-based privacy or security requirements (which may be available in an Agency's information security plan which will be provided to IBM upon its request, and will otherwise be provided by the Agency in writing to IBM) that are applicable to the Eligible Entity's use of the Software, Appliances or Services ordered therein. Such additional standards, laws, regulations, or requirements may include, without limitation: [Health Insurance Portability and Accountability Act of 1996] requirements or [Criminal Justice Information Service] requirements. Contractor will not be responsible for its failure to meet agency-specific or department-specific policies and standards if it was not aware, and could not have reasonably known, of such policies and standards.*

  The following are applicable to all Eligible Entities:

  1. *State Privacy Act (MGL ch. 214, s. 1B)*
  2. *Massachusetts Wiretap Statute (MGL ch. 272, s. 99)*

3. *MGL ch. 93I*

4. *MGL ch. 93H*

The following are applicable to all Agencies, the Commonwealth Health Insurance Connector (or its assignee), independent state agencies including the Center for Health Information and Analysis (or its assignee), and all Secretariats and their constituent agencies, boards, commissions, etc.:

5. *Executive Order 504*

6. *MassIT [now EOTSS] security standards (available at http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/) . . .*

The following is applicable to any Agency, any Constitutional Office, or other office, executive office, department, division, bureau, board, commission or committee thereof; or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction:

7. *Fair Information Practices Act (MGL ch. 66A)*

- ***ITS 53 (IT Project Services—Technical Specialist)—3.16.2 Security and Confidentiality:*** *The Contractor shall comply fully with all security procedures of the Commonwealth and Commonwealth Agencies in performance of the Statewide Contract. The Contractor shall not divulge to third parties any confidential information obtained by the Contractor or its agents, distributors, resellers, subcontractors, officers or employees in the course of performing Contract work, including, but not limited to, security procedures, business operations information, personally identifiable information, or commercial proprietary information in the possession of the Commonwealth Agency.*

Finally, EOE stated that each Request for Response (RFR) it issues includes provisions related to vendor security requirements, including the following:

- ***18ITSMS1-SIF Maintenance and Support***

  5. SYSTEM SECURITY

  As part of its work efforts under this [Statement of Work], [Vendor Abbreviation] will be required to use Commonwealth data and IT resources. For purposes of this work effort, "Commonwealth Data" shall mean data provided by the [Agency Abbreviation] to [Vendor Abbreviation], which may physically reside at a Commonwealth or [Agency Abbreviation] or [Vendor Abbreviation] location.

  5.1 Commonwealth Data

  In connection with Commonwealth Data, [Vendor Abbreviation] will implement commercially reasonable safeguards necessary to:

5.1.1 Prevent unauthorized access to Commonwealth Data from any public or private network;

5.1.2 Prevent unauthorized physical access to any information technology resources involved in the development effort; and

5.1.3 Prevent interception and manipulation of Commonwealth Data during transmission to and from any servers.

5.2 Commonwealth Personal Data

In addition to the above requirements for Commonwealth Data, [Vendor Abbreviation] may be required to use the following Commonwealth personal data under MGL ch. 66A and/or personal information under MGL ch. 93H, or to work on or with information technology systems that contain such data as [here agency should list the categories of such data that the vendor will be required to use] in order to fulfill part of its specified tasks. For purposes of this work effort, electronic personal data and personal information includes data provided by the [Agency Abbreviation] to [Vendor Abbreviation] which may physically reside at a location owned and/or controlled by the Commonwealth or [Agency Abbreviation] or [Vendor Abbreviation]. In connection with electronic personal data and personal information, [Vendor Abbreviation] shall implement the maximum feasible safeguards reasonably needed to:

5.2.1 Ensure the security, confidentiality and integrity of electronic personal data and personal information;

5.2.2 Prevent unauthorized access to electronic personal data or personal information or any other Commonwealth Data from any public or private network;

5.2.3 Notify [Agency Abbreviation] immediately if any breach of such system or of the security, confidentiality, or integrity of electronic personal data or personal information occurs.

5.2.4 [Vendor Abbreviation] represents that it has executed the EO504 Contractor Certification Form, which is attached hereto as Exhibit B.

***5.3 Software Integrity Controls** [Address the following controls if applicable, usually in the case wherein the Vendor will be developing code and migrating that code to a production environment]*

[Vendor Abbreviation] and [Agency Abbreviation] recognize the serious threat of fraud, misuse, and destruction or theft of data or funding. These threats could be introduced when unauthorized or inappropriate modifications are made to a production system. [Vendor Abbreviation] shall implement the following controls for the purpose of maintaining software integrity and traceability throughout the software creation life cycle, including during development, testing, and production:

5.3.1 [Vendor Abbreviation] shall configure at least two software environments including a development/quality assurance (QA) environment and a production environment.

5.3.2 [Vendor Abbreviation] shall implement a change management procedure to ensure that activities in the development/QA environment remain separate and distinct from the production environment. In particular the change management procedure shall incorporate at least the following:

5.3.2.1 Segregates duties between development and testing of software changes and migration of changes to the production environment;

5.3.2.2 Implements security controls to restrict individuals who have development or testing responsibilities from migrating changes to the production environment.

5.3.2.3 Includes a process to log and review all source control activities.

5.3.3 [Vendor Abbreviation] shall implement a source control tool to ensure that all changes made to the production system are authorized, tested, and approved before migration to the production environment.

5.3.4 [Vendor Abbreviation] shall not make any development or code changes in a production environment.

5.3.5 [Vendor Abbreviation] shall implement additional internal controls as specified in [Agency and Vendor incorporate attachment if relevant]

- ***RFR 18ESEKI, the Massachusetts Adult Education Data System***

1.9.10 The Vendor shall provide operations and/or maintenance manuals, user guides and other applicable documentation to meet security and other EOE regulations, policies and IT methodologies as appropriate.

1.9.11 If required, the Vendor shall provide and run, a system in parallel with the incumbent's already working computer environment ensuring security safeguards are in place to eliminate or reduce any security incidents and breaches during the transition period from legacy to [a commercial off-the-shelf] or [software as a service] solution.

2.10 Information Security

2.10.1 The Vendor shall provide protection of sensitive data (e.g. names, addresses, [Social Security numbers], others) by the use of encryption, secure transmission methods and the security methodologies.

2.10.2 The Vendor shall comply with and adhere to Massachusetts Enterprise Security Policy, located at http://www.mass.gov/anf/docs/itd/policies-standards/ent-pol-sec-infosec-low-1-sb-docxsm-kp-docxsm.docx

- *The [Federal Information Security Modernization Act] publications are available online at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*
- *The [National Institute of Standards and Technology, or NIST] publications are available online at http://csrc.nist.gov/publications/PubsSPs.html*

2.10.3 The Vendor shall complete and submit any necessary paperwork for security access to any EOE site if access is needed to the EOE system, as directed and coordinated with the Agency officials.

2.10.4 The Vendor shall meet the following federal standards in order to achieve annual audit requirements:

- *The Vendor shall conduct an annual internal risk assessment of their [Massachusetts Adult Education Data System, or MAEDS] Data Center and infrastructure in accordance with the best practices for the performance of risk assessments contained in the NIST Special Publication 800-30: The Risk Management Guide for Information Technology Systems.*
- *The Vendor shall reference [Federal Information Processing Standards, or FIPS] PUB-199: Standards for Security Considerations of Federal Information and Information Systems and FIPS PUB-200: Minimum Security Requirements for Federal Information and Information Systems to specify minimum security requirements for the MAEDS system and select the security controls using the security categorization standard in FIPS PUB-199.*

Note: ☐ By checking the box your business confirms that the submitted Quote/Response shall meet the mandatory requirements set forth in Section 2.10.1-2.10.4

Further, this departmental RFR asked each vendor to complete the following questions and the score card was evaluated based upon their replies.

Please provide answers to the following questions.

2.2.10 Describe the security model used by your system.

2.2.12 Do you have a disaster recovery plan? If so, describe.

2.2.13 Do you have a backup or redundancy policy or procedure? If so, describe.

2.2.14 Identify the method used for data backup (e.g., Tape, [virtual machine] snapshot, Amazon [Elastic Block Store], etc.)?

2.2.15 If you use tapes, what is the method used to transfer them from the tape storage facility to the data center?

2.2.16 Within the hosted environment, what type of file or application auditing/logging is available?

2.2.17 Explain your ability to see what was changed, who changed it and when. Would we be able to review that information upon request?

2.2.18 Do you have written information security policies that, at a minimum, govern issues such as information handling, systems hardening, user awareness training and incident response? If so, describe.

2.2.19 Do you have breach notification/incident reporting procedures? If so, describe.

2.2.20 What are your maintenance cycles and how do you inform customers of future outages?

2.2.21 Do you provide availability metrics/dashboards? How do you calculate your metrics? What exceptions are granted in your metrics?

2.2.22 Does your company complete a [Statement on Standards for Attestation Engagements No. 16] ([System and Organization Controls reports] 1/2/3) and [Federal Risk and Authorization Management Program] Audit? If yes, when [was the] last one completed?

2.2.23 Do you have a formal written incident response plan? If so, when was the last time it was tested?