Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued July 3, 2018

Massachusetts Rehabilitation Commission

For the period July 1, 2015 through June 30, 2017

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

July 3, 2018

Ms. Toni Wolf, Commissioner
Massachusetts Rehabilitation Commission
600 Washington Street
Boston, MA 02111

Dear Ms. Wolf:

I am pleased to provide this performance audit of the Massachusetts Rehabilitation Commission. This report details the audit objective, scope, methodology, finding, and recommendations for the audit period, July 1, 2015 through June 30, 2017. 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 Massachusetts Rehabilitation Commission for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Marylou Sudders, Secretary, Executive Office of Health and Human Services

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

OVERVIEW OF AUDITED ENTITY 2

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY 3

DETAILED AUDIT FINDINGS WITH AUDITEE’S RESPONSE 5

1. **The Massachusetts Rehabilitation Commission is not properly administering its contract management database. 5**

LIST OF ABBREVIATIONS

CMDB	contract management database
EOHHS	Executive Office of Health and Human Services
EOTSS	Executive Office of Technology Services and Security
IT	information technology
MMARS	Massachusetts Management Accounting and Reporting System
MRC	Massachusetts Rehabilitation Commission
OSA	Office of the State Auditor

EXECUTIVE SUMMARY

The Massachusetts Rehabilitation Commission (MRC), established under Section 74 of Chapter 6 of the Massachusetts General Laws, is a state agency within the Executive Office of Health and Human Services (EOHHS). Its primary mission is to help individuals with disabilities live and work independently in the community.

In accordance with Section 12 of Chapter 11 of the General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of MRC for the period July 1, 2015 through June 30, 2017. In this audit, we determined whether MRC has a system in place to properly administer its billings to vendors.

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

Finding 1 **Page 5**	MRC is not properly administering its contract management database.
Recommendations **Page 7**	1. MRC should immediately address the issues of noncompliance we identified during our audit and take the measures necessary to ensure that its staff members comply with all of EOHHS's Information Security Management Program Standards, including establishing monitoring controls to monitor adherence to these standards. 2. MRC should implement a monitoring process for third-party vendors to ensure compliance with the Commonwealth's information security control requirements as established by the information technology (IT) policies of both EOHHS and the Executive Office of Technology Services and Security.

Post-Audit Action

EOHHS's chief information security officer informed OSA that after the end of our audit period, EOHHS established procedures that include regularly monitoring third-party IT vendors to ensure their compliance with established IT controls and that, effective May 14, 2018, it had implemented new training on IT security for all its staff members.

OVERVIEW OF AUDITED ENTITY

The Massachusetts Rehabilitation Commission (MRC) was created under Section 74 of Chapter 6 of the Massachusetts General Laws. According to its website,

> *The Massachusetts Rehabilitation Commission (MRC) helps individuals with disabilities to live and work independently. MRC is responsible for Vocational Rehabilitation, Community Living and eligibility determination for the Social Security Disability Insurance (SSDI) and Supplemental Security Income (SSI) federal benefits programs.*

MRC is made up of three divisions:

- The Vocational Rehabilitation Division helps people with disabilities find employment in the community.
- The Community Living Division secures vendors to provide in-home and home-care services to people with disabilities.
- Disability Determination Services is funded by the Social Security Administration. It determines eligibility for Supplemental Security Income and Social Security Disability Insurance.

MRC received state appropriations of $48,517,345 and $49,279,922 in fiscal years 2016 and 2017, respectively. It also received federal grants in the amounts of $109,162,053 and $116,290,399 for fiscal years 2016 and 2017, respectively.[1] The tables below outline the specific amounts of state and federal appropriations allocated to the three MRC divisions for fiscal years 2016 and 2017.

State Appropriations

Division	Fiscal Year 2016	Fiscal Year 2017
Community Living Division	$ 35,663,829	$36,345,966
Vocational Rehabilitation Division	12,853,516	12,933,956
Disability Determination Services	0	0
Total Appropriations	$ 48,517,345	$49,279,922

Federal Appropriations

Division	Fiscal Year 2016	Fiscal Year 2017
Community Living Division	$ 2,887,357	$ 2,457,854
Vocational Rehabilitation Division	60,807,333	60,736,557
Disability Determination Services	45,467,363	53,095,988
Total Appropriations	$ 109,162,053	$ 116,290,399

[1] The federal fiscal year runs from October 1 through September 30.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of the Massachusetts Rehabilitation Commission (MRC) for the period July 1, 2015 through June 30, 2017.

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 is our audit objective, indicating the question we intended our audit to answer and the conclusion we reached regarding the objective.

Objective	**Conclusion**
1. Is MRC properly administering its contractor billing process?	**Yes**

While performing our review of MRC's contractor billing process, we identified issues with its administration of its contract management database (CMDB), which are presented as Finding 1 in this report.

We gained an understanding of the internal controls we deemed significant to our audit objectives through interviews and observations. We evaluated the design and effectiveness of those controls and assessed whether they operated as intended during the audit period. In addition, we performed the following procedures to obtain sufficient, appropriate audit evidence to address our audit objectives.

- We performed data analytics to determine whether any of MRC's consumers received services from vendors while hospitalized during the period March 5, 2016 through October 2, 2016. We further analyzed all instances in which vendors provided services during this period when the consumers appeared to have been hospitalized. We then verified that the 10 vendors' contracts were active and determined whether services were allowable while the consumers were hospitalized.
- We performed a statistical test of 24 vendor billings to MRC out of 18,927 billings during the audit period, using a 90% confidence level, a tolerable error rate of 10%, and an expected error rate of 0%. We verified that billings were allowable according to the contracts and compared

invoice amounts to Massachusetts Management Accounting and Reporting System (MMARS) payment data.

To perform our audit procedures, we obtained data for all MRC payments made to vendors from MMARS. We relied on the work performed by OSA in a separate data reliability assessment project that tested certain information system controls in MMARS. As part of the work performed, OSA reviewed existing information, tested selected system general controls, and performed inquiries with knowledgeable agency officials regarding MRC billing data. We performed other validity and integrity tests on all claim data from MMARS by tracing a sample of claims queried to source documents. Based on these procedures, we determined that the vendor payment records obtained from MMARS for our audit period were sufficiently reliable for the purposes of this report.

Additionally, we performed other validity and integrity tests on selected information system general controls over the MRC server, Enterprise Invoice Management / Enterprise Service Management,[2] and the CMDB, including tracing a sample of claims queried to source documents. The selected information system general controls were over access and security management. We tested to determine whether all employees on the active users list were actually active users; all terminated users had their access to MRC's systems revoked; employees who had transferred or been promoted had proper access; employees had proper background checks when hired; and new hires had received security awareness training.

Based on these procedures, we determined that the information system general controls over MRC's contract billings and information systems need improvement.

[2] Enterprise Invoice Management / Enterprise Service Management is one of the three systems that MRC uses to administer vendor billing information.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts Rehabilitation Commission is not properly administering its contract management database.

We found problems with the manner in which the Massachusetts Rehabilitation Commission (MRC) administered the use of its contract management database (CMDB). The CMDB is maintained by MRC's Contracts Unit Team and contains copies of all contracts and contract-related information, such as Requests for Responses. The agency uses it to manage the contracting process. As a result of the administrative problems, there is a higher-than-acceptable risk of unauthorized access and/or improper disclosure of information stored in the MRC network and the CMDB.

We found the following specific problems:

- Three out of 14 terminated employees we tested from the list of terminated employees retained access rights to the MRC network after their dates of termination, for periods ranging from three months to two years.
- Two out of 13 staff members we tested from the list of active employees should have had their access to the MRC network discontinued because they had been terminated.
- Screen locks, which should sign users out after a certain amount of inactive time, did not work.
- Users were allowed seven unsuccessful login attempts before being locked out.
- Nineteen out of 25 employees we reviewed had not received their annual security awareness training.
- MRC did not maintain audit logs to support after-the-fact investigations of security incidents.

In addition, MRC did not properly monitor Eastern Resource Group, the third-party administrator of the CMDB, to ensure compliance with the relevant information system policies and procedures.

Authoritative Guidance

Section 6.1.2 of the Executive Office of Health and Human Services (EOHHS) information technology (IT) Information Security Management Program Standards, dated November 2015, apply to all agencies within EOHHS, including MRC. Regarding access controls for terminated users, the standards state,

> *EOHHS manages information system accounts as follows . . .*
>
> *(g) User managers will notify the Help Desk and/or the system account manager when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;*
>
> *(h) The Help Desk will deactivate accounts of terminated or transferred users when a documented and approved request is completed.*

Section 6.1.9 requires the following for screen locks:

> *EOHHS systems will:*
>
> - *Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.*

Regarding unsuccessful login attempts, Section 6.1.7 states,

> *EOHHS requires that each system or application:*
>
> - *Enforces a limit of three (3) consecutive invalid login attempts by a user during a 60 minute period.*

Section 6.2.2 discusses security awareness training:

> *EOHHS and its agencies will provide basic security awareness training to all users of EOHHS resources as a part of initial training for new users, as system changes occur and annually thereafter.*

On audit logs, the standards state,

> ***6.1.2.4 AC-2(4) Automated Audit Action***
>
> *EOHHS requires the auditing/logging of user account activity to include: account creation, modification and disabling of accounts with proper notice sent to managers and other appropriate staff. . . .*
>
> ***6.3.10 AU-11 Audit Record Retention***
>
> *EOHHS and its agencies will retain audit records for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.*

Finally, regarding third-party compliance, Section 3.1 states,

> *EOHHS Department Agencies are required to ensure compliance by third parties in any aspect of the process of providing goods and services to their agency. These include, but are not limited*

> *to, electronic data collection, storage, processing, disposal, dissemination and maintenance. Third parties that interact in any way with EOHHS IT Resources are required to comply with this policy.*

Additionally, the Executive Office of Technology Services and Security (EOTSS) Enterprise Information Security Policy dated March 2014, with which all executive department agencies must comply, confirms these policies:

> *It is the responsibility of Agency Heads to have controls in place and in effect that provide reasonable assurance that security objectives are addressed. The Agency Head has the responsibility to exercise due diligence in the adoption of this framework. Agencies must achieve compliance with the overall information security goals of the Commonwealth including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.*

Reasons for Noncompliance

MRC has not established monitoring controls to ensure that its staff members comply with EOHHS's IT Information Security Management Program Standards.

Recommendations

1. MRC should immediately address the issues of noncompliance we identified during our audit and take the measures necessary to ensure that its staff members comply with all of EOHHS's Information Security Management Program Standards, including establishing monitoring controls to monitor adherence to these standards.
2. MRC should implement a monitoring process for third-party vendors to ensure compliance with the Commonwealth's information security control requirements as established by both EOHHS and EOTSS IT policies.

Auditee's Response

In response to this audit finding, MRC provided the comments below as well as timelines by which the indicated corrective measures would be completed.

> *MRC is creating policies and an implementation plan to be in compliance with Section 3.1 of the Executive Office of Health and Human Services (EOHHS) information technology (IT) Information Security Management Program Standards.*
>
> *Program managers responsible for the contracts will be trained by the end of the second quarter of fiscal year 2019 on the policy and vendor reviews.*
>
> *MRC will review the policies with all third party IT vendors and develop a monitoring process to ensure compliance with information security control requirements of EOHHS and EOTSS.*

MRC, in collaboration with the EOHHS Information Technology Division, is strengthening its off boarding process to ensure that upon termination an employee's access to systems and networks will be terminated. MRC will create and implement a policy that validates and communicates to responsible parties, when an employee is terminated and the system and network access that must be discontinued.

MRC is reviewing all profiles to ensure only active employees remain, and that active employees only have access to those systems they need to perform their function. This will be completed no later than July 27, 2018.

Training on these policies and forms will be completed by the end of the first quarter of fiscal year 2019 for all employees responsible in the off/on-boarding process.

MRC will review all network users quarterly to ensure compliance. . . .

MRC has reviewed findings with EOHHS Information Technology Division [and] submitted a request for the configurations of all computers to be updated. The configuration build is in process. . . .

The Executive Office of Technology Services and Security recently released a mandatory Security Training for all Commonwealth Employees. MRC required the training to be done no later than June 15. MRC will review records to ensure that all users have completed their annual training.