Commonwealth of Massachusetts

Management Letter

June 30, 2019

KPMG

KPMG LLP
Two Financial Center
60 South Street
Boston, MA 02111

April 3, 2020

Mr. William McNamara, Comptroller
The Commonwealth of Massachusetts
Boston, Massachusetts

In planning and performing our audit of the financial statements of the Commonwealth of Massachusetts (the Commonwealth) as of and for the year ended June 30, 2019, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, we considered the Commonwealth's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Commonwealth's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commonwealth's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our report dated February 10, 2020 on our consideration of the Commonwealth's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be material weaknesses or significant deficiencies or material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. During our audit, we identified deficiencies in internal control summarized as items 2019-001 to 2019-006 in the attached schedule of observations.

The Commonwealth's responses to the findings identified in our audit are described in the schedule of observations. The Commonwealth's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the responses.

This purpose of this letter is solely to describe the deficiencies in internal control identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

KPMG LLP
Two Financial Center
60 South Street
Boston, MA 02111

April 3, 2020

Mr. William McNamara, Comptroller
The Commonwealth of Massachusetts
Boston, Massachusetts

We have audited the basic financial statements of the Commonwealth of Massachusetts) (the Commonwealth), for the year ended June 30, 2019, and have issued our report thereon dated February 10, 2020. In planning and performing our audit of the basic financial statements of the Commonwealth, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the basic financial statements. The objective of our audits is to express opinions on the Commonwealth's basic financial statements, in accordance auditing standards generally accepted in the United States of America (AICPA), but not for the purpose of expressing an opinion on the effectiveness of the Commonwealth's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commonwealth's internal control.

During our audit, we identified deficiencies in internal control summarized as items 2019-007 and 2019-008 on the attached schedule of observations related to internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are not considered to reflect deficiencies, significant deficiencies, or material weaknesses in internal control over financial reporting. All deficiencies, significant deficiencies, and material weaknesses in internal control over financial reporting have been previously communicated to management and the Comptroller's Advisory Board, as applicable.

Our audit procedures are designed primarily to enable us to form opinions on the basic financial statements and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Commonwealth's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The Commonwealth's written responses to our comments and recommendations have not been subjected to the auditing procedures applied in the audit of the basic financial statements and, accordingly, we express no opinion on them.

This communication is intended solely for the information and use of management of the Commonwealth and the Advisory Board, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Commonwealth of Massachusetts

Schedule of Observations

June 30, 2019

2019-001

Office of the Comptroller – Access to HR/CMS Application

Repeat observation: No

Observation

Out of a total population of 100 employees with more than self-service access to the HR/CMS application who were terminated between July 1, 2018 and June 30, 2019, KPMG identified 11 users who did not have access terminated in a timely manner. These users were from the following agencies:

- 5 users were from the MBTA;
- 2 from the Treasury department;
- 2 from the Department of Transportation;
- 1 from the Gaming Commission; and
- 1 from the Human Resources Division.

Timely for purposes of this audit was considered at most 3 business days after termination based on better practice for end-user accounts to systems that contain sensitive data. The users in question had their access terminated between 4 and 117 days after termination.

Removing access swiftly upon termination prevents inappropriate access by individuals who are no longer employed by the Commonwealth and thereby prevents unauthorized transactions in the HR/CMS application.

The Comptroller's office performs a periodic review that identified these users and removed their access. Further, upon investigation by the Comptroller's office, they determined that there was no inappropriate activity by any of the 11 users.

Recommendation

We recommend that management:

- Investigate the possibility to automate the removal of more than self-service access upon termination so that exceptions due to human error are prevented.

- Re-iterate to all HR/CMS personnel with more than self-service access at the Commonwealth the importance of swiftly notifying HR/CMS administrators of termination.

Management's Response

MBTA

The DSO continues to monitor the weekly separations report to determine if any newly separated employees need to have access terminated. In addition in preparation for the Annual Statewide Enterprise Security Audit, the DSO removes access for any user who did not have regular activity/use of the systems. The MBTA was notified on July 1, 2019 that we received a pass for the evidence submitted and the CTR approved our audit submission in compliance with the statewide security policy. The DSO will work closely with HR and payroll to remove users in a timely fashion.

Treasury Department

Going forward, HR will open a ticket for people with HR/CMS access prior to their departure and I.T. will discontinue their UAID's on their last day of service.

Department of Transportation

Both users that were identified were not terminated due to a failure in communications during the offboarding process. To correct this MassDOT HR has initiated a series of changes to our offboarding process that automates the notification of an employee's termination (voluntary and Involuntary) to the security team. This along with other preventative steps implemented during our review will ensure that other such incidents have a reduced likelihood of reoccurring.

Gaming Commission

This was a one-time exception, we are aware of it and we will ensure it is not repeated going forward.

Human Resources Division

The department have met internally to discuss the exception noted and have asked that our HR Director notify us of all terminations in a more timely manner so that we can terminate UAIDs within 1-3 business days.

Responsible Officials

MBTA

Gina Spaziani, Deputy Chief Financial Officer and DSO

Treasury Department

Diane McGuire – Helpdesk & Network Manager

Swee Lin Wong – Director of H.R.

Department of Transportation

Matthew Knosp, Deputy Director of Human Resources, MassDOT

Gaming Commission

Katrina Jagroop-Gomes, Chief Information Officer and Department Security Officer

Human Resources Division

Deb Giacchino, Director of HRD Operations, Business Enterprise Applications Unit, Human Resources Division

2019-002

Executive Office of Health and Human Services – Access to MMIS and MA21 Applications

Repeat Observation: Yes

Observation

In 2019, management performed their first formal review of all users' access to MA21 and MMIS, remediating findings from prior years. As a result of this review, a large number of users (212 for MMIS and 210 for MA21) were identified that had a level of access not commensurate with their job responsibilities. As this was the first review of this nature, a large volume of users requiring access changes was anticipated. The users identified include those no longer employed with the agency and, irrespective of enabled access to MMIS and MA21, may not have been able to access those applications as their Active Directory network account was disabled. The agency proceeded to remove all unneeded access. However, no procedures were performed to determine whether the inappropriate access led to any unauthorized activity.

A user access review is a detective control that can identify users who have inappropriate access and whose accounts may have been used to perform unauthorized activity. Without following up on users identified as inappropriate during an access review the risk that unauthorized transactions go undetected increases.

Recommendation

We recommend that management:

- Enhance the MA21 and MMIS user access reviews to include analysis of activity to determine if a user's access was inappropriate. This could start with a review of the last login date of the user account in question and/or a review of the corresponding network account. If the review uncovered potential inappropriate access, further investigative procedures should be considered. The investigative procedures could be risk based to consider factors such as the level of access available.
- Consider to start the review earlier in the fiscal year to ensure all potential access issues can be addressed appropriately prior to 6/30 fiscal year-end.

Management's Response

In February 2019, the MassHealth Access and Controls (MH A&C) team conducted its first end-to-end User Access Review (UAR) which include a well-defined Impact Analysis procedure designed to investigate dormant system accounts. Results of the Risk Impact Analysis are archived to the team's central MassForge folder for recordkeeping. MH A&C active operational controls are documented in the Application Account Audit and Monitoring Procedure Guide as standard operating practices.

MH A&C will conduct its annual UAR in July – at the start of the new fiscal year. All recommendations noted above are in place. MH A&C believes the audit controls in place provide significant monitoring to identify and mitigate risky systems account access

Responsible Officials

Sheika Babin, MassHealth Systems Teams Lead

2019-003

Executive Office of Labor and Workforce Development – Segregation of Duties in Change Management

Repeat Observation: No

Observation

Two employees at the agency have the technical ability to develop changes and migrate these changes to the UI Online production environment. This enables these two users to circumvent change management controls that are intended to ensure that only appropriate tested and authorized changes are implemented into production. Management indicated that there are technical and operational limitations making it unfeasible to fully segregate the ability to develop and migrate changes.

Management reviewed all changes developed and migrated by these two employees and confirmed that there was no inappropriate activity and that all changes migrated were appropriate.

The risk increases that users migrate unauthorized changes to the production environment which could impact the integrity of data processing in the UI Online environment.

Recommendation

We recommend that management:

- Periodically review all changes migrated to production by individuals who also have the ability to develop changes and verify that the changes were appropriate.
- Continue to consider technical and organizational changes that would make it possible to fully segregate the technical ability to develop changes from the ability to migrate these changes to production.

Management's Response

Executive Office of Labor and Workforce Development (EOLWD) Information Technology (IT) is adopting a quarterly review of all changes by members of the Team Foundation Server (TFS) Release Team to ensure that the only items updated are the Department of Homeland Security Password changes, and any web or app configuration files. All items will have a corresponding TFS Defect item along with an associated ServiceNow Change Request documenting the items changed and the required approvals. Expected report to be completed by February 28, 2020.

EOLWD IT is reviewing with Microsoft regarding best practices for Release Management under the new Azure DevOps platform, and is determining if a new group can be created to just allow changes to any Web and App configuration files, separating the rele**a**se team from any future changes.

Responsible Official

Anthony Fantasia, EOLWD Chief Information Officer

2019-004

Executive Office of Labor and Workforce Development – Access to UI Online Application

Repeat Observation: No

Observation

A User Access Review is performed periodically for all users with access to the UI Online environment. In the review, UI Online Account Management generates a listing of users and their access and distributes this to a set of managers and directors for review of appropriateness. Managers and Directors are required to review the listing and proceed to make requests to IT for any required access. However, there currently is no procedure to ensure all managers and directors have completed the review and have made the requests to IT to remove any inappropriate access.

The risk increases that users with inappropriate access do not have their access removed as part of the periodic review.

Recommendation

We recommend that management revise the current review or institute an additional review that addresses the following:

- Performed at least annually
- Uses a risk based approach to focus on those users that have a level of access that presents the most direct risk to unauthorized transactions impacting state and federal regulations. A risk based approach will ensure a review that is operationally feasible and also mitigates the risk of unauthorized access
- Appropriately documented including review evidence of each individual that performs the review covering all users included in the review, as well as the completeness and accuracy of the reports used in the review.

Management's Response

Department of Unemployment Assistance (DUA) is designing an annual review process so that staff that have the ability to change or influence one of the following functions are reviewed annually:

- payment
- refund
- eligibility for determination
- employer liability
- wages collected influencing a monetary or employer's rate

Roles and functions will be reviewed by management annually. This is a detailed review per individual requiring a sign off by the executive director to confirm that each individual staff member should have the granted access.

Responsible Official

Cari Birkhauser, DUA Systems Integration Director

2019-005

Executive Office of Labor and Workforce Development – Database Administrative Access

Repeat Observation: No

Observation

A total of 12 users, including service accounts, have a level of administrative access to the UI Online database which allows these accounts to add/change/remove users and make significant configuration changes. We found 2 of the 12 users had inappropriate access as the individuals were on medical leave.

Management disabled the access of these individuals during the audit and were further able to determine that these accounts were not used since these employees went on medical leave.

Active administrative users that are unnecessary increase the risk of unauthorized access to the database, potentially resulting in a breach of data confidentiality, integrity and/or availability.

Recommendation

We recommend that management:

- Review current processes related to long-term leave and termination and integrate procedures to remove/disable all access – including administrative access to infrastructure components – of the individuals.
- Perform a periodic review of administrative access to all infrastructure supporting critical applications to validate the appropriateness of all such access.

Management's Response

Executive Office of Labor and Workforce Development (EOLWD) Information Technology (IT) is adopting a quarterly database admin access review and account audit with Smartronix Database Administrators and Account team. This quarterly review will validate the accuracy of the user accounts with DBA access and access defined to each user.

In addition, EOLWD is updating the network access onboarding and offboarding procedures to ensure that accounts are disabled in a timely manner either through Human Resources (HR) action (termination, resignation, retirement, medical leave, etc.) or through inactivity (failure to log in within an appropriate number of days).

Responsible Official

Anthony Fantasia, EOLWD Chief Information Officer

2019-006

Executive Office of Labor and Workforce Development – Access Removal upon Termination

Repeat Observation: No

Observation

Out of a total population of 115 employees with employee access to UI Online who were terminated between July 1, 2018 and June 30, 2019, KPMG identified 45 users who did not have access terminated in a timely manner. Timely for purposes of this audit was considered at most 3 business days after termination based on better practice for end-user accounts to systems that contain sensitive data. The users in question had their access terminated between 4 and 209 days after termination. These users may not have been able to connect to their UI Online account, as their Executive Office of Labor and Workforce Development (EOLWD) network account may have been disabled in a more timely fashion.

Removing access swiftly upon termination prevents inappropriate access by individuals who are no longer employed by the Commonwealth and thereby prevents unauthorized transactions in the UI Online application.

Upon investigation by management, they determined that there was no inappropriate activity by any of the 45 users.

Recommendation

We recommend that management:

- Investigate the possibility to automate the removal of user accounts upon termination so that exceptions due to human error are prevented.
- Re-iterate to all EOLWD personnel the importance of swiftly notifying UI Online administrators of termination so that access can be revoked accordingly.

Management's Response

The Department of Unemployment Assistance (DUA) currently receives a weekly report from EOLWD HR which details new hires and terminations. This report is used to determine if a former staff member has UI Online access and the access is subsequently restricted. A revised process has been agreed upon by EOLWD HR and DUA. Through this process, DUA will receive immediate notification from HR within if an employee has been terminated, or separates voluntarily, and UI Online access needs to be restricted.

DUA is in the process of exploring options for new technology and is limiting future financial investments made to the current UI Online system.

Responsible Officials

Cari Birkhauser, DUA Systems Integration Director

Cheryl Stanton, EOLWD Personnel Officer

2019-007

Office of Comptroller – Lease Standard

Repeat Observation: No

Observation

In June 2017, the GASB issued Statement No. 87, *Leases*. In addition to defining a lease arrangement, this Statement requires recognition of certain lease assets and liabilities for leases that previously were classified as operating leases and recognized as inflows or outflows of resources based on the payment provisions of the contract. The requirements of this Statement are effective for the fiscal year ending June 30, 2021.

In the prior year management letter, we recommended that the Commonwealth develop a project plan to incorporate the following:

- Identification of all leasing arrangements
- Analyze all leasing arrangements to determine if they meet the definition of a lease
- Documentation of procedures performed to identify and analyze all leases
- Establish a process to obtain all future leases, including documentation of such processes
- Analyze anticipated changes to existing financial reporting
- Communication of anticipated changes to existing financial reporting to relevant stakeholders
- Implementation of any necessary changes to the CAFR compilation process

Since then, there are additional implementation issues that the Commonwealth should consider while executing their project plan.

Embedded Leases

Contracts may contain leases that have not been identified under the current lease accounting guidance. These contracts may not use terms such as “lease” or “rent” that identify the embedded lease, and, given the limited impact under current guidance, governments may not have identified these embedded leases. However, identifying leases becomes more important under GASB 87. Embedded leases may be present in many different types of contracts, including IT service contracts, supply contracts, and transportation or construction arrangements.

This initial step of identifying “at-risk” classes of transactions should involve representatives from multiple departments as employees in operational capacities may be more familiar with the specific terms and deliverables of relevant contracts.

The search for embedded leases might begin by selecting a relevant sample of contracts in at-risk arrangements and expanding that sample as needed based on initial results – e.g. if initial reviews identify embedded leases, it will likely be prudent to expand the contract review to additional contracts within that class (or to add additional classes of transactions with a similar embedded lease risk profile). This process will frequently include significant efforts to review contracts and critically evaluate whether the terms convey control of the right to use an asset. This effort may require, especially initially, significant involvement of more experienced and technically proficient personnel. Ultimately, this process should continue until the Commonwealth is able to ensure that no material population of unidentified leases remains.

When an embedded lease is identified, the respective lease liability and lease asset should be calculated based on the particular terms and required payments within the contract. Because embedded leases are often part of contracts that include non-lease elements (e.g. services), it is important to remember that the contract price is required to be allocated to the lease and nonlease components.

Lease Recognition Threshold

Many lessees have expressed interest in using recognition thresholds for lease liabilities and the related lease assets under GASB 87. Question 4.23 of GASB Implementation Guide No. 2019-3 states that a recognition threshold may be applied, but the lessee should consider the quantitative and qualitative significance of the lease liability, in addition to the significance of the lease asset. Accordingly, we believe applying a recognition threshold will generally be acceptable. However, setting that threshold at an appropriate level may require substantial judgment, and it would generally not be appropriate to:

- Default to the capital asset capitalization threshold;
- Evaluate the effect of the threshold on a net basis (lease assets less lease liabilities); or
- Ignore the effect of the threshold established on financial statement disclosures.

It may be helpful for the Commonwealth to think about the lease liability first when establishing the recognition threshold. This is because we would expect it to be relatively rare that a government would conclude that its capitalization threshold for lease assets would be less than its recognition threshold for lease liabilities. Rather, the Commonwealth should generally first consider its recognition threshold for lease liabilities.

Electing a non-GAAP accounting policy to recognize leases only over a certain threshold may provide operational benefit to the Commonwealth. For example, use of a threshold, particularly if the Commonwealth’s non-GAAP policy includes both non-recognition and non-disclosure, may permit the Commonwealth to (not exhaustive):

- Avoid making various judgments and estimates (e.g. judgments such as whether a lease exists for certain contracts, determining discount rates); and
- Not accumulate and maintain some data it would otherwise need for disclosure purposes, such as information on variable payments.

However, it is possible that a recognition threshold will not provide significant benefit. It may be simpler to account for all leases consistently, particularly if leases are relatively ‘plain vanilla’ (i.e. are not difficult to identify and are not subject to frequent remeasurement or modification).

Recommendation

We recommend that management continue to implement this Statement and develop a robust process to analyze at-risk classes of transactions to help identify potential embedded leases.

Further, if the Commonwealth chooses to establish a lease recognition threshold, management should clearly document, by opinion unit, the qualitative and quantitative considerations used when establishing such a threshold. Additionally, as with all non-GAAP accounting policies, management should also establish an annual process to monitor the population of leases below the recognition threshold. This annual exercise would serve to help management identify instances where the unrecognized leases may exceed qualitative and quantitative thresholds and become material to a particular opinion unit.

Management's Response

The Financial Reporting Team is reviewing the requirements of this Statement and will begin the process of implementation during the spring of 2020. Part of that process may include procuring the services of an outside vendor to either assist with or completely implement the standard with management oversight. As work progresses CTR will remain in constant contact with KPMG.

Responsible Officials

Howard Merkowitz, Deputy Comptroller, CTR
Michael Rodino, Director of Financial Reporting, CTR
Pauline Lieu, Deputy Director of Financial Reporting, CTR

2019-008

Executive Office of Health and Human Services – Drug Rebates Accounts Receivable

Repeat Observation: No

Observation

During our audit, we found the Executive Office of Health and Human Services (EOHHS) did not maintain a complete list of invoice level detail supporting drug rebate accounts receivable as of June 30, 2019. The drug rebates invoice level detail is available real-time and was used by EOHHS to report the drug rebates accounts receivable as of June 30, 2019 to the Office of the Comptroller for financial reporting purposes. However, when a complete listing of invoices were requested for audit sampling purposes, EOHHS was only able to provide a listing of invoice level detail for the accounts receivable balances established between April 1, 2019 and June 30, 2019.

While EOHHS was able to provide sufficient appropriate documentation for the drug rebates accounts receivable, maintenance of complete balances as of 6/30/19 would aid efforts to analyze and validate the completeness and accuracy of the fiscal year end accounts receivable balance for financial reporting purposes.

Recommendation

We recommend that management enhance processes and internal controls over financial reporting to maintain documentation necessary to support the completeness and accuracy of drug rebate receivables reported to the Office of the Comptroller for financial reporting purposes.

Management's Response

MassHealth had invoice level detail in the pharmacy rebates system to support the complete balance of accounts receivable. MassHealth will ensure that the invoice level data is available in a single file to analyze and validate the completeness and accuracy of the fiscal year end accounts receivable balance for financial reporting purposes.

Responsible Officials

Mohamed Sesay, MassHealth Director of Finance