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

## Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

The Fiscal Committee of the General Court
State of New Hampshire:

We have audited, in accordance with the 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, the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of New Hampshire (the State) as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the State's basic financial statements, and have issued our report thereon dated December 20, 2019. Our report includes a reference to other auditors who audited the financial statements of the Liquor Commission, Lottery Commission, Business Finance Authority of the State of New Hampshire, Community Development Finance Authority, Pease Development Authority, Community College System of New Hampshire, New Hampshire Retirement System, New Hampshire Judicial Retirement Plan and the New Hampshire Public Deposit Investment Pool, as described in our report on the State's financial statements. This report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors. The financial statements of the New Hampshire Public Deposit Investment Pool and the Business Finance Authority of the State of New Hampshire were not audited in accordance with *Government Auditing Standards*, and accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with the New Hampshire Public Deposit Investment Pool and the Business Finance Authority of the State of New Hampshire.

### Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the State's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

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. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described in the accompanying schedule of findings and responses as items 2019-001 and 2019-002 that we consider to be significant deficiencies.

**Compliance and Other Matters**

As part of obtaining reasonable assurance about whether the State's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

**The State's Responses to Findings**

The State's responses to the findings identified in our audit are described in the accompanying schedule of findings and responses. The State'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.

**Purpose of this Report**

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the State's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Boston, Massachusetts
December 20, 2019

## Schedule of Findings and Responses

**2019-001 Department of Administrative Services (DAS) and Department of Revenue Administration (DRA)**
**Credit Carryovers**

*Background*

At the time a tax return is filed, a Credit Carryover represents the amount of overpaid Business Profit Taxes (BPT) and/or Business Enterprise Taxes (BET), a taxpaying entity elects to apply to future tax obligations rather than request a refund. Based on tax returns filed through June 30, 2019, the State estimated a gross Credit Carryover balance, as adjusted, of approximately $224 million.

The State's current accounting policy is to record a tax refund payable for Credit Carryovers only to the extent that Credit Carryovers exceed estimated incremental fiscal 2019 tax revenues from future audits. At June 30, 2019, the State recorded a net tax refund payable of $10 million dollars consistent with this policy.

*Observation*

At KPMG's request, the Department of Revenue Administration (DRA) took a fresh approach to its Credit Carryover policy and re-examined the gross components of the current year calculation.

First, the gross receivable component was reviewed. Based upon historical tax audit information, DRA estimated that approximately $214 million of incremental fiscal 2019 tax revenues will be generated by future tax audits/assessments. However, those tax audits by-and-large won't occur until fiscal 2020 and beyond. Moreover, the incremental tax revenue generated by such audits won't be fully realized until fiscal 2027.

Next DRA examined the $224 million of gross Credit Carryovers and determined that all but $85 million is expected to be applied towards fiscal 2019 tax obligations. In other words, of the $224 million gross Credit Carryovers at June 30, 2019, DRA estimates that $139 million will be applied to taxes earned by the State during fiscal 2019, predominately for first and second quarter tax periods from January 1st to June 30th of 2019.

*Recommendation*

We recommend that the State discontinue its past practice of offsetting Credit Carryovers with future tax audits due to the uncertainty and length of time involved in realizing the results of yet to be initiated tax audits.

KPMG also recommends that DRA continue to refine its analysis of gross Credit Carryovers. Some consideration should be given to developing a prior year trend analysis as well as to expanding the analysis of gross Credit Carryovers to include the impact on both the General Fund and the Education Trust Fund as BPT and BET revenues and related refunds should be appropriately recognized in both of those funds.

*Management Response*

Since fiscal year 2011, the State has conducted a detailed analysis addressing the accounting treatment of tax revenues under the modified accrual basis of accounting, as reported in the general and education trust funds. Each year, the State calculates the expected amount of overpaid taxes to be refunded (per RSA 71-C:4 requiring a report of the potential liability for credit carryovers from overpaid taxes), however, the State historically has not adjusted the cash basis tax revenues for this potential liability for refundable taxes. The state allows taxpayers to leave overpayments "on balance" with the Department of Revenue Administration (DRA), and extensive past history has shown that taxpayers do not generally request these funds to be refunded, but typically utilize credit carryovers to satisfy future quarterly estimate payments. Additionally, the State has empirical evidence that statutory audits result in the conclusion that taxpayers have underreported taxable income, resulting in an unrecorded receivable. This unrecorded receivable from taxpayer audits as compared to the unrecorded liability for credit carryovers, in most years, has been an excess of audit revenue over the credit carryover liability (discounted for the application of estimated payments). For those instances where the calculated credit carryover liability exceeds the calculated audit revenue, the State records a net

liability at the general fund level, which impacts budgetary surplus. The State, throughout its reporting history, has applied this accounting policy to maintain symmetry and recognize both of these elements, on a net basis.

During the course of the fiscal 2019 audit, it was determined that these two elements should be assessed separately, from an accounting perspective. Since future audit revenue has an extended period of availability out several years, it is unlikely the state would record enough audit revenue to offset the specific liability incurred at the fund level. In order to address the disparity, DAS intends to consult with DRA to determine the estimated credit carryover liability at the end of each fiscal year. This would include establishing certain assumptions based on taxpayer reported data as of fiscal year-end, as well as subsequent taxpayer filing patterns based on a multi-year historical analysis. This "lookback" analysis would provide a better methodology for capturing the true credit carryover liability, beyond what the DRA taxpayer system currently calculates for credit carryforward balances. The timing of such analysis would need to be determined based on availability of taxpayer filing data and the State's current statutory reporting deadlines.

The State's policy review would also include an evaluation of the State's period of availability for the recording of tax revenues and whether it should be extended beyond the established sixty days. This may result in capturing future revenues attributable to the current period that would offset current period liabilities, for which existing accounting policies do not allow the State to recognize in the current reporting year. This approach could result in reporting consistency with other states. However, the State would need to evaluate if the accounting treatment would be inconsistent with the State's budget methodology, which measures obligations on general and education trust fund surplus that are going to be satisfied from current financial resources. The State will also need to evaluate if sufficient data is available to determine the amount of credit carryover liability that would be attributable to both the general fund and education trust fund.

The State expects to conduct its review by June 30, 2020, with any resulting change in accounting policy implemented for the 2020 fiscal year.

**2019-002 Department of Health and Human Services (DHHS)**
**Capital Assets**

*Background*

The State's capitalization policy requires equipment to be capitalized when the individual item exceeds $10,000. Software is capitalized when the cost of externally purchased or internally developed is greater than or equal to $500,000. All other capital assets are capitalized when the cost of individual items or projects exceeds $100,000. Individual departments and agencies are responsible for maintaining accurate and complete records regarding the acquisition, status and disposal of all capital assets and to comply with all applicable accounting and regulatory requirements.

*Observation*

During testwork over capital assets at the Department of Health and Human Services (HHS), we noted that the agency had a backlog of software development projects in work-in-progress (WIP) that should have been capitalized over the past several years. During fiscal year 2019, HHS reviewed the backlog and as a result $49.7 million in software projects was removed from WIP, capitalized and then fully depreciated, as software projects have a pre-determined useful life of 5 years per the State's Long-Term Assets Policy and Procedures Manual, and these software projects were put in place more than 5 years ago. This resulted in the depreciation on these projects being fully expensed in fiscal year 2019 instead of in the years that the projects were being used.

*Recommendation*

We recommend that the Department of Health and Human Services develop formal policies and procedures for identifying completed software projects and removing the associated costs from software work-in-progress in a timely manner.

*Management Response*

DHHS management noted that previously there had been a lack of adequate standards at DHHS, in that not all functional areas were involved in the computer software capitalization reporting process. In addition, not all areas within DHHS had identified reportable software costs, with most of the attention given to the Medicaid IT systems. Throughout the past fiscal year, DHHS hired dedicated staff, who conducted a review and reconciliation of past IT projects, which resulted in the $49.7M correction entry for FY19.

Going forward, DHHS has established an internal process to review software-consulting contracts and differentiate between "design, development and implementation (DDI)" projects from regular maintenance operations (M&O) engagements. This distinction is included in the invoice coding, which allows DHHS financial managers to properly query and report the costs that meet the capitalization criteria set forth in the state's Long-Term Assets Policy manual. An additional review process has been established which includes a compilation of each division's data by the DHHS Financial Data Administrator, as well as review and approval by the DHHS Chief Financial Officer, prior to submitting capitalized assets and depreciation expense on the DAS Exhibit E.

# STATE OF NEW HAMPSHIRE

Management Letter

Fiscal Year Ended June 30, 2019

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

March 30, 2020

Management of the Department of Administrative Services
Honorable Members of the Fiscal Committee of the General Court
State of New Hampshire
Concord, New Hampshire

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the State of New Hampshire (the State) 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 State'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 opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State'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 December 20, 2019 on our consideration of the State's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be 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 the deficiencies in internal control as summarized in the accompanying attachment.

The State's responses to our comments and recommendations are described in the accompanying attachment. The State'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 is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

**Observation 2019-1: Department of Health and Human Services**
**Drug Rebates**

*Background*

The Medicaid Drug Rebate Program (MDRP) offsets the Federal and state costs of most outpatient prescription drugs dispensed to Medicaid patients. The Department of Health and Human Services (DHHS) is responsible for overseeing the State's drug rebate program which includes billing and collections of drug rebates. At fiscal year-end, DHHS compiles a calculation of drug rebates accounts receivable for Comprehensive Annual Financial Report (CAFR) financial reporting purposes.

*Observation*

During our testwork over the year-end receivable related to drug rebates we noted that DHHS inadvertently excluded certain invoices from its calculation and as a result the General Fund gross receivable was understated by $15.5 million. The Department of Administrative Services recorded a post-closing audit adjustment to correct the receivable recorded in the State's CAFR.

*Recommendation*

We recommend that the DHHS review its process for capturing all receivables required to be reported under generally accepted accounting principles (GAAP) and also institute a review process to ensure that receivables are properly captured and recorded.

*Management Response*

DHHS concurs with KPMG's observation related to drug rebates. The Department implemented a process to review receivables from all divisions at the end of the fiscal year 2019. We will continue to evaluate and monitor this process to ensure all receivables required to be reported in accordance with generally accepted accounting principles (GAAP) are properly captured. The Department is currently evaluating the drug rebate revenue cycle with our third-party pharmacy benefit manager. We will implement changes necessary to ensure accuracy and reliability of our drug rebates accounting information by the end of fiscal year 2020.

**Observation 2019-2: Department of Revenue Administration**
**Tax Receivables**

*Background*

During preparation of the State's Comprehensive Annual Financial Report (CAFR), the Department of Administrative Services' (DAS) Bureau of Financial Reporting (BFR) relies on tax estimates prepared by the Department of Revenue Administration (DRA) to record year-end tax receivables and the related revenue. While the BFR is responsible for inclusion of the estimates in the State CAFR, DRA is responsible for the completeness and accuracy of the underlying data. The two agencies collaborate in determining the appropriate CAFR entries.

*Observation*

The calculation of the tax accounts receivable is a complex, manual process involving large sets of data and as a result, the process is susceptible to error. The supporting calculations are compiled by one key individual at DRA and there is currently no review process in place over the data before it is sent to BFR. During our testwork over the year-end tax receivables we noted that the receivables in the General Fund and the Education Fund were overstated by $0.9 million and $0.9 million, respectively, due to computation errors in the compiling worksheets.

In addition to these computation errors we also noted the following:

A. There was insufficient evidence to support the 50% uncollectible estimate for tax notices in hearings.

B. There were inconsistencies in how DRA captures the amounts to be recorded for tax hearings/notices. Specifically, in relation to the amounts owed for hearings, DRA captures all tax types in the receivable, but for tax notices they exclude certain tax types (e.g. smokeless tobacco tax, real estate transfer tax, utility property tax, etc.) from the receivable. These exclusions equate to approximately $4.1 million of unrecorded receivables.

*Recommendation*

With the ongoing rollout of the new Revenue Information Management System (RIMS), we recommend that DRA and DAS take a "fresh" look at the process for estimating the State's taxes receivable. The estimation process should be simplified, if possible, and all final calculations compiled by DRA should be subjected to DRA management review to ensure that the data is complete, accurate and supportable prior to submission to BFR for inclusion in the State's CAFR.

*Management Response*

The DRA agrees with the recommendation. First, additional review processes will be put into place in the future in order to ensure accurate calculations. Second, the DRA will also work with BFR in order to review the estimation process. The goals of this review will include: (1) identifying ways to potentially account for actual figures that might be available during the audit that are not available prior to the deadline for completing calculations for BFR to use in the CAFR (this issue resulted in a portion of the "computation errors" identified in the audit; (2) identifying ways in which RIMS can improve the accuracy of the calculations and simplify the process; and (3) determining appropriate revenue thresholds for the inclusion of additional tax types in the calculations.

**Observation 2019-3: Department of Administrative Services Accounts Payable**

*Background*

At fiscal year-end, the Department of Health and Human Services (DHHS) provides the Department of Administrative Services (DAS) with a manual compilation of invoices that need to be accrued as part of the Comprehensive Annual Financial Report (CAFR) financial reporting process. The fiscal 2019 compilation documentation included invoices for both fiscal 2019 and fiscal 2020.

*Observation*

Although the listing did segregate which year the activity related to, the extraneous fiscal year 2020 information contributed to DAS incorrectly overstating fiscal 2019 General Fund accounts payable by $1.4 million.

*Recommendation*

We recommend that DAS review its procedures for recording manual accrual entries and ensure that a review process is in place to help ensure that recorded entries are accurate.

*Management Response*

DAS and DHHS concur with KPMG's observation related to the accounts payable accrual. The fiscal year 2020 transactions provided were part of the batched transactions interfaced between the subsystems and the State's primary financial accounting system NH First. DHHS provided the information so that the details would reconcile with NH First records. Going forward, DHHS will ensure the amounts to be accrued are explicitly stated when transmitting accrual files to the Department of Administrative Services (DAS). We will collaborate with DAS to improve the manual accrual process as needed.

**Observation 2019-4: Department of Environmental Services**
**State Revolving Fund - Unreconciled Variances**

*Background*

The State Revolving Fund (SRF), administrated by the Department of Environmental Services (DES), is reported as a major enterprise fund in the State's Comprehensive Annual Financial Report (CAFR). The SRF operates to provide loans to public water systems and local governments for wastewater treatment and safe drinking water systems. Funding for the SRF is obtained from the U.S. Environmental Protection Agency with matching funds provided by the General Fund, as well as from interest on outstanding loans. The State established the SRF as a separate enterprise fund in fiscal 2014 through a cash transfer from the General Fund.

*Observation*

The DES utilizes a sub-financial reporting system, Loan and Grants Tracking System (LGTS), to record detailed activity related to the SRF and on a monthly basis reconciles the LGTS activity to the State's general ledger, NH First. The LGTS system is used for financial statement reporting purposes in the CAFR. At June 30, 2019, the two systems did not agree. The DES staff reported the cause of the differences is unknown; however, the differences have existed for several years and the differences grew larger in 2019 than in the prior year.

*Recommendation*

We recommend the DES work with the Department of Administrative Services (DAS) to investigate the root cause of the differences and to adjust the accounting records as necessary.

*Management Response*

DAS and DES have collectively made efforts to identify transactions which may have resulted in cumulative differences between ending balances reflected in the LGTS system and the NH First general ledger. The NH First system incorporates a series of intercompany automated transactions which DAS believes have impacted the ending balances reflected in the NH First general ledger as of June 30, 2019. While the exact cause of the difference has not been identified, the DES will continue to work with the DAS to resolve this NH First issue.

**Observation 2019-5: Department of Health and Human Services**
**New Heights - General Information Technology Controls**

*Background*

The State of New Hampshire uses the New Heights application for eligibility determinations for programs that are in part funded by Federal awards. As part of our audit, we tested the General Information Technology Controls (GITC) related to the New Heights application for the following domains: Access to Programs and Data; Change Management; Computer Operations; Program Development.

*Observation*

The GITC testwork over the New Height application identified certain controls were not operating effectively for the period of July 1, 2018 - June 30, 2019, as noted below:

A. Privileged access rights to the New Heights application and related infrastructure should be restricted to users based on job function and responsibility. During our review, it was noted that 2 user accounts with privileged access rights to the backup scheduling tool belonged to employees whose employment had been previously terminated. KPMG did obtain systematic evidence for the exceptions identified to evidence that the access was not used subsequent to date of termination.

B. Access to the data center housing the New Heights application and related infrastructure should be restricted to individuals who require that access to perform their job roles and responsibilities. During our review, we identified two individuals (both external contractors) with access to the data center beyond the period of time for which the access was required to perform their job roles and responsibilities. The audit team obtained and reviewed systematic evidence for the 2 individuals and determined that the individuals did not access the data center subsequent to the period of time for which the access was required to perform their job roles and responsibilities. Further, subsequent to the identification of these exceptions, access rights to the data center for these 2 individuals was removed.

*Recommendation*

A. Management should reinforce policies and procedures relative to provisioning and de-provisioning controls to ensure access rights for terminated employees are removed in a timely manner for all applications, related infrastructure and tools and that privileged access rights to applications and related infrastructure and tools are restricted to current employees based on job roles and responsibilities.

B. Management should reinforce policies and procedures to strengthen controls to determine that access to the data center is appropriate based on job roles and responsibilities, and that access to the data center is removed in a timely manner when no longer necessary for the individual to perform their job roles and responsibilities

*Management Response*

A. and B.

User accounts are provided to identify authorized users of state network resources and provide access to applications, data and resources as required. In order to protect against unauthorized access, accounts must be maintained as requirements change and inactive accounts routinely identified, disabled and removed. If an employee has terminated service, no longer requires access due to responsibilities changing, or the contractor no longer requires access the central security management system will be updated accordingly. Periodic access reviews will be conducted by application owners to validate User Accounts ensuring synchronization of access with the centralized security management system. A log of when employees/contractors are given access and when they are disabled will be kept.

**Observation 2019-6: Department of Administrative Services**
**NH FIRST ERP System for the Financial Reporting, Time Reporting, and Human Resources/Payroll ERP System (ERP System) - General Information Technology Controls**

*Background*

The State of New Hampshire uses the NHFIRST ERP System (ERP System) for Financial Reporting, Time Reporting, and Human Resource/Payroll functions. As part of our audit, we tested the General Information Technology Controls (GITC) related to the ERP System for the following domains: Access to Programs and Data; Change Management; Computer Operations; Program Development.

*Observation*

The GITC testwork over the ERP System identified certain controls were not operating effectively for the period of July 1, 2018 - June 30, 2019, as noted below:

A. During our review, we noted that access to the NHFIRST ERP application was not removed in a timely manner for 2 of the 25 samples, with a duration of time between the date of termination and the removal of access ranging from 6 to 22 days. The audit team compared a list of terminated employees for the audit period to an active user listing for the ERP application and noted no additional exceptions. Furthermore, the audit team obtained and reviewed systematic evidence to determine that the user accounts related to the 2 identified exceptions were not accessed subsequent to the individual's date of termination.

B. Access to the data center housing the NHFIRST ERP application and related infrastructure should be restricted to individuals who require that access to perform their job roles and responsibilities. During our review, we identified two individuals (both external contractors) with access to the data center beyond the period of time for which the access was required to perform their job roles and responsibilities. The audit team obtained and reviewed systematic evidence for the 2 individuals and determined that the individuals did not access the data center subsequent to the period of time for which the access was required to perform their job roles and responsibilities. Further, subsequent to the identification of these exceptions, access rights to the data center for these 2 individuals was removed.

C. During not our review, we noted that the listing of application changes being reviewed by management was not complete and accurate. Subsequently, NHFIRST management generated a complete and accurate list of application changes and reviewed to validate that all changes promoted to the production environment were appropriate and authorized and no changes were developed and migrated by the same individual. Further, the audit team, on a sample basis, reperformed management's review of application changes to determine that the changes were appropriate and authorized, and that no changes were developed and migrated by the same individuals.

*Recommendation*

A. Management responsible for the NH FIRST ERP application should establish and enforce policies and procedures to ensure that notification of termination for users of the NH FIRST ERP application occurs in a consistent and timely manner, resulting in timely removal of access rights (in excess of read-only), as well as the removal of all access rights upon reaching 90 days post-termination.

B. Management should reinforce policies and procedures to strengthen controls to determine that access to the data center is appropriate based on job roles and responsibilities, and that access to the data

center is removed in a timely manner when no longer necessary for the individual to perform their job roles and responsibilities.

C. Management should continue to monitor a complete and accurate list of application changes to determine that changes are appropriateness and authorized, and that changes are not developed and migrated by the same individuals.

*Management Response*

A. Management has established and provided policies and procedures to ensure that notifications of terminations for users of the NH FIRST ERP application occurs in a consistent and timely manner. A part of the enforcement actions management has taken is to provide non-compliance reports on a periodic basis to State Agencies requiring rationale for non-compliance. These reports will now be sent out monthly to Agency HR staff to provide timely measurements of HR staff compliance to the termination transaction entry standard. The compliance reports reference both the means of compliance and importance of compliance with statewide policies regarding the initiation of termination transactions in the NH FIRST ERP application. Another specific corrective action being taken is to ensure all Agency HR staff understand the standard requirements to process the termination work unit to remove user system access in a timely manner. In addition, to improve reporting and tracking of agency provided non-compliance rationale, modifications were made in NH FIRST providing a limited number of mandatory standardized rationale categories to select from along with a comments section available for additional clarifying information. The standardized rationale and any comments provided have been automated into a report for Administrative Services Department review. Group review of the trends for non-compliance helps to identify areas of concern and possible training needs. The Division of Personnel plans to begin providing corrective training to Agency HR staff not in compliance. Ongoing communications between the Administrative Services Department, Division of Personnel, and State Agencies is seen as the key to achieving compliance goals.

B. User accounts are provided to identify authorized users of state network resources and provide access to applications, data and resources as required. In order to protect against unauthorized access, accounts must be maintained as requirements change and inactive accounts routinely identified, disabled and removed. If an employee has terminated service, no longer requires access due to responsibilities changing, or the contractor no longer requires access, the central security management system will be updated accordingly. Periodic access reviews will be conducted by application owners to validate User Accounts ensuring synchronization of access with the centralized security management system. A log of when employees/contractors are given access and when they are disabled will be kept.

C. Management will ensure that a quarterly NH FIRST List of Production Application Changes report is produced and signed off by the appropriate parties in a timely manner. The review will certify that changes are appropriate and authorized and that changes are not developed and migrated by the same individuals.

**Observation 2019-7: Department of Education**
**Grants Management System (GMS) - General Information Technology Controls**

*Background*

The State of New Hampshire uses the Department of Education (DOE) Grants Management System (GMS) application for eligibility determinations for programs that are in part funded by Federal awards. As part of our audit, we tested the General Information Technology Controls (GITC) related to the GMS application for the following domains: Access to Programs and Data; Change Management; Computer Operations; Program Development.

*Observation*

The GITC testwork over the GMS application identified certain controls were not operating effectively for the period of July 1, 2018 - June 30, 2019, as noted below:

A. Access to the data center housing the GMS application and related infrastructure should be restricted to individuals who require that access to perform their job roles and responsibilities. During our review, we identified two individuals (both external contractors) with access to the data center beyond the period of time for which the access was required to perform their job roles and responsibilities... The audit team obtained and reviewed systematic evidence for the 2 individuals and determined that the individuals did not access the data center subsequent to the period of time for which the access was required to perform their job roles and responsibilities. Further, subsequent to the identification of these exceptions, access rights to the data center for these 2 individuals was removed.

B. Access to the GMS application and related infrastructure should be removed in a timely manner. During our review, we noted that access to the GMS application was not removed in a timely manner for 1 of the 3 samples, with a duration of time between the date of termination and the removal of access of 40 days. The audit team compared a list of terminated employees for the audit period to an active user listing for the GMS application and noted 3 additional exceptions with a duration of time between the date of termination and the removal of access ranging from 10 to 941 days. Furthermore, the audit team obtained and reviewed systematic evidence to determine that the user accounts related to the 4 identified exceptions were not accessed subsequent to the individual's date of termination.

C. Evidence supporting the appropriate requests, testing, and approvals relative to changes made to the database layer for the GMS application should be retained. During our review, we noted that, for 7 of 15 samples, evidence supporting the request, testing, and approval of changes to the database layer were not retained. Subsequent to the identification of this exception, management performed a review of all database changes noting that all changes migrated to production were authorized and appropriate and followed the change management process. Further, the audit team reviewed management's assessment to determine all database changes were reviewed for appropriateness, noting no further exceptions.

*Recommendation*

A. Management should reinforce policies and procedures to strengthen controls to determine that access to the data center is appropriate based on job roles and responsibilities, and that access to the data center is removed in a timely manner when no longer necessary for the individual to perform their job roles and responsibilities.

B. Management responsible for the GMS application should establish and enforce policies and procedures to ensure that notification of termination for users of the GMS application occurs in a consistent and timely manner, resulting in timely removal of access rights.

C. Management responsible for the GMS application should establish and enforce policies and procedures to ensure that evidence supporting that each change made to the GMS application and related infrastructure followed the change management workflow, is retained.

*Management Response*

A. The DOE understands this issue has been addressed by the State Agency responsible for controlling access to the data center. The DOE has no control over access to the data center.

B. Toward the end of the FY19 an update was made to how the notification of terminated employees (with respect to MyNHDOE role access) was handled. Prior to the update, when an employee was terminated the termination was communicated from the DOE Human Resources staff via email to DoIT staff. The update made at the end of FY19 changed this process. The new process became part of the established Help Desk ticket process for Domain account removal (desktop logins). Currently, when the DOE Human Resources staff submits a ticket for an employee termination, DoIT also receives a ticket to review/remove MyNHDOE access for the terminated employee. A search for a MyNHDOE account/roles for the terminated employee is then completed and roles/accounts are disabled as needed. Then the ticket is assigned to the DoIT Database Administrator (DBS) to review database level access and disable this access as needed. This update, along with a change/addition of staff in the DOE Human Resources Department, has greatly increased the notification time and awareness of employee terminations. The DOE Human Resources staff is currently working on a written employee on-boarding/off-boarding process. The submission of a Help Desk ticket to DoIT relative to employee terminations will be included in that off-boarding process. The DOE will ensure that the submission of a Help Desk ticket to DoIT as it relates to the termination of an employee is included in the Human Resources off-boarding process no later than April 30, 2020.

C. The DOE embedded DoIT group is responsible for completing patching and updates for SQL Server while the Central DoIT System Administration Windows group is responsible for operating system level infrastructure including patching, testing and deploying updates. The DOE has worked with both DoIT groups, which identified existing policies and procedure that address the resolution of the finding. The first procedure entitled *Windows 2016 Configstandards* outlines the common, uniform standard for Microsoft Windows 2016 Servers maintained by the DoIT. The second procedure entitled *DOE Microsoft SQL Server Release and Patching Process* provides a description of the process used by DoIT to update a SQL server. With the development and implementation of these two documents, the finding should be resolved.