AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2020

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

This report summarizes our fiscal year 2020 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively, these four agencies spent $18.5 billion or 96 percent of the total expenses for agencies under this secretariat.

- *Department of Behavioral Health and Developmental Services*
- *Department of Health*
- *Department of Medical Assistance Services*
- *Department of Social Services*

Our audits of these agencies for the year ended June 30, 2020, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, each agency's financial systems, and in supplemental information and attachments submitted to the Department of Accounts;

- 53 findings involving internal control and its operation necessary to bring to management's attention. Of these findings, five are considered to be material weaknesses;

- 44 of the 53 findings are also considered to be instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- adequate corrective action with respect to audit findings reported in the prior year that are not referenced in this report.

Our report also includes a Risk Alert, primarily applicable to the Department of Behavioral Health and Developmental Services, that relates to a settlement agreement between the Commonwealth of Virginia and the federal government. This Risk Alert was included in our report last year, and we continue to report it given the significance of the issue to the Commonwealth and the upcoming deadline, which requires compliance by 2021 for the Commonwealth to exit court oversight.

-TABLE OF CONTENTS-

RISK ALERT

During the course of our audit, we encountered issues that are beyond the corrective action of the Department of Behavioral Health and Developmental Services (DBHDS) management alone and require the action and cooperation of management, the Department of Medical Assistance Services (Medical Assistance Services), the General Assembly, the Secretary of Health and Human Resources, and the Administration. The following issues represent such a risk to DBHDS and the Commonwealth during fiscal year 2020.

Continue to Comply with the Department of Justice Settlement Agreement

Repeat: Yes (first issued in fiscal year 2016)

In January of 2012, the Commonwealth of Virginia and the United States Department of Justice (DOJ) reached a settlement agreement to resolve a DOJ investigation of the Commonwealth's system of services for individuals with developmental disabilities. This settlement agreement addressed the Commonwealth's compliance with both the Americans with Disabilities Act and the U.S. Supreme Court Olmstead ruling requiring individuals be served in the most integrated settings appropriate to meet their needs. The major highlights of the settlement include the expansion of community-based services through waiver slots; the establishment of an extensive discharge process for individuals in the state training centers; and strengthened quality and risk management systems for community services.

The Commonwealth continues to work with the DOJ and an independent reviewer to meet the terms of the settlement agreement. Under the agreement, the Commonwealth was expected to demonstrate full compliance by June 30, 2020, in order to sustain a full year of compliance to exit court oversight of the agreement in 2021. DBHDS finalized compliance indicators with DOJ in January 2020 specifying exactly what the Commonwealth must do to achieve compliance; however, the Commonwealth has not yet achieved full compliance. These compliance indicators increase reporting requirements and create a need for data quality systems to comply with negotiated metrics.

Once the court finalized compliance indicators, DBHDS began working with a consultation firm to implement a project management plan resulting in increased transparency, collaboration, and accountability with all involved parties. However, the COVID-19 pandemic has created additional barriers and noncompliance as outlined in the independent reviewer's two most recent reports to the court on the Commonwealth's compliance with the settlement agreement. To mitigate the spread of COVID-19, the Commonwealth temporarily suspended certain in-person contacts as necessary to protect the vulnerable population of individuals and the staff who serve them. There is further risk of noncompliance if DBHDS does not receive adequate funding at the appropriate time for personnel, information technology (IT) resources, and other resources necessary to implement the compliance indicators. Loss or reduction in funding could extend the time that it takes for DBHDS and Medical Assistance Services to implement programs and reach the requirements of the DOJ settlement agreement. Specifically, the involved parties need funds to:

- address critical and ongoing one-time requirements to continue building community capacity as well as remain compliant with other aspects of the settlement agreement;

- support facility transition waiver slots to enable DBHDS to continue moving individuals out of the training centers and children out of nursing homes and intermediate care facilities into community-based services as well as additional community intellectual and developmental disability (ID/DD) waiver slots to help reduce the growing waiting list for services;

- address adequate provider capacity in the areas of nursing, employment, and community engagement; and

- maintain a functioning quality management system.

If DBHDS does not achieve and maintain compliance with the requirements of the settlement agreement, an extension of the agreement or fines and penalties to the Commonwealth are possible. We continue to encourage DBHDS, Medical Assistance Services, the General Assembly, and the Administration to work together to ensure that DBHDS has the funds and support it needs to continue to comply with the settlement agreement and provide services to individuals in the appropriate setting.

AUDIT FINDINGS AND RECOMMENDATIONS

Audit findings and recommendations are reported in two different sections below and are organized by agency. Each individual finding reported includes information on the type of finding and the severity classification for the finding, where applicable. The severity classifications are discussed in more detail in the section titled "Independent Auditor's Report."

Current year findings, as well as prior year findings where there has been limited to no corrective action taken, are reported in the section entitled "Internal Control and Compliance Findings and Recommendations." Prior year findings where corrective action is ongoing are reported in the section entitled "Status of Prior Year Findings and Recommendations" and include information on progress to date.

The following table summarizes the total number of findings by agency including how many repeat findings are reported and how many findings are classified as material weaknesses, which is the most severe classification.

Summary of Findings by Agency

	Total Number of Findings	Number of Repeat Findings	Number of Material Weaknesses
DBHDS	16	13	1
Health	10	7	1
Medical Assistance Services	10	4	2
Social Services	17	15	1
Total	**53**	**39**	**5**

It should be noted that the material weakness for DBHDS is considered material non-compliance and will result in a qualified opinion for the Mental Health Block Grant federal program in the Commonwealth's Single Audit report for the year ended June 30, 2020. The Single Audit report will be available on APA's website at www.apa.virginia.gov in February 2021.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Ensure Consistent Application of Subrecipient Monitoring Controls

Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

DBHDS' Division of Administrative Services (Administrative Services) and Division of Community Services (Community Services) do not adequately monitor consumer-run peer support subrecipients of federal funds provided by Catalog of Federal Domestic Assistance 93.958 Block Grants for Community Mental Health Services (Mental Health Block Grant). During fiscal year 2020, Administrative Services disbursed $1.4 million in Mental Health Block Grant funds to eight entities as contractors to provide consumer-run peer support programs.

DBHDS performed a subrecipient or contractor determination in fiscal year 2015 and made an overall determination that these entities were subrecipients. Although this determination was made in 2015, DBHDS did not consistently treat the entities as subrecipients between fiscal years 2016 and 2020. It should be noted that DBHDS maintains current contracts with these entities, and that the contracts first went into effect during fiscal year 2015. During fiscal year 2020, DBHDS decided to allow the current contracts to expire before reevaluating subrecipient or contractor relationships. Community Services completed a checklist to evaluate the relationship once the contracts expired, and in this process for five entities, all five were identified as subrecipients during fiscal year 2021.

As a result, we determined that Administrative Services and Community Services did not consistently identify these subawards or monitor subrecipients as required by the Code of Federal Regulations (C.F.R.).

- Administrative Services did not include these eight entities in their subrecipient risk assessment. 45 C.F.R. § 75.352(6)(b) requires an evaluation of each subrecipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring described in paragraphs (d) and (e) of this section.

- Four of the eight contracts (50%) with these entities did not include any reference to the required federal award information. The four other contracts included reference to federal award information from prior award periods. 45 C.F.R. § 75.352(a) requires that every subaward is clearly identified to the subrecipient as a subaward and includes the required federal award information at the time of the subaward and if any of these data elements change, include the changes in subsequent subaward modification.

- Community Services contract administrators manage these eight entities through review of quarterly reports outlining the peer support services provided. DBHDS is unable to provide documented evidence of their monitoring. Specifically, 45 C.F.R. § 75.352(6)(d) requires monitoring the activities of the subrecipient as necessary to

ensure that the subaward is used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved. Monitoring of the subrecipient must include review of financial and performance reports, as well as follow up to ensure that the pass-through entity took timely and appropriate action in response to deficiencies detected through audits, on-site reviews, and other means.

- Additionally, 45 C.F.R. § 75.352(6)(e)(1)(2) states that depending upon the pass-through entity's assessment of risk posed by the subrecipient, the following monitoring tools may be useful for the pass-through entity to ensure proper accountability and compliance with program requirements and achievement of performance goals: providing subrecipients with training and technical assistance and performing on-site reviews of the subrecipient's program operations.

Administrative Services completes a risk assessment of subrecipients receiving Mental Health Block Grant funds as required by 45 C.F.R. § 75.352(6)(b); however, since DBHDS did not treat these eight entities as subrecipients during fiscal year 2020, they were not included in the risk assessment. Federal award information was inconsistent between contracts because DBHDS has not updated contract terms throughout the renewal periods. Without evaluating the risk of these entities and monitoring them accordingly, DBHDS is unable to ensure that the subaward is used for authorized purposes in compliance with Mental Health Block Grant requirements. Because DBHDS is not consistently communicating federal award requirements to subrecipients, there is an increased risk that subrecipients are not properly identifying and accounting for Mental Health Block Grant funds, which could result in unallowable or questionable costs.

DBHDS should ensure that Administrative Services and Community Services perform a risk assessment over all subrecipients and complete monitoring activities in accordance with 45 C.F.R. § 75.352(6)(b)(d)(e). Additionally, DBHDS should properly communicate subawards to subrecipients in accordance with 45 C.F.R. § 75.352(a). DBHDS should improve the coordination and oversight of subrecipient monitoring to ensure Administrative Services and Community Services apply consistent subrecipient monitoring controls in accordance with C.F.R. requirements.

Perform Independent Peer Reviews of Community Mental Health Programs
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS Community Services does not perform independent peer reviews for community mental health programs funded by the Mental Health Block Grant. Community Services has not implemented a process for independent peer reviews of community mental health programs.

42 C.F.R. § 300x-53 states that for the fiscal year for which the grant involved is provided, DBHDS must provide for independent peer review of not fewer than five percent of the entities providing

services under such programs to assess the quality, appropriateness, and efficacy of treatment services. Further, DBHDS maintains a contractual agreement with subrecipients, which identifies DBHDS' responsibility to provide for an annual independent peer review of community mental health for at least five percent of subrecipients.

Without performing an independent peer review of community mental health programs funded by the Mental Health Block Grant, DBHDS cannot ensure that subrecipients are offering quality and appropriate services that align with the program objectives. Community Services was unaware of the requirement to perform independent peer reviews for the Mental Health Block Grant; therefore, did not implement an independent peer review process. Community Services should develop and implement a process to provide for independent peer reviews of at least five percent of subrecipients providing community mental health programs funded by the Mental Health Block Grant.

Implement Standardized Off-Boarding Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)
Prior Titles: Improve Controls over Access to the Commonwealth's Retirement Benefits System, Improve Access Controls over the Internal Accounting and Patient Revenue Systems, Promptly Remove Commonwealth's Accounting and Financial Reporting System User Access, Improve Access Controls over the Commonwealth's Payroll System, Retain Documentation of Property Collection and Removal of Terminated Employee Badge Access, and Ensure Terminated Employees Are Properly Classified in the Payroll System.

DBHDS is not properly terminating employees according to their disparate termination policies and procedures. While DBHDS does have termination procedures, including the required completion of termination checklists, checklists vary from facility to facility and Central Office, are not robust, and do not include access removal for all information systems. During our review, we identified the following deficiencies:

- DBHDS did not complete termination checklists confirming the collection of Commonwealth property, such as keys and electronics, and removal of building access for 18 of 40 (45%) terminated employees. For seven terminated employees who abandoned the job, DBHDS did not complete the termination checklist confirming building access removal.

- DBHDS did not change the employment status to "inactive" in the Commonwealth's payroll system for seven terminated or inactive employees.

- DBHDS did not timely request removal of system access to the Commonwealth's accounting and financial reporting system for four of nine (44%) users. Access removal requests for these users ranged between two to 28 days post separation.

- DBHDS did not timely remove system access to the internal accounting and financial reporting system for three of seven (43%) users. Access removal for these users ranged between two to 34 days post separation.

- DBHDS did not timely remove system access to the internal patient revenue system for six of ten (60%) users. Access removal for these users ranged between two to 150 days post separation or change in job duties.

- DBHDS did not timely request removal of system access to the Commonwealth's payroll system for five of five (100%) users. Access removal requests for these users ranged between two to 149 days post separation.

- DBHDS did not timely request removal of system access to the Commonwealth's human resource system for one of two (50%) users. Access removal request for this user took 60 days.

- DBHDS did not timely request or remove system access to the Commonwealth's retirement benefits system for nine of 14 (64%) inactive users. Access removal for these users ranged between ten to 892 days post separation.

- DBHDS has not removed system access for one active Commonwealth's retirement benefits system user who terminated during fiscal year 2018.

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 50320 recommends agencies develop a termination check-off list to complete as part of the termination process to include the collection of outstanding uniforms, badges, keys, etc. CAPP Manual Topic 50320 also states that agencies must verify that information in the Commonwealth's payroll system concerning terminated employees is complete, properly authorized, and entered accurately into the system. Further, the Commonwealth's Information Security Standard, SEC 501 (Security Standard) Section PS-4, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual.

DBHDS experienced significant turnover during the period under review, as evidenced by the fact that DBHDS employs over 6,000 employees and had over 1,700 separations during this period. Without proper and sufficient internal controls over terminated employees that ensure the return of Commonwealth property and removal of all access privileges, DBHDS is increasing the risk that terminated employees may retain physical access to Commonwealth property and unauthorized access to state and internal systems and sensitive information. For DBHDS, the exposure to risk is further increased, due to the secure nature of the individual facilities.

DBHDS acknowledges that these issues occurred because they do not have an overarching and consistent off-boarding procedure across the agency. The Human Resources Department (Human Resources) at Central Office is working on providing baseline procedures to the facilities.

DBHDS should implement a standardized off-boarding procedure across its facilities and Central Office. Human Resources at Central Office should provide baseline procedures to facilities to ensure all CAPP Manual requirements are met. These procedures should at a minimum include: the collection of Commonwealth property and the timely removal of building access for terminated employees, modifications of employment status, and timely removal of all information system access in accordance with the Security Standard. Furthermore, these procedures should speak to certain cases such as job abandonment. Central Office and management across all DBHDS facilities should ensure their facility implements and follows termination policies and procedures.

Improve Controls Over Financial Systems Reconciliations

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

Individual DBHDS facilities who share a fiscal department do not have adequate controls in place to ensure reconciliations between DBHDS and the Commonwealth's financial systems are properly reviewed. Specifically, we found that two of five facilities (40%) tested did not perform a review of the fixed assets reconciliation. Further, the same two facilities did not perform a review of the monthly financial reconciliation between the agency's internal and the Commonwealth's accounting and financial reporting system.

CAPP Manual Topic 20905 states that the fiscal officer must certify that all account balances for the agency are correct. By submitting the Certification of Agency Reconciliations to the Department of Accounts (Accounts), the agency is certifying that management accepts responsibility for the integrity and objectivity of the financial transactions provided to the Comptroller. Further, the internal policies and procedures for the facilities noted require that the reconciliation of the internal fixed assets and financial systems be submitted upon completion to the Financial Services Manager or Financial Services Director for review and online certification. The lack of a proper review of reconciliations to the Commonwealth's accounting and financial reporting system increases the risk of misstatements to go unnoticed.

Both facilities, which share a fiscal department, have experienced significant turnover leading to an influx of responsibilities on management and the review of reconciliations was not made a priority. Management should ensure that proper reviews are performed and reinforce policies and procedures over system reconciliations.

Perform and Document Commonwealth's Retirement Benefits System Reconciliations
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)

Individual facilities within DBHDS did not adequately perform and document reconciliations between the Commonwealth's retirement benefits system and other systems during fiscal year 2020. Specifically, we noted the following at the five facilities tested:

- One of five facilities (20%) did not perform a reconciliation of the credible compensation between the Commonwealth's human resource and retirement benefits systems prior to confirming the contribution.

- Two of five facilities (40%) did not clear reconciling creditable compensation items before confirming the contribution.

- Two of five facilities (40%) have not reviewed or addressed exception items identified on the Commonwealth's payroll system automated reconciliation reports (automated reconciliations) since November 2019. The three other facilities (60%) did perform a proper review; however, they did not clear exceptions timely.

- Facilities did not confirm the contribution snapshot within the required timeframe for nine out of 60 months (15%) at the five facilities tested.

All five facilities tested have reconciliation policies and procedures; however, the Payroll and Human Resource departments do not appear to be following policies and procedures that are in place to ensure the proper performance of the Commonwealth's retirement benefits system reconciliations.

CAPP Manual Topic 50410 states that agencies should perform a reconciliation of creditable compensation between the Commonwealth's human resource and retirement benefits systems monthly before confirming the contribution. Further, CAPP Manual Topic 50410 describes each of the automated reconciliations and the actions agencies should take to promptly clear exception items identified. Improper reconciliation processes can affect the integrity of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire Commonwealth. Since the Virginia Retirement System (VRS) actuary uses retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements.

Additionally, CAPP Manual Topic 50410 requires agencies to confirm retirement contributions by the 10th of the following month in order to maintain compliance with the deadline and procedures established by VRS. Not reviewing or reconciling the contribution snapshot prior to confirmation deadline can result in incorrect payroll deductions and retroactive collections.

Individual facilities' staff were unsure of how to perform several components of the reconciliation process due to a lack of training; therefore, they did not properly perform pieces of the reconciliation process during the fiscal year. As a result, certain facilities decided to cease the review of the automated reconciliations for the remainder of the fiscal year. Additionally, due to turnover, new staff did not perform parts of the reconciliation. Responsibilities for the reconciliation are not clearly delineated between the Payroll and Human Resources departments at some facilities, which contributed to staff not timely clearing exceptions. Staffing shortages and competing priorities in the Fiscal Department were the primary cause for the late contribution snapshots.

Management across all DBHDS facilities, not just those reviewed, should ensure that staff perform and document monthly reconciliations between the Commonwealth's retirement benefits system and other systems. Management should ensure that staff follow policies and procedures. The Payroll and Human Resources departments should provide adequate training to staff to ensure that they know how to properly perform the reconciliation process. When clearing exceptions, facility staff should work together to document the reason for the exception and the remediation activities performed. Management should implement corrective action to ensure that the contribution snapshot is confirmed by the 10th of the following month.

Improve Controls over Payroll Reconciliations
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

DBHDS is not properly performing payroll reconciliations as required by the CAPP Manual. Due to turnover during the time period tested, two of the five facilities tested (40%) were unable to provide documentation to support the required monthly Report 10 to Report 33 reconciliation, to include running control totals of the key control fields that must be reconciled monthly. These two facilities share a fiscal department. Further, one other facility is maintaining key control field totals for reconciliation quarterly instead of monthly.

CAPP Manual Topic 50905 requires that key control totals be maintained and updated every time payroll is processed, or monthly, in order to facilitate the Report 10 to Report 33 reconciliation. CAPP Manual Topic 50905 also requires a monthly reconciliation of Report 10 to Report 33 to help identify potential problems with payroll records such as pre-tax deductions not being properly taxed, manual payment processing that affected taxable fields incorrectly, or improper withholding of certain taxes. Furthermore, not performing the reconciliation may cause errors or discrepancies in either system to go undetected.

Central Office should develop baseline payroll reconciliation policies and procedures based on CAPP Manual Topic 50905 and distribute them to the facilities. These procedures should require completion and retention of monthly Report 10 to Report 33 payroll reconciliations and running control totals.

Improve Controls over Payroll Certifications
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

DBHDS should continue improving controls over payroll certifications. All five facilities tested have policies and procedures in place; however, they do not align with all requirements of the CAPP Manual. Specifically, we found the following:

- Two of the five facilities (40%) do not have adequate policies and procedures over the payroll certification process that reflect procedures performed.

- Policies and procedures at all five facilities do not address the post-certification review of the statewide comparison of the Commonwealth's payroll and human resources systems identifying unresolved exceptions.

- All five facilities did not review all necessary reports during the pre- and post-certification process.

- Two of the five facilities (40%) were unable to provide documentation to support actions taken in response to exceptions identified during post-certification.

The exceptions noted at the facilities stemmed from inadequate policies and procedures, as well as turnover within payroll departments. DBHDS Central Office developed and distributed a post-certification checklist to all facilities during the fiscal year under audit outlining the post-certification report review requirements. Three of the five facilities tested have implemented the checklist in their post-certification process; however, two of these three facilities did not implement it until after the period under audit.

CAPP Manual Topic 20905 requires that agencies have written policies and procedures separate from the CAPP Manual for all processes. CAPP Topics 50810, 50815, and 50820 outline procedures over the certification process, including pre- and post-certification requirements. CAPP Topics 50810 and 50820 require the review of specified reports from the Commonwealth's payroll system during payroll pre- and post-certification review, respectively.

Inadequate policies and procedures expose the agency to unnecessary risk of performing payroll certifications improperly. In addition, written procedures reduce the impact that turnover has on institutional knowledge. Central Office should develop baseline payroll certification policies and procedures to align with the requirements of the CAPP Manual. Policies and procedures should include all necessary pre- and post- certification review requirements to help ensure complete and accurate payrolls. Further, DBHDS facilities should retain documentation to support actions taken in response to exceptions identified in post-certification.

Properly Approve and Monitor Administrative Employee Overtime
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

DBHDS should improve controls over employee overtime. We performed an analysis of employee overtime at the DBHDS facilities and Central Office and selected 18 employees for further testing. During our review, we found that six employees were either improperly paid overtime or worked an excessive amount of overtime during the fiscal year that was not properly approved or was not reasonable in relation to job responsibilities. Specifically, we identified the following exceptions at three DBHDS facilities tested:

- Four out of 18 employees (22%) worked overtime hours that were not properly approved by the department head or their designee.

- Three out of 18 employees (17%) worked overtime that is unreasonable in relation to the employee's responsibilities. The overtime payment for one of these employees exceeded $23,000 or 84 percent of the employee's regular pay.

- One out of 18 employees (6%) had overtime that was found to be unreasonable since the employee received a duplicate payment for overtime of over $600.

The Department of Human Resource Management Policy 1.25, Hours of Work, states that non-exempt employees must not work additional hours that have not been authorized by management. Both facilities with exceptions related to overtime approval and reasonableness have internal policies and procedures, which require the pre-authorization of overtime hours. Both facilities stated that supervisors verbally approved overtime; however, neither facility could provide the proper documentation. Without proper authorization of overtime there is an increased risk of improper payment of overtime hours that are not reasonable in relation to job duties.

In addition to the reasoning stated above for overtime not being properly approved, there were varying reasons for overtime being unreasonable in relation to job responsibilities. Based on the explanation received from one facility, the excessive overtime resulted from an employee working special events; however, this did not align with the job responsibilities within the employee's work profile. Therefore, the overtime could not be properly substantiated. Two of the employees with unreasonable overtime at another DBHDS facility were identified as exceptions in the prior year audit for no pre-approval of overtime hours. Following the previous fiscal year under audit, the DBHDS Office of Compliance, Risk Management, and Audit performed an investigation to address the potential unreasonable overtime hour concerns of these employees. Due to a misunderstanding and inexperience with the type of change in employment status, an employee at the last facility received a duplicate payment for overtime, which the facility was unaware of until we brought it to their attention.

DBHDS facilities should improve controls over employee overtime by properly approving and monitoring employee overtime hours. DBHDS facilities should retain documentation to support the authorization and reasonableness of overtime hours. When possible, DBHDS should allocate additional staff as needed to mitigate excessive overtime hours on existing staff.

Strengthen Controls over Commitments Reporting
Type: Internal Control
Severity: Material Weakness
Repeat: No

The Department of Health (Health) needs to strengthen controls over financial information reported to Accounts. Health submits financial information on year-end commitments to Accounts who then uses this information in preparation of the Commonwealth's financial statements. Staff did not include commitments due to the regional Emergency Medical Services Council (Council) in their initial submission. As a result, total commitments were understated by $18.4 million and the information had to be resubmitted.

Health's financial information is material to the Commonwealth's financial statements, so it is essential for Health to have strong financial reporting practices. Policies and procedures over financial reporting information, as a best practice, should be detailed and thorough with a sufficient review process to prevent and detect potential errors and omissions. As a result of this error, Health staff had to resubmit information to Accounts causing inefficiencies for Health's staff as well as delays for Accounts' staff. Omitting this financial information could cause inaccurate financial information to be reported in the Commonwealth's financial statements.

There are multiple factors that contributed to the error. First, the Council's contract renewals only occur every three to five years, so staff are not as familiar with the reporting implications. Additionally, the contract modification was signed on the last day of the fiscal year and dealt with additional funds related to the public health emergency, which was an extenuating circumstance. Finally, there was a lack of communication within the Council that also contributed to the omission.

The Council compiles the information initially and sends this to Health. Management should strengthen their controls to ensure that all relevant staff among Health and the Council review and communicate about potential commitments before this information is submitted to Accounts.

Improve Information Technology Change Management Process for a Sensitive System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Health does not have an effective IT change management process that includes the minimum requirements of the Security Standard, for one of their sensitive systems. The IT change management process contains key controls that evaluate, approve, and verify configuration changes to software applications that may impact an organization's information security posture.

We identified five control weaknesses and communicated them to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires

agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Health's information systems and data.

Health should develop a plan to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. Improving the IT change management process for this system will decrease the risk of unauthorized modifications and help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Strengthen Process over Employee Separations
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Health staff did not properly perform all off-boarding procedures for employees who separated from the agency. During our review, we identified the following issues related to the off-boarding process for terminated employees:

- Health did not process the final leave payouts for four of 23 (17%) employees in a timely manner. Employees were paid the second pay period after their termination date, which is not in compliance with requirements.

- Health did not complete the required terminations checklist for four of 23 (17%) employees.

- For four of 19 (21%) employees where the terminations checklist was present, Health did not document completion dates for each required task; therefore, there is no evidence that each task was performed in a timely manner.

CAPP Manual Topic 50320 states that "final payments to terminating employees should be issued on the payday following the last period worked." Additionally, Section PS-4 of the Security Standard states that organizations should "disable information system access within 24-hours of employment termination" and retrieve all property related to information systems. The removal of systems access and the surrender of all state property are included as required tasks on Health's terminations checklist.

As a result of an untimely processing of employee terminations, the former employees experienced delays in receiving their final payouts. Further, as no evidence of a timely processing of off-boarding tasks exists for several of the separating employees, this increases the risk that these employees could retain access to sensitive information systems and not surrender computers, purchase cards, or other state property in their possession.

The untimely processing of leave payouts was the result of the outlying departments not providing all required information to the Payroll Department in a timely manner. This was due to resource constraints and a prioritization of other tasks. Although Health's internal policy requires the

completion of a terminations checklist, Health does not have a review process in place to ensure the Office of Human Resources (Human Resources) and/or the Shared Business Services (SBS) Division and the outlying business units correctly complete each of their required off-boarding tasks.

Health should implement a final review of employee off-boarding documents to ensure all termination checklists are properly completed in a timely manner. This review process should also cover each step of the employee off-boarding process to ensure payroll analysts enter all terminations completely and accurately into the statewide payroll system.

Properly Record Financial Transactions
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Medical Assistance Services' Fiscal Division (Fiscal) did not properly allocate pharmacy rebate revenues in the Commonwealth's accounting and financial reporting system or their internal financial system. On a quarterly basis, Fiscal staff analyze pharmacy rebate information and prepare adjustments to allocate the revenue to the proper funds and accounts based on different components of the Medicaid program. Fiscal did not allocate approximately $98 million in pharmacy rebate revenue collected for the quarter ending December 2019, and they erroneously made a year-end entry totaling approximately $16 million because they were not aware that the quarterly entry to reallocate rebate revenue had not been made.

Medical Assistance Services' financial activity is material to the Commonwealth's financial statements, so it is essential for Medical Assistance Services to have strong financial reporting practices. Policies and procedures over financial reporting information, as a best practice, should be detailed and thorough with a sufficient review process to prevent and detect potential errors and omissions. Chapter 1283 Item 307(U) of the 2020 Appropriation Act also requires Medical Assistance Services to determine and properly reflect in the accounting system whether pharmacy rebates received in the quarter are related to fee-for-service or managed care expenditures and whether or not the rebates are prior year recoveries or expenditure refunds for the current year.

As a result of this error, revenue and expense balances in several funds in the Commonwealth's accounting and financial reporting system, as well as Medical Assistance Services' internal financial system, were materially misstated at year end. Medical Assistance Services notified Accounts of this error and adjustments related to these errors were recorded.

This issue was due to an oversight by Fiscal management. Fiscal management prepared the quarterly pharmacy rebate allocation adjustment but did not ensure Fiscal staff processed the adjustment in either the internal financial system or the Commonwealth's accounting and financial reporting system. This omission was not detected by Fiscal through any other review or reconciliation processes. Fiscal should strengthen procedures to ensure required transactions get recorded both timely and accurately in the Commonwealth's accounting and financial reporting system as well as their internal financial system.

Improve Information Security Program and Controls
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Medical Assistance Services needs to continue addressing weaknesses found during a recent audit of IT general controls. The Internal Audit division hired an external consultant to perform this audit

for the period April 1, 2019, through March 31, 2020, while Internal Audit supervised the effort. This audit focused on compliance with certain control areas within the Security Standard. The results of the audit identified 71 individual control weaknesses out of 100 controls tested.

Noncompliance with the required security controls increases the risk for unauthorized access to mission-critical systems and data in addition to weakening the agency's ability to respond to malicious attacks to its IT environment. We believe these weaknesses are due to turnover in various IT positions as well as IT resources being allocated to work on a new system implementation and other priorities.

Medical Assistance Services should continue to dedicate the necessary resources to ensure timely completion of its corrective action plans and to become compliant with the Security Standard. These actions will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data. Medical Assistance Services' management has been working to address the issues from the Internal Audit report, and they estimate completing all corrective actions by June 30, 2021.

Strengthen Review of System and Organization Control Reports for Third-Party Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Medical Assistance Services did not adequately document their review and evaluation of the System and Organization Control (SOC) report for one of their most critical third-party providers. Specifically, they did not adequately document their evaluation of the complementary user entity controls cited in the report or significant weaknesses identified in the report.

Section 1.1 of the Security Standard states that agency heads remain accountable for maintaining compliance with the Security Standard for IT equipment, systems, and services procured from providers, and agencies must enforce the compliance requirements through documented agreements and oversight of the services provided. Additionally, the Commonwealth's Hosted Environment Information Security Standard, SEC 525, Section SA-9-COV-3, requires Medical Assistance Services to perform a security audit or review an audit report of the third-party service provider's environment on an annual basis. Furthermore, CAPP Manual Topic 10305 requires agencies maintain oversight over the provider to gain assurance over outsourced operations and SOC reports provide an independent description and evaluation of a provider's internal controls.

Without performing an adequate review and evaluation of SOC reports, Medical Assistance Services cannot gain assurance that a third-party service providers' controls are designed, implemented, and operating effectively. In addition, Medical Assistance Services is not able to identify and implement complementary user entity controls that the provider relies on to maintain an effective control environment. Although Medical Assistance Services maintains a high degree of interactions with its providers, management is increasing the risk that it will not detect a weakness in a provider's environment by not properly documenting their review of SOC reports.

Medical Assistance Services experienced personnel turnover in the position responsible for reviewing the SOC reports and documenting significant findings. While Medical Assistance Services was able to assign new personnel to obtain the SOC reports, there was no clear procedure for which individuals will review and document significant findings and evaluate complementary controls, and this part of the review was not performed.

Medical Assistance Services should strengthen policies and procedures to review, assess, and document the effectiveness of third-party service providers' controls reported through SOC reports. In addition, Medical Assistance Services should use SOC reports as a component of its oversight activities over its providers to confirm they comply with the applicable requirements. If weaknesses are identified in the SOC reports, Medical Assistance Services should document their evaluation of the weaknesses as well as their approach to mitigating the risk until the provider corrects the deficiency.

Review Eligibility Information as Required

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No
(This finding has also been issued to the Department of Social Services)

We were unable to confirm eligibility for one of 30 (3%) individuals in a sample of Medicaid managed care organization payments. This individual's eligibility should have been redetermined in September 2019 when updated household information was obtained; however, the local eligibility worker did not review eligibility at that time in accordance with Medical Assistance Services' policy. This instance results in federal questioned costs of approximately $3,349 for fiscal year 2020.

42 C.F.R. § 438.3(c)(2) states "Capitation payments may only be made by the State and retained by the Managed Care Organization for Medicaid-eligible enrollees." Section 12VAC30-40-10 of the Virginia Administrative Code lays out the general conditions of eligibility that an individual is required to satisfy in order to be enrolled in the Medicaid program. In addition, section M1520.001 of the Virginia Medical Assistance Eligibility manual requires that the eligibility worker should complete a partial review of eligibility if they become aware of any changes in an individual's circumstances that could affect continued eligibility in the Medicaid program.

In September 2019, as part of the eligibility review for another federal program, the eligibility worker obtained new information and determined that the individual had left the household. This type of change should trigger a partial review of eligibility, but the local eligibility worker did not properly perform the review as required. Medical Assistance Services attempted to determine why this review did not get performed; however, the COVID-19 pandemic has resulted in restricted access to paper case files, and they were unable to obtain necessary documentation to determine why the review did not get performed. As a result of the situation, Medical Assistance Services continued to make Medicaid capitation payments on behalf of an individual who may or may not be eligible to receive them.

Medical Assistance Services, along with the Department of Social Services (Social Services), is continuing to investigate this case to determine the proper outcome, and we recommend they continue with these efforts and take appropriate action. Medical Assistance Services should also work with Social Services to ensure local eligibility workers are familiar with and follow eligibility guidance including policies and procedures over performing partial eligibility reviews when required.

Improve Financial Management System Access Controls
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Medical Assistance Services' Fiscal Division needs to strengthen access controls over their financial management system. Certain access roles and responsibilities within the system are not designed to provide adequate internal controls and segregation of duties as follows:

- Multiple individuals have super user/manager roles that allow full access to the general ledger, payables ledger, receivables ledger, and system administration. Employees with this access can create users, initiate and approve transactions, update and create vendors, and process payments among other permissions.

- One journal entry totaling approximately $76 million was entered and approved by the same user. Although this transaction was appropriate, this individual was able to create and approve a transaction because they had been assigned the super user role discussed above.

- One manager with elevated permissions reviewed and approved their own access as part of the annual security reviews.

Section AC-6 of the Security Standard requires the agency to employ the principle of least privilege and allow users to only have access necessary to accomplish assigned tasks in accordance with job duties and responsibilities. Fiscal should consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Fiscal should also apply least privilege to the development, implementation, and operation of organizational information systems.

When access is not based on the principle of least privilege, it increases the risk of unauthorized and fraudulent transactions. In addition, there is an increased risk that users can circumvent other compensating controls and perform unauthorized actions within the information system. In the case of individuals with the super user/manager access, this level of access creates a lack of segregation of duties.

Fiscal has not customized the super user/manager roles or set up workflow controls within the financial management system due to current staffing levels. Fiscal relies on internal policies and procedures that state users should not enter and approve their own transactions but has not developed

additional compensating or detective controls to ensure that users are not performing unauthorized actions. Medical Assistance Services' Office of Compliance and Security (OCS) is not reviewing system administrator audit logs or activity due to turnover in OCS since the prior year. Insufficient management oversight and workload pressure were attributed to the $76 million journal entry that was entered and approved by the same user.

Fiscal should reevaluate financial system access responsibilities and reassign or customize system roles based on the principle of least privilege. Responsibilities within the system should be created in a way that allows Fiscal to maintain adequate segregation of duties. Further, Fiscal and OCS should develop more effective compensating controls if user roles and responsibilities are not assigned based on the principal of least privilege. In these instances, management should document their risk evaluation and risk acceptance.

Ensure Compliance with National Correct Coding Initiative Requirements
Type: Compliance
Severity: Not applicable
Repeat: No

Medical Assistance Services has contracted with a third-party service provider to implement the National Correct Coding Initiative (NCCI) system edits in the Medicaid claims processing system. Although the contract with the third party does include some language related to confidentiality, the contract language does not meet the specific requirements set out in the NCCI Technical Guidance Manual (Manual).

The Centers for Medicare and Medicaid Services (CMS) developed the NCCI to control improper coding leading to inappropriate payment of claims. Section 7.1.1 of the Manual states that access to the quarterly Medicaid NCCI edit files is limited to a state's Medicaid agency. A state Medicaid agency may share these quarterly files with the contracted fiscal agent if appropriate confidentiality agreements are in place. Section 7.1.2 of the Manual requires seven specific elements that must be included, at a minimum, in the confidentiality agreements for any contracted party using this information. Without the appropriate confidentiality agreement in place, Medical Assistance Services is not in compliance with federal requirements and guidelines. Additionally, Medical Assistance Services could be held accountable if the third party improperly shared the confidential NCCI edit information.

Although Medical Assistance Services' contract with the third party includes a confidentiality clause, it is broad in nature and does not include the seven specific elements required by the Manual. We recommend Medical Assistance Services work with CMS to determine whether the current contract language is appropriate and whether additional language is necessary to meet the federal requirements.

Continue to Improve Controls over SNAP Payments
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Improve Controls over SNAP Payments

In fiscal year 2020, Social Services continued to not have sufficient controls over payments made for the Supplemental Nutrition Assistance Program (SNAP). Social Services' case management system is used to determine who is eligible for SNAP and the benefit amounts. Social Services sends that information to a third-party vendor who gives the benefits to recipients via an Electronic Benefits Transfer card and the vendor then draws down the funds from the federal government. The Finance Division (Finance) completes a daily three-way reconciliation between Social Services' case management system, the vendor's system, and the federal payment system that is used to draw down federal funds. In fiscal year 2019, we noted significant variances between the systems that could not be supported. During the first half of fiscal 2020, there were also variances between the systems, which resulted in the federal payment system having approximately $266 million more benefits given during July through December of 2019, than the case management system reflected. In addition, the daily reconciliation was not reviewed or approved by a supervisor during fiscal year 2020; however, Finance implemented a process to review and approve the daily reconciliation beginning September 2020.

During fiscal year 2020, Social Services' Enterprise Business Solutions Division (Enterprise Business Solutions) and Finance worked together to resolve the discrepancy between the systems beginning January 1, 2020. For the second half of the fiscal year, we noted no significant variances between the systems; however, Enterprise Business Solutions and Finance could not provide support for $266 million out of $1,253 million (13%) that was paid out by the vendor and drawn down from the federal government during the first half of the fiscal year. Finance also used the amount paid out by the vendor when reporting revenue and expenditure amounts for the SNAP program to Accounts for use in the Comprehensive Annual Financial Report (CAFR). By not addressing discrepancies noted during the reconciliation process, Finance increases the risk of inaccurate data being reported in the CAFR. We consider this a material weakness in internal control.

2 C.F.R. § 200.303(a) states that an entity must establish and maintain effective internal control over federal awards that provides reasonable assurance that the entity is managing the award in compliance with the federal statutes, regulations, and terms and conditions of the federal award. As an internal control, a supervisor should review each reconciliation and its support to ensure it is properly supported and accurate. In addition, 7 C.F.R. § 247.4 states that state agencies shall reconcile total funds entering into, exiting from, and remaining in the EBT system each day. Finance and Enterprise Business Solutions should continue to work together to investigate and resolve any reconciling amounts and maintain appropriate documentation for all payments and amounts drawn down from the federal government. Finance should continue to review the SNAP daily reconciliation to ensure data is accurate, discrepancies are resolved timely, supervisor's review and approval is documented, and supporting documentation is maintained.

Define and Communicate Subrecipient Monitoring Responsibilities
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Social Services' Compliance Division (Compliance) has not updated the Agency Monitoring Plan for Social Services that defines the responsibilities of Compliance, including the role of Subrecipient Monitoring Lead Coordinator. During fiscal year 2019, the oversight of Social Services' subrecipient monitoring process transitioned from the Division of Community and Volunteer Services (Community and Volunteer Services) to Compliance, and the Agency Monitoring Plan was not updated to reflect this change. Social Services' divisions were not aware of Compliance's role as a Subrecipient Monitoring Lead Coordinator, resulting in subrecipient monitoring activities not being performed in accordance with federal requirements.

2 C.F.R. § 200.332(d) requires pass through entities to monitor the activities of subrecipients as necessary to ensure that the sub-award is meeting grant requirements. Without clearly defined responsibilities related to the subrecipient monitoring activities, Compliance cannot provide assurance that it adequately monitors all of the agency's subrecipients, ensuring they are achieving program objectives, or complying with the federal requirements that restrict program funds.

Compliance has not updated the Agency Monitoring Plan due to the division being created during fiscal year 2019 and was not assigned a Division Director and Subrecipient Monitoring Lead Coordinator until fiscal year 2020. Compliance should update the Agency Monitoring Plan to define the Compliance Division and Subrecipient Monitoring Lead Coordinator's responsibilities and communicate these subrecipient monitoring responsibilities to divisions to ensure compliance with federal regulations.

Continue Improving IT Risk Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Social Services continues to not have IT Risk Management documentation for all of its sensitive systems in accordance with the Security Standard. Since the prior year audit, Social Services completed two IT System Risk Assessments and one System Security Plan. However, Social Services identified additional sensitive systems in its IT environment, causing the agency to have more IT Risk Management documentation to complete. IT Risk Management documentation identifies the types of data stored and processed within its environment, the sensitivity classification of that data, potential risks and threats to the systems, and risk mitigating controls that should be implemented. Social Services does not comply with the following areas:

- Social Services does not have IT System and Data Sensitivity Classifications for seven (11.3%) out of a total of 62 sensitive systems. The Security Standard requires Social Services classify the IT system as sensitive if any type of data handled by the system is

sensitive based on confidentiality, integrity, or availability (*Security Standard: section 4 IT System and Data Sensitivity Classification*).

- Social Services does not have Risk Assessments for 15 systems (24.2%). The Security Standard requires the agency to conduct and document a Risk Assessment for each IT system classified as sensitive at least once every three years (*Security Standard: section 6.2 Risk Assessment*).

- Social Services does not have System Security Plans for 18 systems (29%). The Security Standard requires Social Services document a System Security Plan for the IT system (*Security Standard: section PL-2 System Security Plan*).

- Social Services does not perform annual reviews for all Risk Assessment and System Security Plans to determine the continued validity of the documents. In 2020, Social Services reviewed 29 of 47 (62%) completed Risk Assessments and ten of 45 (22%) completed System Security Plans. The Security Standard requires Social Services to conduct an annual self-assessment of the Risk Assessment and to review the System Security Plan on an annual basis or more frequently to address environmental changes (*Security Standard: section 6.2 Risk Assessment; section PL-2 System Security Plan*).

- Social Services does not evaluate and implement corrective actions to mitigate risks in its sensitive systems' Risk Assessments. The Security Standard requires Social Services to prepare a report of each Risk Assessment that includes major findings and risk mitigation efforts (*Security Standard: section 6.2.3 Risk Assessment*). Without documenting this information, Social Services cannot determine whether the risks they identify in the Risk Assessment and vulnerability scanning processes have the proper mitigating security controls and procedures.

Without documenting risk management information for all its sensitive systems and reviewing the documentation at least annually, Social Services cannot prioritize information security controls to implement or determine if proper information security controls are in place. This could lead to a breach of data or unauthorized access to sensitive and confidential data.

Social Services experienced turnover in its Chief Information Officer (CIO) position, resulting in additional reorganization for its IT Services and Information Security and Risk Management departments. Furthermore, Social Services dedicated its resources to higher priorities to support its mission-essential functions due to the COVID-19 pandemic. These events collectively delayed Social Services from developing IT Risk Management documentation for its sensitive systems.

Social Services should develop a plan and dedicate the necessary resources to complete Risk Management documentation for its sensitive systems and review those documents annually to validate that the information reflects the current environment. Additionally, Social Services should dedicate the necessary resources to implement security controls to mitigate the risks and vulnerabilities identified in its Risk Assessments. Doing this will help to ensure the confidentiality, integrity, and availability of the agency's sensitive systems and mission essential functions.

Review Eligibility Information as Required
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No
(This finding has also been issued to Medical Assistance Services)

We were unable to confirm eligibility for one of 30 (3%) individuals in a sample of Medicaid managed care organization payments. This individual's eligibility should have been redetermined in September 2019 when updated household information was obtained; however, the local eligibility worker did not review eligibility at that time in accordance with Medical Assistance Services' policy. This instance results in federal questioned costs of approximately $3,349 for fiscal year 2020.

42 C.F.R. § 438.3(c)(2) states "Capitation payments may only be made by the State and retained by the Managed Care Organization for Medicaid-eligible enrollees." Section 12VAC30-40-10 of the Virginia Administrative Code lays out the general conditions of eligibility that an individual is required to satisfy in order to be enrolled in the Medicaid program. In addition, section M1520.001 of the Virginia Medical Assistance Eligibility manual requires that the eligibility worker should complete a partial review of eligibility if they become aware of any changes in an individual's circumstances, which could affect continued eligibility in the Medicaid program.

In September 2019, as part of the eligibility review for another federal program, the eligibility worker obtained new information and determined that the individual had left the household. This type of change should trigger a partial review of eligibility, but the local eligibility worker did not properly perform the review as required. Medical Assistance Services attempted to determine why this review did not get performed; however, the COVID-19 pandemic has resulted in restricted access to paper case files and they were unable to obtain necessary documentation to determine why the review did not get performed. As a result of the situation, Medical Assistance Services continued to make Medicaid capitation payments on behalf of an individual who may or may not be eligible to receive them.

Medical Assistance Services, along with Social Services, is continuing to investigate this case to determine the proper outcome and we recommend they continue with these efforts and take appropriate action. Medical Assistance Services should also work with Social Services to ensure local eligibility workers are familiar with and follow eligibility guidance including policies and procedures over performing partial eligibility reviews when required.

Continue to Improve Reconciliation Process of the Commonwealth's Retirement Benefits System
Type: Internal Control
Severity: Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Social Services' Human Resources continues to not sufficiently reconcile retirement contributions before confirming to VRS that retirement data is correct. Human Resources did not perform the required monthly reconciliations between the Commonwealth's retirement benefits system and the Commonwealth's human resource system during fiscal year 2020, as they did not include the following:

- reconciliation of creditable compensation;
- reconciliation of the approved purchase of prior service agreements;
- review of the Commonwealth's human resource system reports; and
- review of the automated reconciliation and correction of the exceptions noted.

CAPP Manual Topic 50410 requires agencies to perform a reconciliation of creditable compensation between the human resource and retirement benefits systems monthly before confirming the contribution. In addition, agencies must identify exception items on the Automated Reconciliation Reports and communicate them to the proper system of authority for correction, as soon as possible but no later than 31 days from the date of the report.

Improper pre- and post-certification processes can affect the integrity of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire Commonwealth and can result in a misstatement in the Commonwealth's financial statements. Inadequate reconciliations can cause errors in members' retirement related data and can cause under or overpaying retirement contributions to the Benefit System, which can create complications when members retire. Due to high turnover and lack of policies and procedures in the Human Resources division, staff did not perform the reconciliation between the Commonwealth's retirement benefits system and the Commonwealth's human resource system adequately and prior to confirming the snapshot.

Human Resources should ensure that retirement data is reconciled adequately and in accordance with the CAPP Manual prior to confirming the snapshot monthly. This should include assigning appropriate resources to this process and developing written guidance for employees to gain an understanding of the requirements and deadlines established by VRS to ensure the reconciliation is performed correctly.

Review Exceptions Between Commonwealth's Human Resource System and Payroll System
Type: Internal Control
Severity: Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Improve Internal Controls over Commonwealth's Human Resource System

Human Resources continues to not have sufficient controls in place to ensure data in the Commonwealth's human resource system is accurate. Human Resources did not review exceptions between the Commonwealth's human resource system and the Commonwealth's payroll system during fiscal year 2020.

CAPP Manual Topic 50800 states that the certifier should perform a post-certification audit of the payroll following processing, including a review of the exceptions between the Commonwealth's human resource system and the Commonwealth's payroll system.

Human Resources does not have policies and procedures in place to perform a review of exceptions between the Commonwealth's payroll system and the Commonwealth's human resource system and without proper review, there is increased risk of unauthorized or incorrect payroll disbursements. Human Resources should develop procedures to address reviewing and resolving exceptions between the Commonwealth's payroll system and the Commonwealth's human resource system and retain documentation of the review.

STATUS OF PRIOR YEAR
FINDINGS AND RECOMMENDATIONS

Continue Dedicating Resources to Support Information Security Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Dedicate Resources to Support Information Security Program

DBHDS is making progress to allocate the necessary resources to manage its information security program and IT projects. As of November 2020, DBHDS has 321 sensitive systems between the Central Office and its facilities. This number of sensitive systems requires extensive IT resources to ensure compliance with the agency's enterprise security program and the Security Standard.

Since the prior year, DBHDS hired a new Chief Information Security Officer (CISO) and CIO, who revised the agency's corrective action plans to improve the information security program, which includes reducing the number of sensitive systems across the Central Office and facilities. The CISO and CIO are also in the process of filling vacancies between their departments that will assist in corrective actions and managing the information security program. Additionally, DBHDS created the IT Investment Board (ITIB) to maintain oversight of IT investment decisions and allocating the funds and resources for those projects. However, DBHDS dedicated much of its resources to supporting its mission-critical functions due to the COVID-19 pandemic, and the ITIB did not begin meeting until June 2020, delaying the allocation of resources to IT projects. These events caused DBHDS to continue having some audit findings repeat for the fifth year, specifically the absence of baseline configurations and IT contingency management documentation.

The Security Standard, Section 2.4.2, states agency heads are responsible for ensuring that a sufficient information security program is maintained, documented, and effectively communicated to protect the agency's IT systems. Not having sufficient IT resources to manage the sensitive systems at the Central Office and facilities increases the risk that certain controls may not exist, resulting in a data breach or unauthorized access to confidential and mission-critical data. If a breach occurs and Health Insurance Portability and Accountability Act (HIPAA) data is stolen, the agency can incur large penalties, as much as $1.5 million.

DBHDS should continue to reduce its sensitive system inventory and evaluate the need for resources necessary to support the sensitive systems at the Central Office and the facilities. DBHDS should also allocate resources to remediate the weaknesses in the information security program and maintain the program in accordance with the Security Standard. Allocating the necessary resources to improve and maintain the information security program will increase the confidentiality, integrity, and availability of DBHDS' sensitive and mission critical data.

Improve IT Contingency Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2017)

DBHDS continues to not have complete and current Continuity of Operations Plans (COOP) and IT Disaster Recovery Plans (DRP) for the facilities and Central Office. DBHDS has hospitals, mental health institutes, and training centers that manage their own mission-critical IT applications that help provide patient services. Three of the facilities do not have a COOP, one facility and Central Office do not have a DRP, and the remaining facilities' COOPs and DRPs are out-of-date, with some as old as 2009. In addition, the facilities and Central Office are not performing annual tests on the COOPs or DRPs.

Since the prior year audit, DBHDS hired a new CISO and CIO that resulted in process changes for planning and implementing IT projects and tasks. Additionally, DBHDS dedicated its resources to responding to higher priorities to support the agency's mission essential functions due to the COVID-19 pandemic. These events collectively delayed DBHDS from developing COOPs and DRPs for the facilities and Central Office. DBHDS plans to complete the COOPs and DRPs by the end of the 2021 calendar year.

The Security Standard, Section CP-1, requires DBHDS to develop and disseminate procedures to facilitate the implementation of a contingency planning policy and associated contingency planning controls. The Security Standard also requires the agency to maintain current COOPs and DRPs and conduct annual tests against the documents to assess their adequacy and effectiveness.

By not having current COOPs and DRPs, DBHDS increases the risk of mission-critical systems being unavailable to support patient services. In addition, by not performing annual tests against the COOPs and DRPs, DBHDS is unable to identify weaknesses in the plans and may unnecessarily delay the availability of sensitive systems in the event of a disaster or outage.

DBHDS should update the contingency management program for the facilities and Central Office to meet the minimum requirements in the Security Standard. DBHDS should update the COOPs and DRPs ensuring they are consistent with the agency's IT risk management documentation and consistent across the facilities and Central Office. Once the contingency documents are complete, DBHDS should conduct tests on at least an annual basis to ensure the facilities and Central Office can restore mission-critical and sensitive systems in a timely manner in the event of an outage or disaster.

Develop Baseline Configurations for Information Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2015)

DBHDS continues to not have documented baseline configurations for its sensitive systems' hardware and software requirements. Baseline security configurations are essential controls in IT

environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems.

Since the prior year audit, DBHDS hired a new CISO and CIO to manage the agency's IT operations and information security program. As part of this responsibility, the CISO and CIO continued the agency's efforts of reducing the number of sensitive systems across the Central Office and 12 facilities. During these efforts, DBHDS identified additional sensitive systems and applications, totaling 321 with some containing HIPAA data, social security numbers, and personal health information data. DBHDS was unable to make any progress to develop baseline configurations because of its ongoing efforts to identify and reduce the number of sensitive systems as well as dedicating its resources to support its mission-critical functions due to the COVID-19 pandemic.

The Security Standard, Sections CM-2 and CM-2-COV, requires DBHDS to perform the following:

- Develop, document, and maintain a current baseline configuration for information systems.

- Review and update the baseline configurations on an annual basis, when required due to environmental changes and during information system component installations and upgrades.

- Maintain a baseline configuration for information systems development and test environments that is managed separately from the operational baseline configuration.

- Apply more restrictive security configurations for sensitive systems, specifically systems containing HIPAA data.

- Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

The absence of baseline configurations increases the risk that these systems will not meet the minimum security requirements to protect data from malicious access attempts. If a data breach occurs to a system containing HIPAA data, the agency can incur large penalties, up to $1.5 million.

DBHDS should assign the necessary resources to continue its efforts to reduce the number of sensitive information systems across its Central Office and facilities. DBHDS should also establish and maintain security baseline configurations for its sensitive systems to meet the requirements of the Security Standard and protect the confidentiality, integrity, and availability of the agency's sensitive data.

Continue Improving Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2018, with significant progress in all but one area)
Prior Title: Improve Web Application Security

DBHDS continues to improve its security controls for one of its sensitive web applications in accordance with the Security Standard. The web application is the originating system for wage employee hours and interfaces with the Commonwealth's payroll system. While DBHDS resolved one of the two prior year weaknesses, DBHDS continues not to have an updated Risk Assessment to reflect the upgrade changes implemented to the system.

The Security Standard, Section 6.2, requires DBHDS to conduct and document an IT system Risk Assessment once every three years and perform an annual self-assessment to validate the information. Without completing new Risk Assessments when a system undergoes a significant modification or performing an annual review, DBHDS may not identify risks to the system and implement the necessary mitigating controls.

Since the prior year audit, DBHDS hired a new CISO and CIO, who developed a new Risk Assessment template to apply to its sensitive systems. However, DBHDS has not yet had a chance to use this template to update Risk Assessments for its sensitive systems. Additionally, DBHDS dedicated its resources to support its mission critical business processes due to the COVID-19 pandemic. These events collectively delayed DBHDS from resolving the remaining weakness to the web application, but DBHDS expects to complete the Risk Assessment for the web application by the end of fiscal year 2021.

DBHDS should use the new template to update the web application's Risk Assessment to identify risks and mitigating controls. DBHDS should also maintain its Risk Assessments by performing annual self-assessments and updating the information as needed to protect the confidentiality, integrity, and availability of its sensitive and mission-critical data.

Continue to Develop and Implement Compliant Application Access Management Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Develop and Implement Compliant Application Access Management Procedures

DBHDS continues to focus on the development of access management procedures at the facility level, which meet the baseline standard defined by the Security Standard. In the prior year, the Information Security Office issued baseline procedures and implemented an application to approve access requests for all DBHDS facilities. However, the facilities still have not developed procedures they can adapt for their specific environment that will ensure compliance with the Security Standard.

Security Standard, Section AC-1, requires an organization to develop, document, and disseminate an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and compliance. The access control policy should include procedures to facilitate the implementation of the policy and associated access controls. Security Standard, Section AC-2, addresses requirements over account management practices for requesting, granting, administering, and terminating accounts. Not having adequate access control policies and procedures increases the risk that individuals will have inappropriate access and can potentially process unauthorized transactions.

The DBHDS Information Security Office sent the baseline security procedures to all DBHDS facilities with the expectation that they would bring their internal procedures in line with the baseline procedures by March 2018. However, the Information Security Office did not monitor the facilities' implementation of these procedures because each facility has unique processes related to access. The Information Security Office should continue to work with the individual facilities to set reasonable deadlines and monitor their actions to ensure that they bring their application access management procedures in line with the office's baseline procedures and the Security Standard.

Comply with Employment Eligibility Requirements
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Individual facilities within DBHDS continue to improve processes and controls over the employment eligibility process. In fiscal years 2018 and 2019, Employment Eligibility Verification forms (Form I-9) were not completed by Human Resources at the facilities in accordance with guidelines issued by the United States Citizenship and Immigration Services of the Department of Homeland Security. During fiscal year 2020, DBHDS Central Office provided all facilities with a checklist for completing Form I-9s. In addition, a formal Human Resources forum was planned to be held in April 2020. However, the originally scheduled training was cancelled due to the COVID-19 pandemic.

The Immigration Reform and Control Act of 1986, requires that all employees hired after November 6, 1986, have a Form I-9 completed to verify both employment eligibility and identity. The U.S. Citizenship and Immigration Services sets forth federal requirements for completing the Form I-9 in the Handbook for Employers known as the M-274. Per M-274, the employer is responsible for ensuring all parts of Form I-9 are completed and retained for a period of at least three years from the date of hire or for one year after the employee has separated, whichever is longer. Not complying with federal requirements could result in civil and/or criminal penalties and debarment from government contracts.

Management should continue updating processes in place over the completion of Form I-9s and provide adequate training to Human Resources staff to reinforce the expectation of compliance with the applicable federal requirements.

Continue to Improve Opioid Grant Subrecipient Monitoring
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Implement Opioid Grant Subrecipient Monitoring

As identified during fiscal year 2019, DBHDS' Office of Recovery Services (Recovery Services) is not properly monitoring subrecipients who receive federal funds from the State Targeted Response to the Opioid Crisis (Opioid STR) grants, which encompasses the State Targeted Response and the State Opioid Response (SOR) grants.

During fiscal year 2020, Recovery Services completed on-site visits to monitor programmatic progress for eight of 40 subrecipients (20%) of the Opioid STR grant funds. Monitoring activities performed during fiscal years 2019 and 2020 provided no authoritative proof that subrecipients are providing services as outlined in the performance contract between DBHDS and the subrecipients. Nor did documentation of on-site reviews provide sufficient assurance that monitoring was performed in accordance with federal requirements.

45 C.F.R. § 75.352(6)(b) requires the pass-through entity to evaluate each subrecipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring described in paragraphs (d) and (e) of this section.

45 C.F.R. § 75.352(6)(d) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.

Additionally, 45 C.F.R. § 75.352(6)(e)(1)(2) states that depending upon the pass-through entity's assessment of risk posed by the subrecipient (as described in paragraph (b) of this section), the following monitoring tools may be useful for the pass-through entity to ensure proper accountability and compliance with program requirements and achievement of performance goals: providing subrecipients with training and technical assistance on program-related matters and performing on-site reviews of the subrecipient's program operations.

The Opioid STR grants were new for fiscal year 2019, and Recovery Services did not have a structured and coordinated internal process for the monitoring of the grants. Insufficient and unreasonable evidence of subrecipient monitoring activities could result in noncompliance with grant requirements and jeopardizes current and future funding. Recovery Services developed a structured process for monitoring the Opioid STR grants at the beginning of fiscal year 2021. Recovery Services should continue to improve subrecipient monitoring for the Opioid STR grants to ensure proper accountability and compliance with program requirements and achievement of performance goals.

Provide Federal Award Requirements to Subrecipients
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

DBHDS' Office of Management Services (Management Services) continues to improve processes over communicating federal award requirements to the Community Service Boards (CSBs) for the SOR grant. In the prior year, DBHDS did not have a performance contract in place with the CSBs for the funding of the SOR grant. Additionally, in fiscal year 2019, DBHDS did not communicate federal award information for the SOR grant in the CSB performance contract. As part of Amendment No. 1, Management Services revised the fiscal year 2019–2020 performance contract to include the required information for the SOR grant; however, changes to the contract were not implemented until after the fiscal year under audit.

45 C.F.R. § 75.352(a) states that every subaward must be clearly identified to the subrecipient as a subaward and include certain information at the time of the subaward and if any of these data elements change, include the changes in subsequent subaward modification. When this information is not available, the pass-through entity must provide the best information available to describe the Federal award and subaward. The lack of a performance contract or memorandum of understanding outlining the requirements of the SOR grant increases the risk of the CSBs using the awards for activities not related to the SOR grant or for unallowable costs associated with the SOR grant. This creates a potential financial liability for DBHDS, and they have limited recourse with the CSBs due to the lack of a legally binding document.

We notified Management Services of the exclusion of the SOR grant in January 2020, and they did not update performance contracts for fiscal year 2020 to include the grant due to the lack of time to implement these changes. Management Services should follow through with their existing plan and ensure that a signed performance contract with the CSBs exists and contains the federal requirements for the SOR grant.

Continue Improving Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Web Application Security

Health continues to not secure one of their sensitive systems with some of the minimum-security controls required by the Security Standard and industry best practices. We communicated the weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to the descriptions of security mechanisms contained within the documents.

The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the Security Standard, Health cannot ensure the confidentiality, integrity, and availability of data within their systems.

Health should implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner. It is our understanding the corrective action to address this issue will be completed by December 2020.

Continue Improving the Disaster Recovery Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Improve the Disaster Recovery Plan

Health continues to not perform certain processes in their DRP required by the Security Standard. We identified a weakness in this area and communicated this to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to descriptions of security mechanisms contained within the document.

The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the Security Standard, Health cannot ensure the confidentiality, integrity, and availability of data within their systems.

Health should continue their efforts and implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner to ensure availability of Health's systems.

Continue Improving the Contingency Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Contingency Management Program

Health continues to not properly manage certain aspects of their Contingency Management Program to meet the requirements in the Security Standard. The Contingency Management Program is the baseline for Health to continue mission-essential functions in the event of an outage or disaster. We identified one weakness and communicated it to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to the descriptions of security mechanisms contained within the document.

The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the Security Standard, Health cannot ensure the confidentiality, integrity, and availability of data within their systems.

Health should coordinate efforts among departments to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner. Health anticipates corrective action to address this issue will be completed by January 2021.

Continue Strengthening the System Access Removal Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)
Prior Title: Improve Timely Removal of Critical System Access

Health's management acknowledges the agency is still making improvements to their controls for removing terminated users' access to certain information systems in a timely manner following the users' separations from the agency. This year, we again identified several instances across five systems in which a terminated employee still had access to the system after leaving the agency.

Section PS-4 of the Security Standard requires agencies to "disable information system access within 24 hours of employment termination." Terminated employees who still have access to critical systems may be able to access these systems after leaving the agency. By not deleting users' accounts to sensitive information systems, this also increases the risk of an internal or external party compromising these unneeded accounts and using them to access these systems. Each of these scenarios increases the risk of inappropriate transactions and the exposure of sensitive data.

Health should strengthen their access removal policy to remove each user's access from individual information systems within 24 hours of the user's separation from the agency. If Health intends to rely on another agency for the removal of access to sensitive information systems, Health

should document an agreement with the other organization to ensure mutually agreed-upon responsibilities and expectations are clear. Human Resources and/or the SBS division should clarify their access removal notification policy and provide guidance to all users throughout the state. This will reduce the rates of noncompliance with the Security Standard and reduce the risk of unauthorized transactions and exposure of sensitive data.

Continue Enhancing Reviews of System Access
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Perform System Access Reviews

Health's management acknowledges the agency is still making improvements to their controls for performing comprehensive system access reviews within timeframes established by internal and statewide procedures. These systems support various business functions, including accounting, patient management, and benefits administration, so there are various internal policies that address periodic system access reviews. This year, there continued to be several instances across three systems in which Health did not comply with their internal policies over periodic reviews of system access.

Health's internal policy requires supervisors of Health's different business areas to review and certify access to Health's financial and patient management systems monthly. Additionally, for sensitive information systems, Section AC-6-7a of the Security Standard requires agencies to "review on an annual basis the privileges assigned to all users to validate the need for such privileges." Regular access reviews ensure that system administrators processed all requests to add, modify, or delete users properly and in accordance with requests from the system owners. Not performing regular access reviews within their established timeframes increases the risk of individuals having inappropriate access to information systems. This increases the risk of unauthorized activity within these systems.

Health may want to review their internal policy over system access reviews since it is more stringent than statewide requirements. Consideration should be given to the significance of each system and the potential risk weighed against the administrative burden for Health staff. Based on this evaluation, Health may want to modify their internal policy for some information system access reviews. Regardless of any changes they make to their internal policy, Health should ensure backup personnel are available to perform the reviews if the primary reviewer is unable to complete them. Additionally, Health should perform follow-up procedures when reviewers do not provide certifications within their established timeframes and ideally should require a positive confirmation when a review is done. This will reduce the rates of untimely reviews and decrease the risk of inappropriate access to sensitive information systems.

Continue Following Administrative Code Requirements for Above-50-Percent Vendors
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2018 with significant progress in all but one area)
Prior Title: Follow Administrative Code Requirements for Above-50-Percent Vendors

Health's management acknowledges they are still making improvements to the process for ensuring new vendors in the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) are reviewed within the first six months of authorization to validate that they are not a 50-percent vendor. Health updated the Administrative Code in July 2019, which now includes this stipulation; however, the monitoring report developed by Health identified vendors who have been authorized for less than 12 months, not the six months set forth in the requirements.

While federal regulations allow states to have vendors who make more than 50 percent of their grocery revenue from WIC sales, Virginia has elected to prohibit 50-percent vendors entirely. Administrative Code of Virginia (12VAC5-195-310) prohibits Virginia WIC vendors from being or becoming 50-percent WIC vendors. To ensure compliance with this state requirement, 12VAC5-195-310 requires a review of newly authorized WIC vendors for above-50-percent status after six months in the WIC program. If it is determined that a retailer is an above-50-percent-vendor, Family Health must remove the retailer from the WIC program.

Family Health division management should ensure staff are knowledgeable about and comply with specific requirements for the WIC program as set out in the Administrative Code. Health should continue to refine their reporting and reviewing capabilities to allow them to identify vendors who make more than 50 percent of their grocery revenue from WIC sales within their first six months of authorization.

Continue Addressing Compliance with the Conflicts of Interest Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Comply with the Conflicts of Interest Act

Health's management acknowledges that corrective action is ongoing to ensure that all employees designated as occupying positions of trust complete the required Statement of Economic Interest (SOEI) training within the required timeframe. Pursuant to § 2.2-3130 of the Code of Virginia, SOEI filers must complete orientation training to help them recognize potential conflicts of interest. Employees in positions of trust must complete this training within two months of hire and at least once during each consecutive period of two calendar years.

Human Resources should monitor all employees designated in positions of trust to ensure they complete the required SOEI training once within each consecutive period of two calendar years. Human Resources should also update the notification system to include the SOEI Orientation and all other required trainings. Health is continuing to address this issue and estimates completing the corrective action by December 2020.

Strengthen Controls over Year End Accrual Reporting
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Medical Assistance Services needs to strengthen controls over financial reporting information submitted to Accounts. Medical Assistance Services submits information on year-end accruals to Accounts who uses this information in preparation of the Commonwealth's financial statements. The information submitted by Medical Assistance Services contained several errors, which affected multiple accounts and funds as follows:

- Staff did not correctly include DBHDS supplemental payments in the calculations supporting year-end payables. As a result, multiple adjusting journal entries related to Medicaid payables and federal receivables were understated by $8.4 million.

- Staff did not use the correct Excel formulas in calculating the pharmacy rebate receivable, which caused a misclassification between funds. As a result, three adjusting journal entries were misstated by $8.1 million.

- There were several less significant errors that impacted multiple adjusting journal entries and ranged from $86,000 to $2.5 million.

In addition, Medical Assistance Services' documentation supporting their methodology for preparing this information does not adequately document certain aspects of the process.

Medical Assistance Services' financial activity is material to the Commonwealth's financial statements, so it is essential for them to have strong financial reporting practices. Policies and procedures over financial reporting information, as a best practice, should be detailed and thorough with a sufficient review process to prevent and detect potential errors and omissions. Also, the Fiscal, Budget, and Provider Reimbursement divisions should collaborate to complete the year-end accrual information reported to Accounts since the process relies on information from all three divisions. Lastly, when using accounting estimates in financial reporting, best practices dictate that management document the basis for the methodology.

As a result of these errors, Medical Assistance Services' staff had to resubmit information to Accounts causing inefficiencies for their staff as well as delays for Accounts' staff. There are multiple factors that contributed to these errors. First, there was a lack of communication between the Fiscal and Budget divisions. In addition, several errors were the result of incorrect spreadsheet formulas not detected by staff. The overall complexity of the calculations, along with reliance on various formulas in the spreadsheets, increases the risk of human error.

Medical Assistance Services should strengthen their controls over the preparation of year-end financial reporting information for Accounts. Although there were less significant errors in the

information than in the prior year, this information submitted to Accounts continues to be an issue. Medical Assistance Services should consider incorporating a technical supervisory review into the process given the complexity of the information to ensure significant errors are detected and prevented. Also, as part of preparing the information, the various divisions should collaborate as needed to ensure there is a common understanding of significant financial reporting policies and that submitted information is accurate. Lastly, the current methodology has been in place for a number of years and there have been significant changes in the Medicaid program over the last few years. Medical Assistance Services should re-evaluate their methodology and ensure it is the most efficient and effective approach for determining year end accrual amounts.

Complete and Approve the System Security Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

Medical Assistance Services continues to not have a complete and formally approved System Security Plan (Security Plan) with the third-party service provider that manages the claims processing system. Medical Assistance Services has been working with the provider to ensure they comply with their contractual requirements and complete the Security Plan; however, multiple gaps remain between the provider's controls and Medical Assistance Services' internal policies and procedures.

Medical Assistance Services received a Security Plan revision from the third-party service provider in October 2019 and planned to review and approve it by the end of December 2019, depending on the gaps that remain. However, Medical Assistance Services did not complete the review due to turnover in its CISO and Risk Manager positions and dedicating its resources to address the COVID-19 pandemic to support the agency's mission-critical functions.

The contract between Medical Assistance Services and the third-party service provider, section 6.0 Security and Risk Assessment, states that the provider will maintain a current Security Plan according to Medical Assistance Services' policies, procedures, standards, and guidelines. Additionally, 45 C.F.R. § 95.621 requires the establishment of a security plan that addresses various system security requirements.

A Security Plan is important because it documents the minimum control requirements the third-party service provider must implement to protect confidential and sensitive Commonwealth data. Without a complete Security Plan that is formally approved by Medical Assistance Services and the provider, the claims processing system may lack certain controls to protect the confidentiality, integrity, and availability of its mission-essential data. Additionally, without a complete Security Plan, the roles and responsibilities between Medical Assistance Services and the provider may be unclear, thereby increasing the risk of service disruption or data breach due to missing or ambiguous controls.

Medical Assistance Services should dedicate the necessary resources to review and approve the revised Security Plan received from the third-party service provider. Furthermore, Medical Assistance

Services should ensure the Security Plan aligns with the requirements in their own policies, procedures, standards, and guidelines. It is our understanding Medical Assistance Services plans to complete the Security Plan by March 2021.

Remove Separated Employee Access in a Timely Manner

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2017)

Medical Assistance Services' management acknowledges that corrective action is ongoing to ensure that effective, regular communication is established to report staff changes to those individuals responsible for managing systems access to ensure users' access is removed timely. The Security Standard and Medical Assistance Services' IT Access Control AC-1 Policy, Section A11(b)(i) requires that "all user accounts must be disabled immediately upon separation or within 24 business hours upon receipt by the Office of Compliance and Security." Medical Assistance Services was not removing access to the claims processing system timely for individuals who no longer needed access. Medical Assistance Services is continuing to address this issue and estimates completing the corrective action by January 2022.

Continue Improving the Overpayment Collection Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2016)

Medical Assistance Services' management acknowledges that corrective action is ongoing to evaluate resources assigned to the Accounts Receivable area to ensure that they can perform the necessary functions in accordance with policies and procedures. Medical Assistance Services, to comply with §§ 2.2-4800 through 2.2-4809 of the Code of Virginia, established procedures to pursue collection of overpayments from recipients and providers but did not have sufficient resources to follow the established procedures. Medical Assistance Services is continuing to address this issue and estimates completing the corrective action by January 2021.

Improve Controls over Income Verification for the TANF Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Social Services continues to work on implementing a control to ensure the Income Eligibility and Verification System (IEVS) is used when determining eligibility for Temporary Assistance to Needy Family (TANF) participants. Social Services submitted a change request to Enterprise Business Solutions to design and implement a defined process for working the IEVS matches. The design for the new IEVS process was completed and implemented in the August 2020 release for fiscal year 2021. IEVS will have a new requirement for Local Departments of Social Services to have background investigations, including Federal Bureau of Investigation (FBI) fingerprinting for employees who can access IEVS as it contains federal tax information. Virginia law does not require local agency employees to obtain background investigations; therefore, Social Services submitted a legislative proposal, and the proposal is currently in the Office of the Governor undergoing review. This new requirement of IEVS will not be fully operational until after a change in legislation through the General Assembly.

45 C.F.R § 205.55 requires agencies to collect income information through IEVS. By not ensuring that IEVS is used when verifying income for TANF participants, Social Services cannot verify that participants in the TANF program have met all eligibility requirements. IRS Publication 1075, Section 5.1.1 Background Investigation Minimum Requirements, states background investigations for any individual granted access to federal tax information must include, at a minimum, FBI fingerprinting, check where the subject has lived, worked, and/or attended school within the last five years, and check citizenship/residency. Social Services should ensure the implementation of the new IEVS process for local agencies processing TANF applications properly verifies income and is utilized when determining eligibility for TANF. Additionally, Social Services should implement policy and procedures when the legislation is passed requiring background checks of local agency employees who access IEVS.

Continue to Improve Controls over SNAP Federal Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Controls over SNAP Federal Reporting

Finance and Enterprise Business Solutions continues to work together to ensure all information submitted in the FNS-209 "Status of Claims Against Households" Report (FNS-209) can be sufficiently validated. In fiscal years 2018 and 2019, Social Services could not provide supporting documentation for some line items in the quarterly FNS-209 reports. Enterprise Business Solutions scheduled two system changes to be released in production in September 2020 that should ensure the FNS-209 is accurate and can be adequately supported. Additionally, Finance created policies and procedures over the reporting process to ensure accurate reporting of claims against households.

7 C.F.R. § 273.18(m) requires agencies to maintain a system for monitoring recipient claims against households that maintains claims records and corresponding receivable information. The system must also be able to produce summary reports and reconcile to supporting records. Reporting potentially inaccurate or incomplete information prevents the United States Department of Agriculture, Food and Nutrition Service from adequately monitoring the status of claims against households. Finance and Enterprise Business Solutions should continue to ensure that all amounts in the FNS-209 reports are adequately supported.

Continue to Improve Controls over TANF Federal Performance Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Controls over TANF Federal Performance Reporting

Enterprise Business Solutions should continue to correct system deficiencies to ensure all information submitted in two TANF performance reports, the ACF-199 "TANF Data Report" and ACF-209 "SSP-MOE Data Report," is accurate. In fiscal years 2018 and 2019, we identified instances where key line items in these reports did not agree with data in the case management system. These reporting errors were attributed to the implementation of the case management system. In March of 2020, a system update was released to fix two of the data fields; however, there are still additional improvements needed to address all of the deficiencies with TANF reporting.

45 C.F.R. § 265.7(b) requires states to have complete and accurate reports, which means that the reported data accurately reflects information available in case records, is free of computational errors, and is internally consistent. Reporting potentially inaccurate or incomplete information prevents the Administration for Child and Families from adequately monitoring Social Services' work participation rates and overall performance for the TANF program. In addition, if Social Services is found to not be meeting minimum work participation rates, a penalty can be imposed on the awarded grant.

Ensure Appropriate Oversight over Divisions' Monitoring Activities
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Ensure Subrecipient Reviews Adhere to Monitoring Plan

Social Services continues to not exercise agency-wide oversight over the subrecipient monitoring process to ensure various divisions are following the established monitoring plans. Agency-wide oversight also includes producing reports to consolidate the monitoring activity agency-wide. Social Services has not produced quarterly reports to brief Executive Management on subrecipient monitoring activities for each division in fiscal years 2018, 2019, and 2020. During fiscal year 2019, Social Services underwent a reorganization and the oversight for the agency's subrecipient monitoring transitioned from the Community and Volunteer Services to Compliance. In fiscal year 2020, Compliance has not developed a monitoring oversight process as the Lead Subrecipient Monitoring Coordinator. Without

providing reports to executive management, we are not able to determine if Social Services is assessing each of its division's completed subrecipient reviews and if Executive Management is acting upon possible deviations from the plan.

2 C.F.R. § 200.332(d) requires pass-through entities to monitor the activities of subrecipients as necessary to ensure that the sub-award is meeting grant requirements. To aid in this process and mitigate risk, Social Services' approach includes developing annual monitoring plans across divisions, which outline the review process, and reporting the results of the reviews to Executive Management quarterly. Social Services should ensure all divisions are adhering to the established approach for monitoring subrecipients. Specifically, Social Services should work to ensure progress reports from each division are consolidated and provided to Executive Management for review and monitoring of subrecipients.

Review Audits for Non-Locality Subrecipients and Communicate Results Timely

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Continue to Improve Controls over Subrecipient Monitoring

Social Services continues to not provide assurance that audits are conducted and reviewed for non-locality subrecipients expending $750,000 or more in federal funds and that management is making timely decisions based on the results of the audit report reviews. Community and Volunteer Services was responsible for tracking and reviewing all other entities' (non-localities) audit reports; however, during fiscal year 2019, the subrecipient monitoring oversight responsibility transitioned to Compliance. During fiscal year 2020, there were no reviews of audit reports performed for non-locality subrecipients. In addition, Social Services has not developed policies and procedures to ensure subrecipients other than localities are monitored in accordance with all federal requirements. By not ensuring subrecipients receive the required audits and not reviewing those audit reports, Social Services is unable to provide assurance that it is meeting the audit requirements set by the federal regulations. Additionally, without providing senior management the results of the audit reports timely, management cannot make decisions within the timeframes set by the federal regulations.

According to the Uniform Guidance 2 C.F.R. § 200.332, all pass-through entities must verify their subrecipients are audited if it is expected that subrecipient's federal awards expended during the fiscal year equaled or exceeded $750,000 and requires pass-through entities to issue management decisions within six months of acceptance of the audit report. Social Services should ensure non-locality subrecipients are monitored in accordance with all federal requirements. Additionally, Social Services should develop a process to ensure that senior management and other responsible parties are notified timely of the results of the non-locality audit reviews so that prompt and meaningful management decisions can be issued in accordance with federal requirements.

Continue Improving Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2016, with significant progress in all but one area)

Social Services continues to make progress implementing certain security procedures over the database supporting its financial reporting system in accordance with the Security Standard and industry best practices.

Since the prior year, Social Services implemented database security controls and procedures to its case management system but was unable to apply those controls to the remaining database environment. Social Services experienced turnover in its CIO position, resulting in additional organizational changes for its IT Services and Information Security and Risk Management departments. Additionally, Social Services dedicated its resources to higher priorities to support its mission-essential functions due to the COVID-19 pandemic. These events prevented Social Services from hiring additional personnel to apply and manage the security procedures to the financial reporting system. We communicated the remaining weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The Security Standard requires agencies to implement certain minimum controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not implementing the controls discussed in the FOIAE communication, the system's database is not secure against known vulnerabilities. This increases the risk for malicious users to exploit those vulnerabilities and compromise sensitive Commonwealth data.

Social Services should continue implementing the database procedures and controls in accordance with the Security Standard. This will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Continue Developing Record Retention Requirements and Processes for Electronic Records
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Develop Records Retention Requirements and Processes for Case Management System

Social Services continues to develop and implement record retention requirements for its case management system. We communicated the weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Since the prior year audit, Social Services has worked with its external vendor that assists in supporting the case management system to gather retention requirements from the applicable business divisions. Social Services relies on the external vendor to develop controls and processes for the case

management system, so the information gathered will assist the vendor to develop a process to remove specific data from the system after reaching the retention threshold.

Federal regulations require different record retention requirements for different federal programs. Additionally, the Virginia Public Records Act (§ 42.1-91 of the Code of Virginia) requires each agency to be responsible for ensuring that its public facing records are preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration. Furthermore, the Security Standard, Section CP-9-COV, requires for every IT system identified as sensitive relative to availability, an agency implement backup and restoration plans that address the retention of the data in accordance with the records retention policy.

Retaining records longer than necessary causes the Commonwealth to spend additional resources to maintain, back-up, and protect the information. Additionally, without documenting and implementing record retention requirements, Social Services may not be able to ensure that backup and restoration efforts will provide mission-essential information according to recovery times.

Social Services should continue to identify the remaining retention requirements for the data within its case management system. Additionally, Social Services should continue coordinating with its vendor to develop and implement a process, whether manual process or automated control, to ensure consistent compliance with the retention requirements for each data set within Social Services' IT systems.

Continue Improving Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Improve Web Application Security

Social Services continues to not configure a sensitive web application in accordance with the Security Standard. We determined that Social Services has not remediated the five control weaknesses identified in the previous year and communicated them to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data.

Social Services experienced turnover in its CIO position, resulting in additional organizational changes for its IT Services and Information Security and Risk Management departments. Additionally, Social Services dedicated its resources to higher priorities to support its mission-essential functions due to the COVID-19 pandemic. These events collectively delayed Social Services from addressing the weaknesses within the web application environment.

Social Services should dedicate the necessary resources to remediate the weaknesses discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. This will help to ensure Social Services secures the web application to protect its sensitive and mission-critical data.

Continue Improving IT Change and Configuration Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)
Prior Title: Improve IT Change and Configuration Management Process

Social Services continues to improve its IT change and configuration management process to align with the Security Standard. Change management is a key control to evaluate, approve, and verify configuration changes to security components.

Since the prior year audit, Social Services corrected seven out of nine weaknesses. We communicated the remaining two weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data.

Social Services experienced turnover in its CIO position, resulting in additional organizational changes for its IT Services and Information Security and Risk Management departments. Additionally, Social Services dedicated its resources to higher priorities to support its mission-essential functions due to the COVID-19 pandemic. These events delayed Social Services from addressing the remaining weaknesses in its IT change and configuration management process.

Social Services should continue its progress to resolve the remaining two weaknesses discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. Continuing to improve Social Services' IT change and configuration management process will decrease the risk of unauthorized modifications to sensitive systems and help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Continue to Improve Access Controls to Critical Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Access Controls to Critical Systems

Social Services continues to work on implementing controls to ensure system access to critical systems is reasonable and system access reviews are performed and adequately documented. This includes Social Services' financial system, central security system, childcare system, the Commonwealth's accounting and financial reporting system, retirement benefits system, human resource system, and attendance and leave system. Social Services updated and created overall policies and procedures to reflect the requirements in the Security Standard during fiscal year 2020; however, Finance did not update the access restrictions to reflect compensating controls on the Security and Responsibility forms for the Social Services' financial system. Our review of Social Services' financial system user access identified the following:

- Three new users were granted access permissions in excess of the employee's job responsibilities, and two of the three users did not have the access listed on the approved access request form.

- One current employee had new access assigned in fiscal year 2020, however, the access request form could not be provided to show authorization, and the access did not align with the employee's job responsibilities.

- Nineteen users were granted conflicting access to Social Services' financial system according to the system's Security and Responsibility forms.

The Security Standard, Section 8.1 AC-2(j), requires the agency to "review accounts for compliance with account management on an annual basis or more frequently if required to address environmental change." Security Standard, Section 8.1 AC-6(7), requires the agency to "review on an annual basis the privileges assigned to all users to validate the need for such privileges; and to reassign or remove privileges, if necessary, to correctly reflect organizational mission/business needs." The Security Standard, Section PS-4, states that the organization, upon employee termination "disables information system access within 24-hours of employment termination." In addition, the Security Standard, Section AC-6, requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks.

Social Services should continue to update policies and procedures for all critical systems to reflect the requirements in the Security Standard. This would include ensuring access is granted based on the principal of least privilege, access is removed timely, and access does not involve conflicting roles. Social Services should perform an annual access review for all critical systems and retain documentation of this review indicating the review was performed and any actions that were taken as a result of the review.

Comply with Federal Regulations for Documentation of Employment Eligibility
Type: Internal Control and Compliance
Severity: Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Continue to Improve Internal Controls over Employment Eligibility Verification Process

Human Resources does not have sufficient internal controls over the employment eligibility verification process. During fiscal year 2020, Human Resources provided training to staff, which included all required employment eligibility practices; however, during our review we noted errors or missing documentation in seven out of 25 (28%) forms reviewed. Human Resources does not properly complete Employment Eligibility verification forms for new employees in accordance with guidelines issued by the United States Citizenship and Immigration Services of the Department of Homeland Security.

The Immigration Reform and Control Act of 1986 requires employers to verify employee's identity and employment authorization of each person they hire, as well as complete and retain a Form I-9, Employment Eligibility Verification, for each employee. Per M-274, issued by the United States Citizenship and Immigration Services (M-274), Form I-9s must be retained for a period of at least three years from the date of hire or for one year after employee's employment termination, whichever is longer. The United States Citizenship and Immigration Services sets forth federal requirements for completing the Form I-9 in M-274. Not complying with federal regulations could result in civil fines and/or criminal penalties and debarment from government contracts. By not performing due diligence regarding Form I-9s as required by the Immigration Reform and Control Act of 1986, Human Resources is in noncompliance with federal regulations.

Human Resources should continue to communicate policies and procedures to employees, provide training, and ensure all employees follow federal guidelines when verifying employment eligibility for newly hired employees. Additionally, Human Recourses should ensure Form I-9s are retained for all employees, as required by United States Citizenship and Immigration Services.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 15, 2021

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records, operations, and federal compliance of the **Agencies of the Secretary of Health and Human Resources,** including federal programs, as defined in the Audit Scope and Methodology section below for the year ended June 30, 2020. We conducted this audit 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, in support of the Commonwealth's Annual Financial Report and Single Audit. 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.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of the Agencies of the Secretary of Health and Human Resources' financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia and test federal compliance in support of the Commonwealth's Single Audit for the year ended June 30, 2020. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, in each agency's financial systems, and in supplemental information and attachments submitted to the Department of Accounts (Accounts); reviewed the adequacy of their internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings and recommendations from prior year reports.

Audit Scope and Methodology

Management of the Agencies of the Secretary of Health and Human Resources has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following federal grant programs, significant cycles, classes of transactions, and account balances at the following agencies:

Department of Behavioral Health and Developmental Services

- Accounts receivable
- Commonwealth's retirement benefit system
- Community Service Board contracts
- Federal revenues, expenses, and compliance for:
  - Block Grant for Community Mental Health Services
  - Opioid STR
- Information system security
- Institutional revenues
- Licensing behavioral health providers
- Operational expenses
- Payroll expenses
- Systems access controls

Department of Health

- Accounts payable
- Accounts receivable
- Collection of fees for services
- Commonwealth's retirement benefit system
- Cooperative agreements between Health and local governments, including:
  - Accounts payable
  - Aid to and reimbursement from local governments
  - Cost allocations
- Federal revenues, expenses, and compliance for:
  - Child and Adult Care Food Program
- Information system security
- Inventory
- Payroll expenses
- Rescue squad support
- Systems access controls

Department of Medical Assistance Services

- Accounts payable
- Accounts receivable
- Contract management
- General Fund revenues (drug rebate) and expenses

Federal revenues, expenses, and compliance for:
- Medicaid Cluster
- Children's Health Insurance Program

Provider assessment revenues and expenses
Information system security

Department of Social Services

Accounts payable
Accounts receivable
Budgeting and cost allocation
Child Support Enforcement additions and deletions
Eligibility for the following programs:
- Child Care and Development Fund
- Low Income Heating and Energy Assistance
- Temporary Assistance for Needy Families

Federal revenues, expenses, and compliance for:
- Child Care and Development Fund
- Child Support Enforcement

Network and system security
Subrecipient monitoring
- Child Care and Development Fund
- Medicaid Cluster
- Children's Health Insurance Program
- Crime Victim Assistance

Supplemental Nutrition Assistance Program supplemental information
System access controls

The following agencies under the control of the Secretary of Health and Human Resources are not material to the Comprehensive Annual Financial Report for the Commonwealth of Virginia. As a result, these agencies are not included in the scope of this audit:

Department for Aging and Rehabilitative Services
Department for the Blind and Vision Impaired
Department for the Deaf and Hard-of-Hearing
Department of Health Professions
Office of Children's Services
Virginia Board for People with Disabilities
Virginia Foundation for Healthy Youth
Virginia Rehabilitation Center for the Blind and Vision Impaired
Wilson Workforce and Rehabilitation Center

We performed audit tests to determine whether the agencies' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with

provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the agencies' operations. We performed analytical procedures, including budgetary and trend analyses. We also tested details of transactions to achieve our objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting and federal compliance (internal control) was for the limited purpose described in the section "Audit Objectives" 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. However, as described in the sections entitled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations," we identified certain deficiencies in internal control that we consider to be 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 or noncompliance 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 or material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected and corrected on a timely basis. We have explicitly identified five deficiencies in the section titled "Internal Control and Compliance Findings and Recommendations," to be material weaknesses. One material weakness titled "Ensure Consistent Application of Subrecipient Monitoring Controls," will result in the Mental Health Block Grant federal program receiving a qualified opinion on compliance.

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. We explicitly identified 44 findings in the sections titled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations," to be significant deficiencies.

In addition to the material weaknesses and significant deficiencies, we detected deficiencies in internal control that are not significant to the Commonwealth's Comprehensive Annual Financial Report and Single Audit but are of sufficient importance to warrant the attention of those charged with governance. We have explicitly identified three findings in the sections titled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations," to be deficiencies.

Conclusions

We found that the Agencies of the Secretary of Health and Human Resources, as defined in the Audit Scope and Methodology section above, properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, each agency's financial systems, and supplemental information and attachments submitted to Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the sections entitled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations."

The Agencies of the Secretary of Health and Human Resources have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter.

Since the findings noted above include those that have been identified as material weaknesses and significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards" and the "Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by Uniform Guidance," which are included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2020. The Single Audit Report will be available at www.apa.virginia.gov in February 2021.

Exit Conference and Report Distribution

We discussed this report with management for the agencies included in our audit as we completed our work on each agency. Management's responses to the findings and recommendations identified in our audit are included in the section titled "Agency Responses." We did not audit management's responses and, accordingly, we express no opinion on them.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

LCW/vks

COMMONWEALTH of VIRGINIA

ALISON G. LAND, FACHE
COMMISSIONER

DEPARTMENT OF
BEHAVIORAL HEALTH AND DEVELOPMENTAL SERVICES
Post Office Box 1797
Richmond, Virginia 23218-1797

Telephone (804) 786-3921
Fax (804) 371-6638
www.dbhds.virginia.gov

January 27, 2021

Staci A Henshaw, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw:

We have reviewed your report on our audit for the year ended June 30, 2020. We concur with the findings and our corrective action plan has been provided separately.

The Department of Behavioral Health and Developmental Services (DBHDS) has made significant progress to close several findings from prior year audits as well as those noted again this year. We greatly appreciate that this report reflects the progress made to date on those findings and the positive feedback on our ongoing corrective actions. Based on the progress demonstrated during this audit cycle, we anticipate closing several additional findings next year and are committed to making significant strides to resolve new findings noted this year. Several points noted in the new findings occurred at two facilities that share a fiscal department and are not systemic issues across the DBHDS system. Despite continuing to face unprecedented challenges in the behavioral health and developmental disability community as well as the COVID-19 pandemic this fiscal year, we are proud of our staff for their incredible efforts to face those challenges while remaining committed to enhancing our operations and system of care.

We appreciate your team's efforts, constructive feedback, and acknowledgement of progress made by the agency despite facing many challenges in the past year. Please contact Alvie Edwards, Assistant Commissioner for Compliance, Risk Management, and Audit, if you have any questions regarding our corrective action plan.

Sincerely,

Alison G. Land

Alison. G. Land, FACHE

c: Alvie Edwards

COMMONWEALTH of VIRGINIA
Department of Health
P O BOX 2448
RICHMOND, VA 23218

M. Norman Oliver, MD, MA
State Health Commissioner

TTY 7-1-1 OR
1-800-828-1120

January 6, 2021

Ms. Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

We have reviewed your report on our audit for the year ended June 30, 2020. We concur with the findings, and our corrective action plan will be provided in accordance with the Department of Account guidelines.

We appreciate your team's efforts and constructive feedback. Please contact Maisha Beasley, Internal Audit Director, if you have any questions regarding our corrective action plan.

Sincerely,

M. Norman Oliver MD

M. Norman Oliver, MD, MA
State Health Commissioner

COMMONWEALTH of VIRGINIA

KAREN KIMSEY
DIRECTOR

Department of Medical Assistance Services

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
800/343-0634 (TDD)
www.dmas.virginia.gov

January 15, 2021

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
Commonwealth of Virginia
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

We have reviewed the draft Management Report for the Department of Medical Assistance Services (DMAS) that will be included in the report for the Audit of the Agencies of the Secretary of Health and Human Resources for the Fiscal Year Ending June 30, 2020. We concur with the audit findings assigned to DMAS and will submit a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the work plans for corrective actions that DMAS will take to address the audit findings.

We appreciate your team's work and flexibility, especially in this unusual year. If you have any questions or require additional information, please do not hesitate to contact the DMAS Internal Audit Director, Susan Smith.

Sincerely,

Karen Kimsey

Karen Kimsey

COMMONWEALTH of VIRGINIA
DEPARTMENT OF SOCIAL SERVICES
Office of the Commissioner

S. Duke Storen
Commissioner

January 22, 2021

The Auditor of Pubic Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Mrs. Henshaw:

The Virginia Department of Social Services concurs with the audit findings included in the 2020 review by the Auditor of Public Accounts.

Should you require additional information, please do not hesitate to contact Ross McDonald, Director of Compliance, by e-mail at ross.l.mcdonald@dss.virginia.gov or by telephone at (804) 663-5539.

Sincerely

S. Duke Storen

S. Duke Storen

801 East Main Street · Richmond, VA 23219-2901
www.dss.virginia.gov · 804-726-7011 · TTY Dial 711

SECRETARY OF HEALTH AND HUMAN RESOURCES AGENCY OFFICIALS

As of June 30, 2020

Daniel Carey, M.D., Secretary of Health and Human Resources

Department of Behavioral Health and Developmental Services
Alison G. Land, FACHE – Commissioner

Department of Health
M. Norman Oliver, M.D., MA – Commissioner

Department of Medical Assistance Services
Karen Kimsey – Director

Department of Social Services
S. Duke Storen – Commissioner