



AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2021

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

This report summarizes our fiscal year 2021 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively, these four agencies spent \$21.3 billion or 97 percent of the total expenses for agencies under this secretariat.

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

Our audits of these agencies for the year ended June 30, 2021, 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;
- 44 findings involving internal control and its operation necessary to bring to management's attention. Of these findings, four are considered to be material weaknesses;
- 38 of the 44 findings are also considered to be instances of noncompliance with applicable laws and regulations or other matters that are required to be reported. Of these findings, one is considered to be material non-compliance; 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 two Risk Alerts that require the action and cooperation of the applicable agency's management and the Virginia Information Technologies Agency (VITA), and three operational matters as Comments to Management. The Risk Alerts are applicable to DBHDS, Health, and Medical Assistance Services. The Comments to Management are applicable to DBHDS.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
COMMENTS TO MANAGEMENT	1-3
AUDIT FINDINGS AND RECOMMENDATIONS	4
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	5-32
Department of Behavioral Health and Developmental Services	6-13
Department of Health	14-17
Department of Medical Assistance Services	18-19
Department of Social Services	20-32
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS	33-46
Department of Behavioral Health and Developmental Services	34-39
Department of Health	40-43
Department of Medical Assistance Services	44
Department of Social Services	45-46
RISK ALERTS	47-48
INDEPENDENT AUDITOR'S REPORT	49-53
AGENCY RESPONSES	54-59
Department of Behavioral Health and Developmental Services	54
Department of Health	55
Department of Medical Assistance Services	56-58
Department of Social Services	59
APA COMMENT ON MEDICAL ASSISTANCE SERVICES' RESPONSE	60
SECRETARY OF HEALTH AND HUMAN RESOURCES AGENCY OFFICIALS	61

COMMENTS TO MANAGEMENT

During the course of our audit, we became aware of operational matters that impact DBHDS facilities and the Central Office. While agency personnel may also be aware of these matters and are preparing to meet these challenges, we issue these communications to highlight their impact on operations to a broader audience to encourage continued progress by agency personnel and to ensure there is visibility into their efforts by senior-level management of the entity and the Commonwealth.

Continue to Comply with the Department of Justice Settlement Agreement

Repeat: Yes (first issued as a Risk Alert in 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 agreement 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, and sustain a full year of compliance to exit court oversight of the agreement in 2021. The Commonwealth has not yet achieved full compliance and the settlement agreement has been extended to July 1, 2022. DBHDS finalized compliance indicators with DOJ in January 2020, specifying exactly what the Commonwealth must do to achieve compliance. These compliance indicators increase reporting requirements and create a need for data quality systems to comply with negotiated metrics. These metrics help to ensure that individuals are receiving quality services that meet the needs of the target population. The need for reliable and valid data that satisfies the reporting requirements is one of the largest barriers to achieving full compliance.

Over the past year, DBHDS has increased collaboration with all involved parties to prioritize remaining actions needed to exit the settlement agreement. However, the COVID-19 pandemic, a decline in personnel across the system, and increased reporting requirements have created additional barriers to compliance. Specifically, DBHDS' decision to significantly restrict in-person contacts and other community engagements to ensure the safety of individuals during the pandemic impacted its ability to comply with the requirements of the settlement agreement. There is further risk of non-compliance if DBHDS does not receive adequate funding at the appropriate time for personnel, information technology resources, and other resources necessary to implement actions which satisfy 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 meet the requirements of the settlement agreement.

If DBHDS does not achieve and maintain compliance with the requirements of the settlement agreement, further extension of the agreement or fines and penalties to the Commonwealth are possible. We continue to encourage DBHDS to work together with Medical Assistance Services, the Governor, the Secretary of Health and Human Resources, and the General Assembly 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.

Dedicate Resources to Reduce Census Pressures and Ensure Adequate Staffing

DBHDS has experienced hardships over the last few years with high patient census and critically low staffing levels. The effects of the COVID-19 pandemic amplified many of these hardships during the fiscal year under audit. DBHDS has taken measures to increase staffing by completing salary studies, providing sign-on and retention bonuses using one-time COVID-19 pandemic funding, and using hazard pay to appropriately compensate direct care employees. Based on our review of employment data from the Commonwealth's human resources system we noted that DBHDS experienced an overall seven percent decrease in employment from fiscal years 2020 to 2021; however, the decrease was more significant for direct care staff. Specifically, within health and human services positions there was an overall 11 percent decrease in employment, with some individual facilities having a decrease as high as 23 percent. DBHDS was experiencing staff shortages before fiscal year 2020 so the additional decreases in staffing have had a significant impact on their operations. Furthermore, seven of the 12 (58 percent) facilities saw an increase in overtime pay even though staffing decreased. The most notable correlation between staffing and overtime at one facility was a 13 percent decrease in employment and a 20 percent increase in total overtime pay.

At the end of fiscal year 2021, DBHDS reported a total census to staffed bed capacity utilization rate of 95.4 percent. This high utilization rate combined with critically low staffing levels resulted in DBHDS closing admissions at five state psychiatric hospitals in July of 2021 to reduce patient census counts and build staffing levels. This closure placed the agency in noncompliance with § 37.2-809 of the Code of Virginia, also known as the "Bed of Last Resort" law; however, DBHDS deemed this necessary to ensure the safety of patients and staff. The "Bed of Last Resort" law issued in 2014 requires that state facilities accept patients under a temporary detention order (TDO) if no alternate treatment location is available. Since the implementation of the law, DBHDS reported that the number of TDO admissions to state hospitals rose from 3.7 patients a day to at or over 18 a day. This places an additional burden on state facilities if discharge rates do not match or surpass admissions. During the closure to new admissions, facilities were able to focus on building staffing levels and reducing bed capacity by discharging patients to step down or long-term care facilities. As a result, facilities were able to discharge over two hundred patients and eventually reopen to admissions as staff to patient ratios improved.

This situation has also had a significant financial impact on DBHDS. During the time the facilities were closed to new admissions, DBHDS redirected individuals seeking services to private institutions. In some cases, the diversion of admissions to private institutions is at the cost of DBHDS. Additionally,

DBHDS used emergency funds to procure additional contract staff and providers to help lighten the existing workload and issue bonuses to direct care staff in acknowledgement of their efforts during the staffing crisis. Per DBHDS, staffing contracts are expensive, sometimes up to three times the cost of regular staff salaries. We noted that contractual medical service expenses increased by over 50 percent since fiscal year 2020. Despite the measures taken by the agency to address this issue, DBHDS reports that staffing levels have not improved and have even worsened at some facilities.

The lack of proper staffing to support the high patient census could impact the safety of both patients and direct care staff. In addition, not complying with the “Bed of Last Resort” law could lead to other repercussions for the agency or the Commonwealth. We encourage DBHDS to continue to work together with the Governor, Secretary of Health and Human Resources, and the General Assembly to find solutions or improvements to the hardships identified and dedicate necessary resources to reduce census pressures and ensure adequate staffing across the system.

Status of Individual and Family Support Program Data Breach

DBHDS continues to investigate causes for a data breach it experienced over its Individual and Family Support Program (IFSP) system on October 7, 2021. The IFSP assists individuals with developmental disabilities and their families with accessing resources, services, and other assistance.

When the IFSP system went live for the public to apply for 2022 funding assistance, DBHDS identified within minutes that applicants could see the personal information, including Health Insurance Portability and Accountability Act (HIPAA) data, of other applications through the system’s portal and immediately took the system offline. This is the agency’s second data breach in three years, as a similar data breach occurred with the IFSP system in October 2019. DBHDS is currently finishing its process to identify and notify those affected by the breach and will release more information about the potential cause(s) by the beginning of the 2022 calendar year.

As the data breach occurred during fiscal year 2022, subsequent to the year-end our report covers, we will follow up further during the fiscal year 2022 audit. DBHDS should continue its efforts to notify constituents that were potentially affected by the data breach and finish investigating the cause of the breach. Additionally, DBHDS should implement controls to mitigate the vulnerabilities reported from its investigation.

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 titled “Internal Control and Compliance Findings and Recommendations.” The status of findings from prior years which have not been resolved, but progress has been made by the agency’s management in addressing the recommendation are reported in the section titled “Status of Prior Year Findings and Recommendations.” Findings in this section include an update on progress made since the issuance of the prior year’s audit report.

The following table summarizes the total number of findings by agency for fiscal years 2021 and 2020, including how many repeat and new findings are reported and how many findings are classified as material weaknesses, which is the most severe classification.

Summary of Findings by Agency

	Repeat Findings	New Findings	Material Weaknesses	Total Findings 2021	Total Findings 2020
DBHDS	9	4	0	13	16
Health	7	4	2	11	10
Medical Assistance Services	2	1	1	3	10
Social Services	11	6	1	17	17
Total	29	15	4	44	53

It should be noted that one of the material weaknesses for Health is considered material non-compliance and will result in a qualified opinion for the Women, Infants and Children (WIC) federal program in the Commonwealth’s Single Audit report for the year ended June 30, 2021. The Single Audit report will be available on APA’s website at www.apa.virginia.gov in February 2022.

Internal Control and Compliance Findings and Recommendations

Improve Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

DBHDS does not secure the database server that supports its internal accounting system in accordance with its internal policies, the Security Standard, and industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmark). We identified four 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 DBHDS to implement certain security controls to safeguard systems that contain or process sensitive data. By not meeting the minimum requirements in the Security Standard and industry best practices, DBHDS cannot ensure the confidentiality, integrity, and availability of data within its system.

The lack of a documented baseline configuration caused several of the weaknesses noted above. Additionally, DBHDS' lack of sufficient staff has prevented DBHDS from ensuring the database is secure in accordance with its policies, the Security Standard, and the CIS Benchmark. DBHDS should dedicate the necessary resources to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and industry best practices. This will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Risk Assessment Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

DBHDS is missing certain elements in its risk assessment process to ensure the agency assesses all potential risks and vulnerabilities to information technology (IT) systems and business operations. DBHDS evaluated whether some controls are in place based on the Security Standard requirements but did not assess other potential risks and vulnerabilities specific to DBHDS' environment and business processes. DBHDS also did not include an assessment of the likelihood and magnitude of impact of the risks identified. In addition, DBHDS did not submit a risk treatment plan as the Security Standard requires.

The Security Standard, Sections 6.2 and RA-3, requires DBHDS to assess risk, including the likelihood and magnitude of harm from the potential risk or threat, and review and update the risk assessment annually. Additionally, the Commonwealth's Information Technology Risk Management Standard, SEC 520 (Risk Management Standard), requires that each risk identified in the risk assessment

contain elements, such as the system name, sensitivity rating, risk vulnerability family, vulnerabilities, threats, risk summary, magnitude of impact, and a brief description of the controls in place. For risks with a residual risk greater than low, the Risk Management Standard, Sections 4.5.3 and 4.5.5, requires DBHDS to submit a risk treatment plan to the Commonwealth's Chief Information Security Officer that includes certain elements, like the authoritative source, control ID, risk summary, risk rating, status, status date, planned resolution, and resolution due date.

Without having a risk assessment that includes all the required elements, DBHDS increases the risk that it will not detect and mitigate existing weaknesses in the IT environment. By not detecting the weaknesses, it increases the risk of a malicious user compromising sensitive data and impacting the system's availability.

DBHDS uses the Commonwealth's security and risk management platform to upload or complete various documentation requirements, such as risk assessments. The Risk Management Standard, Section 3.4, also requires DBHDS to use the platform to annually complete the National Cyber Security Review (NCSR) questionnaire, which is a separate Risk Management Standard requirement that covers the core National Institute of Standards and Technology (NIST) Cybersecurity Framework components and which VITA uses to assess the Commonwealth's risk profile across all executive branch agencies. While the NCSR questionnaire assesses an agency based on Security Standard controls, which are based on NIST, it does not include elements like a summary of the risk, magnitude of impact to the agency, or planned resolution if DBHDS does not have a mitigating control in place. DBHDS believed completing the NCSR questionnaire was fulfilling the risk assessment requirements, causing DBHDS to not have a complete risk assessment process that includes all the required elements.

DBHDS should dedicate the necessary resources to complete a risk assessment for each sensitive system that includes all elements required by the Security Standard and Risk Management Standard. DBHDS should also complete a risk treatment plan for those risks identified with a residual risk greater than low that details the necessary information, like the planned corrective action and expected completion date. This will help DBHDS identify potential risks and implement adequate controls to mitigate risk to its individual systems, IT environments, and business operations.

Improve Implementation of Off-Boarding Procedures

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2014)

Prior Title: Implement Standardized Off-Boarding Procedures

DBHDS is not properly terminating employees and retaining appropriate documentation to support the completion of off-boarding procedures for terminated employees. Three of the four (75%) facilities under review did not have sufficient off-boarding policies which align with actual off-boarding procedures. While DBHDS does have off-boarding procedures, including the required completion of termination checklists, checklists vary across facilities and Central Office, are not comprehensive, 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, for nine of 40 (23%) terminated employees tested. For eight of these employees, DBHDS was unable to provide documentation to support removal of building access.
- DBHDS did not timely request removal of system access to the Commonwealth's accounting and financial reporting system for three of ten (30%) terminated users. Access removal requests for these users occurred between ten to 16 days post separation. DBHDS did not request access removal for one of these users.
- DBHDS did not timely request removal of system access to the internal patient revenue system for three of eight (38%) terminated users. Access removal requests for two of these users occurred ten to 33 days post separation. At the time of review, one terminated user was still active in the system as the facility did not notify the system administrator of the termination.
- DBHDS did not timely request removal of system access to the Commonwealth's payroll system for three of 13 (23%) terminated users. Access removal requests for these users occurred between 33 to 116 days post separation.
- DBHDS did not change the employment status to "inactive" in the Commonwealth's payroll system for four terminated employees. These employees remained active in the system ranging from 45 to 763 days post separation.
- DBHDS did not timely remove access to the Commonwealth's retirement benefits system for two of four (50%) terminated users during the fiscal year.

- DBHDS did not timely request removal of system access to the Commonwealth's human resource system for one of 11 (9%) terminated users. The access removal request for this user occurred 56 days post separation.

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 50320 recommends agencies develop and implement a termination checklist 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 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 5,500 employees and had over 1,500 separations during this period. In addition to the high volume of turnover, there were numerous factors which contributed to these issues, such as a lack of communication, insufficient oversight, competing priorities, and insufficient implementation of policies and procedures. Without proper, sufficient, and documented 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. DBHDS has increased exposure to this risk due to the secure and decentralized nature of the individual facilities' operations.

DBHDS should continue to improve the implementation of off-boarding policies and procedures across its facilities and Central Office. These policies and 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 CAPP Manual and Security Standard. Furthermore, these procedures should speak to certain cases such as job abandonment. Central Office and management across all DBHDS facilities should ensure proper implementation and adherence with termination policies and procedures to include retention of supporting documentation.

Improve Controls over the Process for Calculating Contractual Commitments

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

DBHDS Central Office did not accurately report contractual commitments to the Department of Accounts (Accounts) for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). These inaccuracies were a result of various weaknesses with DBHDS' process for calculating

commitments. Further, DBHDS has historically not reported commitments to Accounts timely. During fiscal year 2021, DBHDS reported commitments 47 days after the deadline established by Accounts. We identified the following weaknesses which resulted in DBHDS revising the non-construction and construction commitment amounts reported to Accounts:

- DBHDS does not have policies and procedures over the complex process for calculating commitments which involves estimation, manual processes, and coordination between the following divisions: Budget and Financial Reporting (Financial Reporting), Architectural and Engineering Services (A&E Services), and Procurement and Administrative Services (Procurement).
- During Procurement's compilation of non-construction contract data provided to Financial Reporting, Procurement only considers contracts procured by Central Office and does not consider contracts procured at the individual facility level.
- Procurement did not compile non-construction contract data timely following fiscal year end; therefore, data it provided to Financial Reporting was incomplete and did not include contracts which had a remaining commitment from July to September 2021.
- A&E Services and Financial Reporting used inconsistent reporting components within their internal capital project management system to produce reports which aid in the calculation of construction commitments.

The above weaknesses resulted in a \$7.4 million overstatement of non-construction commitments and a \$2.4 million overstatement in construction commitments. DBHDS also understated the commitment amount due to contracts that Procurement incorrectly excluded; however, we were not able to determine the exact amount of the understatement. In addition to the lack of policies and procedures, A&E Services, Financial Reporting, and Procurement did not complete a thorough review of their calculations which contributed to the weaknesses. Additionally, the Commonwealth's purchasing system has limited capabilities to produce reports on contractual commitments which requires Procurement to manually compile data. Lastly, Procurement and A&E Services did not complete their responsibilities related to commitments timely which impacted Financial Reporting's ability to report commitments to Accounts by the required deadline. While these weaknesses do not have a material impact, there is an increased risk that DBHDS will report inaccurate commitment amounts which could be misleading to users of the ACFR.

Accounts Comptroller's Directive No. 1-21 establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the ACFR as required by the Code of Virginia. Accounts requires state agencies to submit information as prescribed in the Comptroller's Directives and individuals preparing and reviewing the submissions are required to certify the accuracy of the information provided to Accounts.

DBHDS should improve the process for calculating commitments through the development and implementation of policies and procedures which outline each division's specific responsibilities. When developing policies and procedures, DBHDS should ensure there are proper controls in place over estimations and manual processes. Further, DBHDS should ensure there is proper oversight and communication between all divisions to ensure accurate and timely reporting of commitments.

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 do not have sufficient processes and controls over the employment eligibility verification process. During fiscal year 2021, we found that Human Resources Departments (Human Resources) at three of the four facilities (75%) tested did not complete Employment Eligibility Verification forms (Form I-9) in accordance with guidelines issued by the United States Citizenship and Immigration Services of the Department of Homeland Security. Of the forms reviewed, we noted various exceptions for 26 of 40 (65%) employees. Specifically, we found the following:

- Human Resources could not locate the Form I-9 for two of 40 (5%) employees tested.
- Human Resources did not ensure completion of all required fields in Section 1 of the Form I-9 for 16 of 40 (40%) employees tested.
- Human Resources did not properly complete Section 2 of the Form I-9 for ten of 40 (25%) employees tested. Further, Human Resources accepted expired documentation providing proof of identity and employment authorization (List A Documents) for one of these employees.
- Human Resources did not properly complete electronic verification (E-Verify) and reverification procedures for four of 40 (10%) employees tested.

In addition, one facility did not have written policies and procedures over the employment eligibility process. A separate facility had written policies and procedures; however, they were not sufficiently detailed to allow them to be followed in the event of turnover and the procedures presented conflicting information in comparison to the United States Citizenship and Immigration Services instructions.

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 United States 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.

The issues listed above occurred because Human Resources at the facilities did not have experienced staff with sufficient knowledge regarding the Form I-9 process. Additionally, policies and procedures were not adequate for staff with employment eligibility responsibilities to complete the Form I-9 in accordance with the requirements. Management should provide adequate training to Human Resources staff on the proper completion of the Form I-9 and ensure Human Resources properly completes, reviews, and retains the forms in accordance with the United States Citizenship and Immigration Services guidelines. Furthermore, management should develop and document sufficient policies and procedures over the employment eligibility verification process to ensure compliance with the requirements detailed by the United States Citizenship and Immigration Services guidelines.

Ensure Compliance with the Conflict of Interests Act

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

DBHDS is not properly identifying and tracking individuals in a position of trust to ensure compliance with the Conflict of Interests Act (COIA) requirements. As DBHDS only evaluates individuals in a position of trust annually prior to the filing period, DBHDS does not provide proper and timely notification of filing and training requirements to individuals upon hire or promotion into a position of trust. Based on our review, we identified five employees in a position of trust with senior-level, decision-making responsibilities who did not file a Statement of Economic Interest (SOEI) form or complete the required training upon hire. In addition, due to a misunderstanding of filing requirements, one out of nine (11%) board members did not file a financial disclosure by the required deadline.

We also determined that DBHDS did not ensure all employees in a position of trust completed the required COIA training. Twelve out of 14 (86%) employees selected did not complete COIA training within the last two years. Six of these employees have never completed COIA training. DBHDS has a process for providing COIA training but does not monitor to ensure completion of training.

Per the Code of Virginia § 2.2-3114, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council, as a condition to assuming office or employment, and thereafter shall file such a statement annually on or before February 1. Additionally, per Executive Order Number Eight (2018), positions of trust include senior-level positions with responsibility affecting legislative policies and rule-making authority or substantive authorization and decision-making regarding policy, contracts and procurement, audits, licensure, inspections and investigations, and investments or other financial matters. Sections 2.2-3128 through 2.2-3131 of the Code of Virginia requires that each employee within a position of trust complete COIA training within two months of their hire date and at least once every two years after the initial training.

Without appropriately identifying employees in positions of trust and ensuring completion of required training, DBHDS could be susceptible to actual or perceived conflicts of interest and may be limited in its ability to hold its employees accountable for not knowing how to recognize and resolve a conflict of interest. Employees and board members could be subject to penalties for inadequate disclosure on their filings, as outlined within § 2.2-3120 through § 2.2-3127 of the Code of Virginia. DBHDS follows the Department of Human Resource Management Policy 2.1 over hiring but does not have their own internal policies and procedures to meet Code of Virginia requirements for COIA filing and training.

DBHDS should implement a process to identify employees within positions of trust and ensure that they file appropriate disclosures upon hire or promotion, and subsequently at each annual filing period. In addition, DBHDS should track these individuals to ensure COIA training is completed timely. Finally, DBHDS should create and implement their own policies and procedures to reflect current Code of Virginia requirements and the guidance issued by the Commonwealth's Ethics Advisory Council.

Strengthen Controls over Financial Reporting

Type: Internal Control

Severity: Material Weakness

Repeat: No

Health needs to strengthen controls over financial reporting information submitted to Accounts. The Office of Financial Management (OFM) is responsible for submitting information to Accounts including multiple attachments used in preparation of the Commonwealth's ACFR. Health submitted multiple items to Accounts late and had to resubmit the following items as they contained errors:

- OFM is required to report information on year-end inventory to Accounts on Attachment 8. The initial submission was not correct and OFM had to submit revised information because they did not have accurate information for personal protective equipment (PPE) inventory received or used during the year. Although Health developed a process to track the PPE received and used, local health districts did not follow the process and there was a lack of oversight from the central office. As a result, there was a lack of accurate inventory information for year-end financial reporting to Accounts.
- OFM is required to report information on accounts receivable to Accounts on Attachment 21. The initial submission was several weeks late and had a \$2.3 million misclassification. OFM had to correct this information and resubmit the information to Accounts. The untimely submission of this information also resulted in a finding in the agency's internal Agency Risk Management and Internal Controls Standards (ARMICS) review.

In addition to the two items above, Health also submitted other multiple year-end reporting items late. These include Supplemental Item #5 (Adjusted Payables) which was 26 days late and Attachment 31 (Report of Financial Condition) which was 47 days late. Lastly, Accounts' included Health in its two most recent quarterly reports for failing to respond to inquiries from Accounts on various financial reporting issues. These issues included delays in submitting required Coronavirus Relief Fund reporting information and providing explanations about an accounting entry to a federal cash pass-through account.

Health's financial activity is material to the Commonwealth's ACFR, so it is essential for the agency to have strong financial reporting practices. Health should submit financial reporting information, as a best practice, to Accounts by their due dates and communicate any expected delays as soon as they are known.

There are several factors which contributed to these issues in OFM. Overall, the entire agency has been under stress with the additional responsibilities added with the COVID-19 pandemic and the agency's role in statewide health policy. Specific to OFM, this division has experienced a significant amount of turnover over the last year, having as many as ten vacancies in the division at various times. This level of turnover represents 25 percent of the division's overall staffing level and impacted the ability

of OFM to effectively perform all of its functions. Additionally, the Director of General Accounting was on extended leave for several months which also contributed to these issues.

We have multiple recommendations to address the various issues in this finding. Management should work with OFM to promptly fill vacant positions to ensure a more stable and adequate staffing level in this division. It is our understanding that this is a priority for the division, and they are currently taking steps to address this. As part of this, OFM should ensure they have adequate written policies and procedures, as well as identify opportunities for cross-training, to ensure that they have adequate measures in place to mitigate the effects of significant turnover in the future. Related to PPE inventory, OFM needs to evaluate the financial reporting implications of this inventory and work with other divisions to ensure adequate processes are in place to properly track, manage, and provide accurate information for financial reporting of this inventory going forward.

Follow Eligibility Documentation Requirements for Women, Infants and Children Program

Type: Internal Control and Compliance

Severity: Material Weakness

Repeat: No

Local health department eligibility staff did not complete required eligibility documentation for certain recipients under the WIC program. As a result of the COVID-19 pandemic, Health implemented new procedures for determining eligibility remotely which required proof of identification through alternative methods. If local health staff were unable to collect this proof of identification, the procedures required them to complete an affidavit to confirm identity and residency. For 15 of 25 (60%) cases, the local health department staff did not obtain acceptable forms of proof of identification or complete an affidavit confirming identity and residence requirements.

Local health department staff are primarily responsible for determining eligibility for the WIC program. In March 2020, with the onset of the Public Health Emergency (PHE), the federal government issued a waiver related to physical presence and requirements to address situations where staff could not obtain documentation required for eligibility determinations in person. The waiver allowed states to come up with alternative policies and procedures to verify identity and residence requirements. To address this situation, Health initially developed policies and procedures that deferred identification and residency requirements for applications and eligibility recertifications. In June 2020, the United States Department of Agriculture Food and Nutrition Service (FNS) determined that these policies and procedures were not adequate and that proof of identification through encrypted emails or other approved collection methods was necessary. If local health staff were unable to collect this proof of identification, they were to complete an affidavit to verify identity and residency. Additionally, FNS communicated that Health should have recipients sign a statement as to why they could not provide proof of identification or residency.

When local health department staff do not verify identification and residential eligibility for recipients, there is a risk that WIC benefits could be paid to ineligible recipients. In addition, if local

health department staff do not complete an affidavit and maintain a copy, recipients cannot be held accountable for their information.

Local health department staff did not verify WIC applicants' identification and residential eligibility due to inadequate policies and procedures initially created in response to the FNS waiver. There was limited guidance from FNS once the COVID-19 pandemic occurred, and Health did not receive guidance to update their policies and procedures until June 2020. Once Health updated the policies and procedures and they became effective in August 2020, there was a lack of communication from Health to the local health districts regarding their requirements related to verifying eligibility. Additionally, Health did not update their policy and procedure to require recipients to sign a statement as to why they could not provide proof of identification.

Health central office staff should work with local health department staff to ensure they adhere to policies and procedures and maintain required documentation for WIC eligibility. Health central staff should update the policies and procedures over remote WIC services to include a requirement that recipients must sign a statement as to why they cannot provide proof of identity and residency, if applicable, and should communicate these updated policies and procedures to all local health districts.

Improve Service Provider Oversight

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Health does not perform certain processes to monitor security control compliance by external service providers that do not qualify for VITA's Enterprise Cloud Oversight Services (ECOS) as required by the Security Standard. We identified weaknesses in this area, which we communicated 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. Additionally, Health did not obtain a Service Organization Control (SOC) report for critical outsourced services for its third-party service provider for the WIC Electronic Benefit Transfer System.

The Security Standard requires agencies to maintain compliance through documented agreements with providers and oversight of services provided. Additionally, the Security Standard requires that organizations employ appropriate processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. By not meeting the minimum requirements in the Security Standard, Health cannot ensure the confidentiality, integrity, and availability of data within its systems. CAPP Manual Topic 10305 requires that agencies have adequate interaction with service providers to gain an appropriate understanding of the service provider's control environment and agencies must maintain oversight over third-party service providers.

The Office of Information Management, the Information Security Office, the Office of Purchasing and General Services (OPGS), and the business operations managers should coordinate efforts to monitor security control compliance by external service providers on an ongoing basis. Health should

implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner to ensure availability of Health's systems.

Improve Controls over Small Purchase Charge Cards

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

Health needs to address control weaknesses found during a recent review of the agency's small purchase charge cards (SPCC) practices. The Internal Audit division hired an external consultant to perform work in support of the agency's ARMICS review. One area this review focused on was SPCC policies and procedures and compliance with the CAPP Manual. The review identified eight individual control weaknesses related to SPCC as follows:

- SPCC policies and procedures were outdated; Health last updated these procedures in 2018 and do not reflect changes in spending limits.
- SPCC log reviewers are not consistently using the OPGS 370 Supervisor/Reviewer Checklist.
- The Program Administrator did not cancel the SPCCs timely for three out of four (75%) terminated cardholders.
- The Program Administrator did not sign the Purchase Card Agreements.
- One out of 20 (5%) cardholders did not submit the Annual Review Certification to OPGS.
- Cardholder supervisors did not take the annual SPCC training by the May 31 deadline.
- Program Administrators have not been completing periodic reviews of inactive cards.

These issues are the result of several factors, including but not limited to a lack of training and adherence to Health's SPCC policies and procedures.

Non-compliance with the CAPP Manual and outdated policies and procedures increases the risk for inappropriate use of the SPCCs. Health should continue to dedicate the necessary resources to ensure timely completion of its corrective action plans to become compliant with the CAPP Manual, and update and comply with its internal policies and procedures.

Strengthen Process over Medicaid Coverage Cancellations

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

(This finding was also issued to the Department of Social Services)

Local social services eligibility staff entered an incorrect coverage cancellation code in the state's eligibility system for a Medicaid recipient who moved out of state during fiscal year 2021. As a result, Medical Assistance Services improperly reinstated Medicaid coverage for this individual and continued to make Managed Care Organization (MCO) payments on their behalf although they were no longer eligible for coverage. We detected this error in a sample of 60 individuals receiving their Medicaid coverage through an MCO. This instance resulted in known federal questioned costs of \$9,563. Questioned costs are costs that the auditor questions due to a possible violation of a federal requirement.

We further analyzed the supporting data for the entire population of MCO payments Medical Assistance Services made during the fiscal year and estimate the agency also reinstated Medicaid coverage for approximately 7,200 individuals who had an out of state address in both the claims processing system and the eligibility system, and appeared to no longer be eligible for coverage. From this detailed analysis, we estimate likely questioned federal costs of approximately \$10.9 million for fiscal year 2021.

Local social services eligibility staff are primarily responsible for canceling Medicaid coverage in the eligibility system based on pre-defined cancellation codes. In Spring 2020, with the onset of the PHE, Medical Assistance Services implemented a new reinstatement review process to ensure they complied with the PHE requirements for Medicaid coverage cancellations. The Families First Coronavirus Response Act § 6008(b)(3) does not allow states to cancel Medicaid coverage during the PHE except in the following situations – an individual's death, an individual requests the cancellation of coverage, or an individual permanently relocates to another state. To ensure compliance with these requirements, Medical Assistance Services began reviewing coverage cancellation information on a monthly basis to ensure eligibility staff only canceled coverage for allowable reasons during the PHE. Under the process, Medical Assistance Services reviewed cancellation codes in the eligibility system and reinstated coverage for those cases that did not meet certain cancellation criteria. For this process to be effective, Medical Assistance Services was relying on correct cancellation codes in the eligibility system; however, for the cases we identified, eligibility staff cancelled the coverage using a generic cancellation code causing Medical Assistance Services to reinstate the Medicaid coverage.

There is some ambiguity in the cancellation codes which contributed to the eligibility staff using the incorrect codes; however, Medical Assistance Services provided information and guidance to eligibility staff throughout the year to ensure they used the correct cancellation codes. In addition, as part of the new process, Medical Assistance Services requested eligibility staff review canceled cases prior to reinstatement of the Medicaid coverage, but it does not appear that the eligibility staff consistently performed this review.

Medical Assistance Services, along with the Social Services, needs to review coverage cancellation codes and ensure there is clear guidance for local eligibility staff on when to use the various codes. For the remainder of the PHE, both agencies need to work together to ensure that eligibility staff correctly record any future coverage cancellations related to relocations to another state in the eligibility system. It is our understanding Medical Assistance Services will review enrollment actions once the PHE ends to retroactively correct enrollments and recoup any MCOs payments they determine to be inappropriate.

Continue to Improve Controls over SNAP Payments

Type: Internal Control and Compliance

Severity: Material Weakness

Repeat: Yes (first issued in fiscal year 2019)

Social Services continues to not have sufficient internal 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 (EBT) card and the vendor then draws down the funds from the federal government. The Division of Finance (Finance) completes a daily three-way reconciliation between Social Services' case management system, the vendor's system, and the federal payment system the vendor uses to draw down federal funds. When Finance identifies a reconciling discrepancy between systems, Finance will notify the Enterprise Business Solutions Division (Enterprise Business Solutions) and Cloud Infrastructure Operations Division (Operations) to resolve the discrepancy. During fiscal year 2021, there was a \$24.5 million variance between the systems. Enterprise Business Solutions could not provide support for \$24.5 million the vendor paid to recipients and drew down from the federal government. Finance uses the amount paid by the vendor when reporting revenue and expense amounts for the SNAP program to Accounts for use in the ACFR.

The Code of Federal Regulations (CFR), 2 CFR § 200.303(a) states the 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. 7 CFR § 274.4(b) states the state agency shall require the EBT system to provide reports that enable the state agency to manage the system. The reports shall be available to the state agency or FNS as requested on a timely basis. In addition, CAPP Manual Topic 20905 prescribes the level of detail agencies should reconcile records, accounts, and logs depending on the nature of the transactions. If recorded in multiple systems, transactions should be traceable from one system to another, any variance between accounting data should be traceable to specific transactions, and agencies should explain and justify all variances.

Enterprise Business Solutions did not receive the necessary information from the case management system contractor (contractor) in order to investigate and resolve the discrepancies between Social Services' case management system and amounts the vendor provided to recipients and drew down from the federal government. Reconciliations are a key internal control for ensuring financial activity recorded in multiple systems is accurate in each of those systems and for preventing improper payments. Not resolving discrepancies and ensuring proper support for amounts the vendor draws down from the federal government could create questions as to whether the nature of the payments is permissible and could lead to the federal government disallowing charges. In addition, not addressing discrepancies noted during Finance's reconciliation process increases the risk of Finance reporting

inaccurate data to Accounts for inclusion in the ACFR. We consider this a material weakness in internal control.

When Finance notifies Operations of a reconciling discrepancy, Operations should assign a high priority level to inform Enterprise Business Solutions, Operations, and the contractor to work together to investigate and resolve all reconciling amounts Finance identified in a timely manner. In addition, Social Services should maintain appropriate documentation for all payments and amounts drawn down from the federal government.

Evaluate Subrecipients' Risk of Noncompliance

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Social Services' Division of Benefit Programs (Benefit Programs) does not evaluate subrecipients' risk of noncompliance with federal regulations as they relate to the administration of the federal programs. Benefit Programs develops its subrecipient monitoring approach using the size of the subrecipient; however, does not perform any further risk assessment procedures in order to determine the monitoring approach.

According to 2 CFR § 200.332 (b) all pass-through entities are required 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. Pass-through entities must consider the results of previous audits, subrecipient's prior experience with the same or similar subawards, and whether the subrecipient has new personnel or new or substantially changed systems.

Benefit Programs was not aware of a requirement to evaluate subrecipients' risk of noncompliance for each of the federal programs it administers. Benefit Programs established its subrecipient monitoring approach without first conducting a risk assessment which would allow it to tailor the approach to the level of risk for each subrecipient. Without consideration of the subrecipients' risk of noncompliance, Benefit Programs is not able to develop an adequate monitoring approach necessary to ensure compliance with federal awards it passes through to the subrecipients.

Benefit Programs should evaluate its subrecipients' risk of noncompliance as it relates to each federal program it administers and adequately document the risk assessment. Additionally, Benefit Programs should modify its monitoring approach based on the risk assessment to ensure it conducts adequate monitoring of subrecipients.

Ensure Appropriate Oversight over Divisions' Monitoring Activities

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2018)

The Compliance Division (Compliance) has the responsibility of being the Lead Subrecipient Monitoring Coordinator; however, Compliance continues to not adhere to its established approach to oversee subrecipient monitoring efforts to ensure various divisions are following their monitoring plans. Compliance does not conduct analysis of review efforts and does not produce detailed reports of variances and noncompliance for review and consideration by the agency's leadership. Social Services has not produced quarterly reports to brief Executive Management on subrecipient monitoring activities for each division since fiscal year 2018.

2 CFR § 200.332(d) requires pass-through entities to monitor the activities of subrecipients as necessary to ensure that the subrecipient is in compliance with federal statutes, regulations, and the terms and conditions of the subaward. To aid in this process and mitigate risk, Social Services developed an agency-wide subrecipient monitoring approach, which includes: coordinating submission of annual monitoring plans and Social Services' monitoring efforts; assessing the monitoring activities of each division to determine adherence to subrecipient monitoring plans; confirming any plan deviations; summarizing potential impact on Social Services' overall risk; producing reports to consolidate the monitoring activities agency-wide; and reporting the results of the reviews to Executive Management quarterly.

Without proper oversight over divisions' monitoring activities, Social Services is not able to assess the agency's overall compliance with subrecipient monitoring requirements. By not providing reports to Executive Management, we are not able to determine if Social Services is assessing each of their division's completed subrecipient reviews and if Executive Management is acting upon possible deviations from the plan.

Compliance has been responsible for the agency's oversight over subrecipient monitoring activities since fiscal year 2019. As of fiscal year 2021, Compliance has not implemented a monitoring oversight process. Social Services is working on automating controls over subrecipient monitoring, which should aid Compliance in fulfilling its oversight responsibilities.

Social Services should ensure there is proper oversight over divisions' subrecipient monitoring efforts. Specifically, Social Services should consolidate progress reports from each division and provide the reports to Executive Management for review and monitoring of subrecipients. Additionally, Compliance should implement manual processes until the automated system is operational.

Review Non-Locality Subrecipients' Audit Reports and Communicate Results Timely

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2018)

Prior Title: Review Audits for Non-Locality Subrecipients and Communicate Results Timely

Social Services continues to not provide assurance that non-locality subrecipients expending \$750,000 or more in federal funds are receiving audits, that Compliance is reviewing the results of those audits, and that management is making timely decisions based on the results of the audit report reviews. Compliance has not performed reviews of audit reports performed for non-locality subrecipients and has not issued any management decisions related to the audit reports since it became responsible for subrecipient monitoring in fiscal year 2019. Compliance has not yet developed internal controls to verify that non-locality subrecipients' audits take place and to review these audit reports.

According to 2 CFR § 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. Additionally, 2 CFR § 200.332 requires pass-through entities to issue management decisions within six months of acceptance of the audit report and to resolve audit findings related to the subawards.

Without verifying whether non-localities' subrecipients meet federal regulations requiring an audit and reviewing applicable 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 and Regional Directors the results of the reviews of the audit reports timely, management cannot make decisions within the timeframes set by the federal regulations. Compliance does not have resources to implement a centralized process to verify and review audit reports and is working with the corresponding program divisions to develop and implement internal controls over this process.

Social Services should monitor non-locality subrecipients in accordance with all federal regulations. Compliance should develop a process to timely notify senior management and other responsible parties of the results of the non-locality subrecipients' audit reviews so that senior management can issue prompt and meaningful decisions in accordance with federal requirements.

Strengthen Process over Medicaid Coverage Cancellations

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

(This finding was also issued to Medical Assistance Services)

Local social services eligibility staff entered an incorrect coverage cancellation code in the state's eligibility system for a Medicaid recipient who moved out of state during fiscal year 2021. As a result,

Medical Assistance Services improperly reinstated Medicaid coverage for this individual and continued to make MCO payments on their behalf although they were no longer eligible for coverage. We detected this error in a sample of 60 individuals receiving their Medicaid coverage through an MCO. This instance resulted in known federal questioned costs of \$9,563. Questioned costs are costs that the auditor questions due to a possible violation of a federal requirement.

We further analyzed the supporting data for the entire population of MCO payments Medical Assistance Services made during the fiscal year and estimate the agency also reinstated Medicaid coverage for approximately 7,200 individuals who had an out of state address in both the claims processing system and the eligibility system, and appeared to no longer be eligible for coverage. From this detailed analysis, we estimate likely questioned federal costs of approximately \$10.9 million for fiscal year 2021.

Local social services eligibility staff are primarily responsible for canceling Medicaid coverage in the eligibility system based on pre-defined cancellation codes. In Spring 2020, with the onset of the PHE, Medical Assistance Services implemented a new reinstatement review process to ensure they complied with the PHE requirements for Medicaid coverage cancellations. The Families First Coronavirus Response Act § 6008(b)(3) does not allow states to cancel Medicaid coverage during the PHE except in the following situations – an individual’s death, an individual requests the cancellation of coverage, or an individual permanently relocates to another state. To ensure compliance with these requirements, Medical Assistance Services began reviewing coverage cancellation information on a monthly basis to ensure eligibility staff only canceled coverage for allowable reasons during the PHE. Under the process, Medical Assistance Services reviewed cancellation codes in the eligibility system and reinstated coverage for those cases that did not meet certain cancellation criteria. For this process to be effective, Medical Assistance Services was relying on correct cancellation codes in the eligibility system; however, for the cases we identified, eligibility staff cancelled the coverage using a generic cancellation code causing Medical Assistance Services to reinstate the Medicaid coverage.

There is some ambiguity in the cancellation codes which contributed to the eligibility staff using the incorrect codes; however, Medical Assistance Services provided information and guidance to eligibility staff throughout the year to ensure they used the correct cancellation codes. In addition, as part of the new process, Medical Assistance Services requested eligibility staff review canceled cases prior to reinstatement of the Medicaid coverage, but it does not appear that the eligibility staff consistently performed this review.

Medical Assistance Services, along with Social Services, needs to review coverage cancellation codes and ensure there is clear guidance for local eligibility staff on when to use the various codes. For the remainder of the PHE, both agencies need to work together to ensure that eligibility staff correctly record any future coverage cancellations related to relocations to another state in the eligibility system. It is our understanding Medical Assistance Services will review enrollment actions once the PHE ends to retroactively correct enrollments and recoup any MCOs payments they determine to be inappropriate.

Continue Improving IT Change and Configuration Management Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2019)

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.

Two weaknesses continue to remain since our last review, which we communicated to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing description 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 delayed its corrective actions to dedicate its resources to higher priority projects because of the ongoing response to the COVID-19 pandemic. Additionally, Social Services' IT department has experienced staff turnover, delaying the corrective actions further. Social Services should continue its progress to resolve the remaining two weaknesses discussed in the communication marked FOIAE in accordance with the Security Standard. 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 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 a formal and effective IT risk management program that aligns with the requirements in the Security Standard. Since we first issued this finding in 2018, we provided Social Services details of IT risk management documentation missing for some of its sensitive systems. However, over the last three years, Social Services has reported a fluctuating number of sensitive systems and cannot verify the accuracy of the list of sensitive systems. Additionally, Social Services has not made progress to remediate five control weaknesses identified in the previous year.

We communicated the 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 delayed its corrective actions to dedicate its resources to higher priority projects because of the ongoing response to the COVID-19 pandemic. Additionally, Social Services' IT department has experienced staff turnover, delaying the corrective actions further. Social Services should dedicate the necessary resources to remediate the weaknesses discussed in the communication marked FOIAE in accordance with the Security Standard. This will help to ensure the confidentiality, integrity, and availability of the agency's sensitive systems and mission essential functions.

Continue Developing Record Retention Requirements for Electronic Records

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2018)

Prior Title: Continue Developing Record Retention Requirements and Processes for Electronic Records

Social Services continues to develop 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 2019 fiscal year, 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 in developing a process to remove specific data from the system after reaching the retention threshold. Social Services initially prioritized to complete corrective actions in the 2021 calendar year. However, due to limited technical resources necessary for the project, Social Services has delayed the project until 2022.

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 records-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 a manual process or automated control, to ensure consistent compliance with the retention requirements for each data set within Social Services' IT systems.

Improve Timely Removal of System Access

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Finance does not consistently deactivate terminated employees' access to Social Services' financial system in a timely manner. Our review identified that Finance did not remove access to the financial system for six terminated employees until three to 81 days after the termination date.

The Security Standard, Section PS-4, requires an organization to disable information system access within 24-hours of employment termination. By not removing access timely, Social Services is increasing the risk that terminated employees may retain unauthorized access to state systems and sensitive information.

While Finance eventually removed access for five out of the six terminated employees following their internal process of system access reviews, supervisors did not submit separation checklists to Finance timely or not at all, which prevented Finance from removing system access timely. Social Services should communicate the importance of completing and submitting a separation checklist when an employee terminates to ensure timely removal of system access in accordance with the Security Standard. In addition, Finance should update policies and procedures to reflect the requirements in the Security Standard.

Continue to Improve Access Controls over Child Care System

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2018)

Prior Title: Continue to Improve Access Controls to Critical Systems

Social Services' Central Security Team (Central Security) does not have sufficient controls in place to ensure access to the child care system is reasonable. Twenty terminated contractors retained access for 19 days after termination in Social Services' central security system. Additionally, of the 46 employees reviewed, Central Security did not retain system access forms for six (13%) employees and provided two (3%) employees access roles that did not match their approved access request form due to the form not including all available access roles.

The Security Standard, Section AC-2-COV 2(e/f), requires notification of terminations and transfers of employees and contractors and prompt removal of access when no longer needed. The Security Standard, Section PS-4, states that the organization, upon employee termination, “disables information access within 24-hours of employment termination.” Additionally, the Security Standard, Section AC-2-COV 2(a), requires granting access to the system based on a valid access authorization. The 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.

Central Security does not have sufficient policies in procedures in place to ensure staff timely remove access, verify access agrees to the authorized system request form, and retain access forms. Additionally, Central Security did not receive the separation checklist in order to terminate the contractors timely. Not communicating when a contractor terminates and not ensuring system users have appropriate access to the child care system increases the risk of unauthorized individuals having access to sensitive information.

Central Security should update their policies and procedures in accordance with the Security Standard to ensure the termination of access within 24-hours. Additionally, Central Security should update the system access forms to include all childcare system roles, and Central Security should retain all forms to ensure access is reasonable when performing the annual access review.

Review and Document Service Organization Control Reports of Third-Party Service Providers

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Social Services is not consistently reviewing its third-party service providers’ (providers) SOC reports, including subservice organizations, to ensure it implements effective complementary user entity controls. Social Services did not obtain SOC reports for two providers outsourced to process sensitive information, such as benefit card payments, and obtained and reviewed a SOC report for one provider, but did not document their evaluation of the complementary user entity controls or significant weaknesses cited in the report. Additionally, Social Services did not obtain the SOC report for a subservice organization that provides IT services for one of its providers.

CAPP Manual Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the provider’s internal control environment. Agencies must also maintain oversight over the provider to gain assurance over outsourced operations. Additionally, 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 that agencies must enforce the compliance requirements through documented agreements and oversight of the services provided.

SOC reports (specifically SOC 1, Type 2 reports) provide an independent description and evaluation of the operating effectiveness of providers' internal controls over financial processes and are a key tool in gaining an understanding of the provider's internal control environment and maintaining oversight over outsourced operations. Social Services does not have any policies and procedures related to reviewing SOC 1 reports or complementary controls, which is why Social Services did not document their evaluation of the SOC report provided and did not obtain SOC reports from subservice organizations and providers contracted by another state agency or providers that do not fall under VITA's ECOS. Without adequate policies and procedures over SOC reports, Social Services is unable to ensure that their complimentary controls are sufficient to support their reliance on the providers' controls design, implementation, and operating effectiveness and address any internal control deficiencies and/or exceptions noted in the report. Although Social 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 obtaining the necessary SOC reports or properly documenting their review of SOC reports.

Social Services should create and implement policies and procedures that comply with the requirements outlined in the CAPP Manual and Security Standard to ensure they obtain SOC 1 reports for all providers performing significant functions or processes and their subservice organizations. These policies and procedures should include documentation requirements for complementary user entity controls, the steps needed to address internal control deficiencies and/or exceptions found in reviews, and responsible staff for corrective actions necessary to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Improve Compliance with Conflict of Interests Act

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Social Services' Human Resources is not properly identifying and tracking individuals in a position of trust to ensure such individuals file the required disclosure form and complete the orientation training. Our review identified the following:

- two out of 48 (4%) board members in a position of trust did not file a financial disclosure form and complete orientation training;
- ten out of 48 (21%) board members in a position of trust did not complete orientation training;
- 12 out of 58 (21%) employees were not identified in a position of trust and did not file a SOEI form and complete orientation training;

- one out of 58 (2%) employees filed the SOEI form and completed orientation training, but Human Resources did not identify them as in a position of trust; and
- two out of 58 (2%) employees identified in a position of trust did not file a SOEI form and complete the orientation training.

Executive Order Number Eight (2018) requires that the head of each agency, institution, board, commission, council, and authority within the Executive Branch to be responsible for ensuring that designated officers and employees file their SOEI form in accordance with § 2.2-3114 of the Code of Virginia. Agency heads shall also be responsible for ensuring the appropriate individuals receive the necessary orientation on the COIA in accordance with the provisions of § 2.2-3128 of the Code of Virginia. Sections 2.2-3114 and 2.2-3118.2 of the Code of Virginia state, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council of their personal interests and such other information as is required on the form, on or before the day such office or position of employment is assumed, and thereafter shall file such a statement annually on or before February 1. Additionally, § 2.2-3128 through § 2.2-3131 of the Code of Virginia states, orientation training is required to be completed by filers within two months of their hire/appointment and at least once during each consecutive period of two calendar years.

Human Resources does not have an adequate process in place to ensure compliance with the COIA. Without appropriately identifying and tracking individuals in a position of trust, Human Resources cannot ensure that these individuals file the required disclosure form and complete orientation training. Individuals could be susceptible to actual or perceived conflicts of interest and Human Resources may be limited in its ability to hold employees accountable for not knowing how to recognize a conflict of interest and how to resolve it. Additionally, employees and board members could be subject to penalties for inadequate disclosure on their filings, as outlined within § 2.2-3120 through § 2.2-3127 of the Code of Virginia.

Human Resources should implement a process to identify employees in a position of trust upon hire or change in job responsibilities, and board members upon appointment to ensure they file disclosure forms and complete orientation training in a timely manner. Additionally, Human Resources should monitor all employees designated in a position of trust to ensure they complete the required SOEI training once within each consecutive period of two calendar years and maintain a record of such attendance.

Comply with Federal Regulations for Documentation of Employment Eligibility

Type: Internal Control and Compliance

Severity: Deficiency

Repeat: Yes (first issued in fiscal year 2018)

Human Resources does not have sufficient internal controls over the employment eligibility verification process. Social Services' policy manual includes all the required employment eligibility practices; however, Human Resources continues to not complete Employment Eligibility Verification forms in accordance with guidelines issued by the United States Citizenship and Immigration Services of the Department of Homeland Security. During our review we noted errors or missing documentation in six out of 20 (30%) forms reviewed.

The Immigration Reform and Control Act of 1986 requires employers to verify employee identity and employment authorization of each person they hire, and complete and retain a Form I-9, Employment Eligibility Verification, for each employee. Per Handbook for Employers M-274, issued by the United States Citizenship and Immigration Services (M-274), Forms I-9 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.

Failure to comply with federal regulations could result in civil fines and/or criminal penalties and debarment from government contracts. By not performing due diligence with regard to Form I-9s as required by the Immigration Reform and Control Act of 1986, Human Resources is in noncompliance with federal regulations.

Due to the high turnover in Human Resources during fiscal year 2021, management did not ensure all employees received proper training, nor did management communicate federal government requirements in regard to the employment eligibility verification process. Human Resources should 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 Resources should retain Form I-9s for all employees, as required by the United States Citizenship and Immigration Services guidelines.

Ensure Compliance with the Commonwealth's Executive Leave Policy

Type: Internal Control

Severity: Deficiency

Repeat: No

Human Resources does not receive and retain leave calendars and written leave certification letters for their at-will employees stating that they have not exceeded their leave limit during the allotted time period. Additionally, Human Resources could not provide such documentation for auditor's review.

The Commonwealth's Executive Leave Policy states that all at-will employees must certify, in writing, that their established leave limit was not exceeded during the allotted time period; employees should maintain a leave calendar to attach to the certification letters. In addition, the agency's Human Resources office must maintain these certification letters and make them available for review by the Auditor of Public Accounts.

Human Resources experienced significant turnover in managerial and staff positions during the fiscal year. Although Human Resources maintains internal policies and procedures over executive leave, it has not properly reassigned the responsibility of maintaining at-will employees leave calendars and certification letters. Without maintaining at-will employees' leave calendars and certification letters, Social Services cannot provide assurance that at-will employees complied with the provisions set forth within the Commonwealth's Executive Leave Policy.

Human Resources should properly assign responsibility of maintaining at-will employees leave calendars and certification letters within the Division. Additionally, Human Resources should maintain leave calendars and certification letters, and make them available for review by the Auditor of Public Accounts to ensure compliance with the Commonwealth's Executive Leave Policy.

Status of Prior Year Findings and Recommendations

Continue to Ensure Consistent Application of Subrecipient Monitoring Controls

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2020)

Prior Title: Ensure Consistent Application of Subrecipient Monitoring Controls

DBHDS Divisions of Administrative Services (Administrative Services) and Community Services (Community Services) continue to improve processes to ensure consistent application of subrecipient monitoring controls. However, there are three out of eight (38%) consumer-run peer support programs that are subrecipients of the Block Grants for Community Mental Health Services (Mental Health Block Grant) federal program which are being treated as contractors instead of subrecipients.

Following the identification of this issue during our fiscal year 2020 audit, DBHDS implemented subrecipient funding agreements to ensure proper application of subrecipient monitoring controls for five of these eight entities. DBHDS plans to implement subrecipient funding agreements with the remaining three entities following the expiration of the current contract terms. Additionally, during fiscal year 2021, DBHDS improved the process for assessing risk and monitoring for all eight consumer-run peer support subrecipients, but did not properly communicate federal award information to the three entities that are classified as contractors.

45 CFR § 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. As 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 continue to transition the three remaining entities to a subrecipient funding agreement following the expiration of current contract terms. DBHDS should ensure that these agreements properly communicate subawards to subrecipients in accordance with 45 CFR § 75.352(a). Further, DBHDS should continue to improve the coordination and oversight of subrecipient monitoring to ensure Administrative Services and Community Services apply consistent subrecipient monitoring controls in accordance with CFR requirements.

Continue Dedicating Resources to Support Information Security Program

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2019)

DBHDS is making progress to allocate the necessary resources to manage its information security program and IT projects. As of November 2021, DBHDS has reduced its number of sensitive systems and applications from 321 in the prior year to 183 between the Central Office and its facilities, which are now centrally located at the Commonwealth's data center. While DBHDS continues efforts to further reduce

its sensitive system inventory, 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 has filled one position in the Information Security department and two Deputy Chief Information Officer positions in the Information Technology department. However, Information Security continues to have two vacancies and Information Technology has five vacancies, limiting the agency from making progress to remediate prior year recommendations. DBHDS also continues to prioritize IT resources to support mission-critical functions in response to the COVID-19 pandemic. These events caused DBHDS to continue having some audit findings repeat for the sixth year, specifically the absence of baseline configurations and IT contingency management documentation.

As required by the Security Standard, Section 2.4.2, 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 for 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 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 continue efforts to fill the current vacancies between the Information Security and Information Technology departments. 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 strengthen the controls to protect 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 have incomplete and outdated Continuity of Operations Plans (COOP) and IT Disaster Recovery Plans (DRP) for the facilities and Central Office. In addition, the Central Office and facilities are not performing annual tests on the COOPs or DRPs.

Since the fiscal year 2020 audit, DBHDS migrated all systems from the individual facilities to the Commonwealth's central data center to ensure there is more consistency for system management and services. Additionally, DBHDS participated in the Commonwealth-wide disaster recovery test for its servers. Information Technology and Information Security are working with the Central Office's Emergency Coordinator to develop or revise COOP plans for the individual facilities and Central Office, as well as an overarching DRP that will cover all systems since the IT environment has migrated to the central data center. DBHDS expects to complete the COOP and DRP plans 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 continues to experience staffing shortages within its Information Technology and Information Security departments, causing DBHDS to prioritize tasks and delay some corrective actions.

DBHDS should update the contingency management program for the Central Office and facilities 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 Central Office and facilities 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 information technology 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 reduced its information system environment from 321 to 183 sensitive systems and applications across the Central Office and 12 facilities, with some containing HIPAA data, social security numbers, and Personal Health Information data. Additionally, DBHDS created a three-year plan to complete a baseline configuration for each system alongside other risk management documentation while continuing to reduce the number of systems and applications within its environment. DBHDS was unable to make progress to develop baseline configurations in the last year because of staffing shortages and focusing on higher priorities, such as supporting its mission-critical functions during ongoing response 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 to Implement Compliant Application Access-Management Procedures

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2018)

Prior Title: Continue to Develop and Implement Compliant Application Access Management Procedures

DBHDS continues to focus on implementing compliant access-management procedures at the facility level which meet the baseline standard defined by the Security Standard. During fiscal year 2018, the Information Security Office sent baseline security procedures to all facilities with the expectation that they would align their internal procedures with the baseline procedures by March 2018.

Due to improper monitoring of the implementation of these procedures and subsequent turnover within the Information Security Office, DBHDS has yet to confirm that facilities have implemented compliant access-management procedures. The Information Security Office has been working to reduce and standardize applications across the system to aid in the implementation of compliant access-management procedures. During fiscal year 2022, the Information Security Office plans to work directly with facilities to provide proper training on compliant access-management procedures and implement processes to ensure compliance with these procedures.

The 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. The 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 Information Security Office should continue to reduce and standardize applications across the system as necessary. Throughout this process the Information Security Office should continue to work with facilities to set reasonable deadlines, provide proper training, and monitor actions to ensure that application access-management procedures at the facility level align with the office's baseline procedures and the Security Standard.

Continue to Improve Controls over the Retirement Benefits System Reconciliation

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2014)

Prior Title: Perform and Document Commonwealth's Retirement Benefits System Reconciliations

DBHDS is working to standardize and improve policies and procedures over the Commonwealth's retirement benefits system reconciliation process. From fiscal years 2014 to 2020, Central Office and individual facilities were not properly performing and documenting various aspects of the reconciliation process. During fiscal year 2020, it was determined that all facilities have policies and procedures in place; however, DBHDS has not standardized the policies and procedures across the facilities, and the facilities are not always properly following them. Due to staffing shortages, there has been a delay in drafting and implementing the updated policies and procedures. Further, during fiscal year 2022, DBHDS will transition to the Commonwealth's new payroll and human resource system which will affect the controls in place over the reconciliation process. Due to ongoing corrective action during the period under audit and the forthcoming transition to the new system, we did not perform a detailed review of the retirement benefits system reconciliation process during the current audit.

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. 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 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.

Management should continue to standardize and improve policies and procedures over the reconciliation of the Commonwealth's retirement benefits system and ensure that staff follow the

updated procedures when performing the reconciliation. Throughout this process management should also evaluate changes in controls related to the implementation of the Commonwealth's new payroll and human resource system.

Continue to Improve Controls over Payroll Reconciliations

Type: Internal Control

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2020)

Prior Title: Improve Controls over Payroll Reconciliations

DBHDS continues to improve processes and controls over the payroll reconciliation process. During the fiscal year 2020 audit, two DBHDS facilities with a shared campus were unable to provide documentation to support the required monthly Report 10 to Report 33 reconciliation, to include proper maintenance of key control totals. Since the prior audit, DBHDS Central Office provided further guidance to facilities to ensure proper performance of payroll reconciliations and maintenance of appropriate supporting documentation. In fiscal year 2022, the agency will transition to the Commonwealth's new payroll and human resource system which will affect the controls in place over the payroll reconciliation process. Due to ongoing corrective action during the period under audit and the forthcoming transition to the new system, we did not perform a detailed review of the payroll reconciliation process during the current audit.

CAPP Manual Topic 50905 requires that agencies maintain and update key control totals every time payroll is processed, on a monthly basis, 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 to go undetected.

Management should evaluate the change in controls over the payroll reconciliation process associated with the transition to the Commonwealth's new payroll and human resource system. In addition, Central Office should develop and distribute payroll reconciliation policies and procedures to facilities that reflect these changes and meet the CAPP Manual requirements.

Continue Improving the Disaster Recovery Plan

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2019)

Health continues to not perform certain processes in its disaster recovery plan 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.

Health made progress to remediate the issues identified in the prior year but is still in the process of implementing their plan. The Security Standard requires agencies to develop IT disaster recovery components that identify each IT system that is necessary to recover agency business functions or dependent business functions. By not meeting the minimum requirements in the Security Standard, Health cannot ensure the confidentiality, integrity, and availability of data within its systems.

Health should implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard 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: Partial (first issued in fiscal year 2018)

Health continues to not properly manage certain aspects of its continuity program to meet the requirements in the Security Standard. The continuity 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 its systems.

Health should coordinate efforts among departments to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner.

Continue Improving Information Technology Change Management Process for a Sensitive System

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2020)

Prior Title: Improve Information Technology Change Management Process for a Sensitive System

Health continues to not have a formal and effective IT change control and configuration management process that includes the minimum requirements of the Security Standard for one of its 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 four control weaknesses and communicated them 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 the confidentiality, integrity, and availability of Health's information systems and data.

Health should document and 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.

Continue Strengthening the System Access Removal Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2014)

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' separation from the agency. This year, we found that Health did remove terminated users' access in a timely manner for their internal financial and accounting system; however, we again identified several instances across four other 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 continue to strengthen its access removal policy to remove each user's access from individual information systems within 24 hours of the user's separation from the agency. Human Resources should clarify its access removal notification policy and provide guidance to all users throughout the state. This will reduce the rates of non-compliance 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: Partial (first issued in fiscal year 2018)

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, we determined that Health did perform adequate system access reviews over their eligibility system for the WIC program; however, there continued to be several instances across two 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 is currently in the process of updating their internal policy to require system access reviews quarterly instead of monthly, which is still in compliance with statewide requirements. Regardless of changes they make to their internal policy, Health should ensure backup personnel are available to perform regular reviews of access in the event that the primary reviewer is unable to perform them. Additionally, Health should perform follow-up procedures when reviewers do not provide certifications within their established timeframes and should require a positive confirmation upon completion of a review. These procedures should help to reduce the number of untimely reviews and decrease the risk of inappropriate access to sensitive information systems.

Continue Strengthening the Termination Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (First issued in fiscal year 2020)

Prior Title: Strengthen Process over Employee Separations

Health continues to not properly execute all off-boarding procedures for employees who separated from the agency. During our review, we identified several instances where Health did not complete the required terminations checklist or process the final leave payouts 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. Health’s termination checklists require the removal of systems access and the surrender of all state property.

Health should continue to implement a review process of employee off-boarding documents to ensure staff properly complete all off-boarding checklists. 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. This will reduce the risk of Health not completing off-boarding checklists in a timely manner.

Continue Addressing Compliance with the Conflict of Interests Act

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2019)

Health’s management acknowledges that corrective action is ongoing to ensure that all employees designated as occupying positions of trust complete the required 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.

Health’s Office of Human Resources should continue to 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 and hold the employees accountable for untimely completion. This will reduce the rate of non-compliance with the COIA and reduce the risk of improper or incomplete conflicts disclosure. It is our understanding that Health is in the process of further updating their SOEI policy, and the policy is pending management approval.

Improve Information Security Program and Controls

Type: Internal Control and Compliance

Severity: Material Weakness

Repeat: Yes (first issued in fiscal year 2020)

Medical Assistance Services continues to address weaknesses found during an audit of IT general controls. The audit performed by an external consultant during the period April 1, 2019, through March 31, 2020, resulted in 71 individual control weaknesses out of 100 controls tested.

Non-compliance 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. Medical Assistance Services originally estimated corrective actions to be complete by June 30, 2021, but experienced delays due to staffing turnover and shortages. Medical Assistance Services' most recent corrective action update states that corrective actions are still ongoing and estimates completion by the end of the 2021 calendar year.

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.

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 was ongoing as of June 30, 2021, to establish effective, regular communication to report staff changes to ensure the Office of Compliance and Security removes users' access timely for separated employees. 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. Given that corrective action was still ongoing throughout the audit period, we did not follow up on this issue in the current audit and will test this area in the fiscal year 2022 audit to determine if Medical Assistance Services has taken adequate corrective action.

Improve Controls over Income Verification for the TANF Program

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2018)

Social Services continues to implement controls to use the Income Eligibility and Verification System (IEVS) when determining eligibility for Temporary Assistance to Needy Family (TANF) participants. In August 2020, Social Services completed the design and implemented system changes for the new IEVS process; however, due to Internal Revenue Service (IRS) security requirements, staff at Local Departments of Social Services (local agencies) are unable to use IEVS. IEVS requires local agencies 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 drafted a legislative proposal, and will present the proposal to the General Assembly in fiscal year 2022. This new requirement of IEVS will not be fully operational until after the General Assembly approves a change in legislation; therefore, local agencies will continue to determine eligibility for TANF participants by verifying income and other information using various state databases that do not contain data from the IRS.

45 CFR § 205.55 requires agencies to collect income information through IEVS. By not ensuring that local agencies use IEVS 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 that the implementation of the new IEVS process includes properly verifying income when local agencies are processing TANF applications. Additionally, Social Services should implement policy and procedures, once the General Assembly passes legislation, requiring background checks of local agency employees who access IEVS.

Continue to Communicate Subrecipient Monitoring Responsibilities to the Coordinators

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2020)

Prior Year Title: Define and Communicate Subrecipient Monitoring Responsibilities

Social Services updated the draft Agency Monitoring Plan to define subrecipient monitoring oversight responsibilities of the Compliance Division, including the role of the Subrecipient Monitoring Lead Coordinator. Compliance has not yet finalized the Agency Monitoring Plan and has not implemented oversight controls as defined in the plan.

2 CFR § 200.332 (d) requires pass-through entities to monitor the activities of subrecipients as necessary to ensure that the subrecipient is in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Without clearly defined responsibilities related to the subrecipient monitoring activities, Compliance cannot provide assurance that Social Services is adequately monitoring all of the agency's subrecipients, achieving program objectives, or complying with the federal requirements that restrict program funds. Social Services is in the process of implementing an agency-wide subrecipient monitoring system, which should aid Compliance in fulfilling its subrecipient monitoring oversight responsibilities.

Compliance should finalize the Agency Monitoring Plan to properly communicate subrecipient monitoring responsibilities within the agency and implement adequate oversight controls to achieve compliance with federal regulations.

Continue Improving Web Application Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2019)

Social Services continues to not configure a sensitive web application in accordance with the Security Standard. Since the prior year audit, Social Services has remediated one of the five previously identified weaknesses. We communicated the remaining four 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 delayed addressing the weaknesses within its web application environment due to preparing for its migration to a new data center, as well as dedicating its resources to the COVID-19 pandemic response effort. Additionally, Social Services' IT department has experienced staff turnover, delaying the corrective actions further.

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

RISK ALERTS

During the course of our audit, we encountered issues that are beyond the corrective action of agency management alone and require the action and cooperation of management and VITA. The following issues represent such a risk to several of the agencies under the Secretary of Health and Human Resources, as well as the Commonwealth during fiscal year 2021.

Unpatched Software

Repeat: No

Applicable to: DBHDS, Health, and Medical Assistance Services

VITA contracts with various information technology (IT) service providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. DBHDS, Health, and Medical Assistance Services rely on contractors procured by VITA for the installation of security patches in their systems that support agency operations. Additionally, the agencies listed above rely on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors.

As of October 2021, the ITISP contractors had not applied a significant number of critical and highly important security patches to DBHDS' and Medical Assistance Services' IT environment. In addition, as of November 2021, the ITISP contractors had not applied a significant number of critical and highly important security patches to Health's IT environment.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to systems at the agencies listed above to remediate vulnerabilities in a timely manner or taken actions to obtain these required services from another source. Missing system security updates cause an increased risk of cyberattack, exploitation, and data breach by malicious parties.

The Commonwealth's Information Security Standard, SEC 501 (Security Standard) Section SI-2, requires the installation of security-relevant software updates within 90 days of release. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 90-day window from the date of release as its standard for determining timely implementation of security patches.

DBHDS, Health, and Medical Assistance Services are working with VITA and the ITISP contractors to ensure that servers and workstations have all critical and highly important security patches installed. Additionally, our separate audit of VITA will address this issue.

Access to Audit Log Monitoring Tool

Repeat: No

Applicable to: DBHDS and Medical Assistance Services

DBHDS and Medical Assistance Services rely on the ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, these agencies rely on contractors procured by VITA to provide access to a centralized monitoring tool that collects audit log information about activities in their IT environments so that DBHDS and Medical Assistance Services can review logged activity. Additionally, these agencies rely on VITA to maintain oversight and enforce the service-level agreements and deliverables with the ITISP contractors.

While VITA did not originally enforce the deliverable requirement when the ITISP contracts were ratified in 2018, VITA tried to compel the ITISP contractor responsible for granting agencies access, such as DBHDS and Medical Assistance Services, to provide access to the monitoring tool and audit log information for the last two years. However, as of November 2021, VITA and the ITISP contractor have not been able to grant access to individual agencies due to software limitations. VITA is overseeing the ITISP contractor's current efforts to replace the existing centralized monitoring tool with a new system to grant individual agencies access to monitor audit log information.

The Security Standard, Section AU-6, requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity. Without VITA enforcing the deliverable requirements from the ITISP contractors, the risk associated with the Commonwealth's data confidentiality, integrity, and availability is increased.

DBHDS and Medical Assistance Services are working with VITA and the ITISP contractors to obtain access to the audit log information within the centralized monitoring tool to ensure they can review the activities occurring in their IT environments in accordance with the Security Standard. Additionally, our separate audit of VITA will address this issue.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 15, 2022

The Honorable Glenn Youngkin
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, 2021. 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 Comprehensive 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 Annual Comprehensive 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, 2021. 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 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 and the following significant cycles, classes of transactions, and account balances at the following agencies:

Department of Behavioral Health and Developmental Services

- Commonwealth's retirement benefit system
- Community Service Board contracts
- Information system security (including access controls)
- Institutional revenues
- Licensing behavioral health providers
- Operational expenses
- Payroll expenses

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:
 - Special Supplemental Nutrition Program for Women, Infants and Children
 - Coronavirus Relief Fund Program
 - Epidemiology and Laboratory Capacity for Infectious Diseases Program
- Information system security (including access controls)
- Inventory
- Payroll expenses
- Rescue squad support

Department of Medical Assistance Services

- Accounts payable
- Accounts receivable
- Contract management
- Contract procurement
- General Fund revenues (drug rebate) and expenses
- Federal revenues, expenses, and compliance for:
 - Medicaid Cluster
 - Coronavirus Relief Fund
- Provider assessment revenues and expenses
- Information system security (including access controls)

Department of Social Services

- Accounts payable
- 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:
 - Supplemental Nutrition Assistance Program Cluster
 - Low-Income Home Energy Assistance
 - Pandemic EBT Food Benefits
- Information system security (including access controls)
- Subrecipient monitoring
 - Supplemental Nutrition Assistance Program Cluster
 - Low-Income Home Energy Assistance
 - Medicaid Cluster
- Supplemental Nutrition Assistance Program supplemental information

The following agencies under the control of the Secretary of Health and Human Resources are not material to the Annual Comprehensive 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, and tested details of transactions to achieve our audit 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 titled "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 identified four findings in the sections titled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations," to be material weaknesses. One material weakness titled "Follow Eligibility Documentation Requirements for Women, Infants and Children Program," will result in a qualified opinion on compliance for the Women, Infants and Children federal program.

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 have identified 38 findings in the sections titled "Internal Control and Compliance Findings 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 Annual Comprehensive Financial Report

and Single Audit but are of sufficient importance to warrant the attention of those charged with governance. We have identified two findings in the “Internal Control and Compliance 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 titled “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 and recommendations 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, 2021. The Single Audit Report will be available at www.apa.virginia.gov in February 2022.

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 response to the findings and recommendations identified in our audit is 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 12, 2022

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, 2021. 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, and we appreciate that this report reflects the progress made to date on those corrective actions. We also greatly appreciate the audit team's interest and effort to evaluate the ongoing census and staffing crisis in our facilities across the Commonwealth, and the acknowledgement of ongoing efforts to identify resources and other interventions to mitigate the risks associated with these ongoing challenges. 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, FACHE
Commissioner



COMMONWEALTH of VIRGINIA

Colin M. Greene, MD, MPH
Acting State Health Commissioner

Department of Health
P O BOX 2448
RICHMOND, VA 23218

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

January 21, 2022

Staci 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, 2021. 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 Wayne Goodman, Interim Internal Audit Director, if you have any questions regarding our corrective action plan.

Sincerely,

Colin M. Greene, MD, MPH
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 13, 2022

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.

In the finding titled Strengthen Process over Medicaid Coverage Cancellations, the audit report states that eligibility staff used the incorrect cancellation codes even with DMAS providing information, direction, and guidance to Department of Social Services (DSS) eligibility staff throughout the year to ensure they used the correct process. In addition, as part of the new process, DMAS requested DSS eligibility staff review canceled cases prior to reinstatement of the Medicaid coverage, but it does not appear that the eligibility staff consistently performed this review.

Pursuant to the Families First Coronavirus Relief Act (FFCRA), signed into law on March 18, 2020, in response to the federal Public Health Emergency (PHE) due to the COVID-19 pandemic, the federal government allowed for a 6.2% increase in Federal Medical Assistance Percentage (FMAP) contingent on states meeting the Maintenance of Effort (MOE) requirements. The MOE required states to halt any adverse action on Medicaid enrollments for the duration of the PHE to include any reduction or termination of coverage. Federally issued guidance during the PHE (42 CFR § 403(j)(3) and 42 CFR 457.320(3)(i)) does not allow the closure of individuals who resided in another state with the intent to return to the state in which residency was claimed. This guidance upholds DMAS' actions to refrain from closing coverage based on temporary absences. Data fields do not exist in the system to reflect these federal mandates and flexibilities.

This audit covers a period of time that falls during the PHE. Not taking the actions to reinstate coverage as required by the MOE would have put the Commonwealth at risk of losing the 6.2% enhanced FMAP which currently equals approximately \$300 million a quarter of federal funding for the Commonwealth.

DMAS took action to quickly make system and policy changes to bring the Commonwealth into compliance with federal requirements. As changes to the eligibility determination system require a lengthy and costly process, DMAS and DSS were unable to make what would be major system modifications in a timeframe that would allow the Commonwealth to meet the requirements of the MOE. Not knowing how long the federally declared PHE would end created an additional level of complexity in determining the amount of resources to allocate to major system updates that would be temporary. To ensure the Commonwealth met compliance with the MOE, DMAS put into place a system of checks and balances through reporting and reinstatement in the DMAS owned Medicaid Management Information System (MMIS), which is the enrollment system of record for Medicaid in Virginia.

DMAS monitored any closures made to ensure the MOE was being appropriately adhered to and ensure members were not inadvertently losing coverage during the emergency. DMAS found a high number of closures and reductions in enrollments by local agencies after multiple communications and information sessions. In order to prevent these actions and preserve the Commonwealth's eligibility for the enhanced FMAP, DMAS implemented an emergency change to the MMIS system. These changes automatically reinstated terminated or reduced coverage unless the cancellation reason met one of the three federally accepted reasons for closure.

After completing an internal review of the initial data compiled by the APA for this audit, DMAS was able to eliminate those enrollments where a 100% match occurred reflecting an allowable reason for a member to live outside of the Commonwealth. However, due to the intricacies of Medicaid eligibility and enrollment rules, which have been further complicated with flexibilities required during the PHE, a manual review is required to validate the remaining members. There are many complexities around Medicaid eligibility that cannot be quantified purely with a data run – especially during a PHE where many temporary flexibilities and requirements are in place that are outside of normal operations and system capabilities.

The General Assembly allocated \$10 million in American Rescue Plan Act (ARPA) funding to assist with the unwinding of the federal PHE and to rectify any issues as a result of the actions taken during the emergency. An additional \$5 million in ARPA funding has been included in the Governor's Introduced Budget. A portion of this funding has been earmarked to review and correct enrollment actions that were inappropriately taken, which will include instances where an individual may have permanently left the state with no intent to return. If such scenarios are found, DMAS will retroactively correct the enrollment and retract any inappropriate capitation payments made to the health plan resulting in the Commonwealth being made whole for any funds paid.

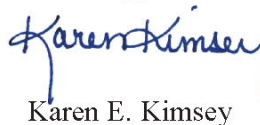
It is important to note the state of Virginia is still under a federal PHE and certain actions cannot be taken until the Federal Secretary of Health and Human Services declares an end to the

emergency. DMAS contends there are multiple items of consideration regarding this point that are dependent on the unprecedented actions required as part of the COVID-19 PHE to include the federally mandated requirements, the inability to accurately reflect incorrect enrollments through a data pull alone, and the fact that the Medicaid agency has not yet begun the work to unwind the processes put into place and take action to correct any issues occurring as a result of the MOE.

We 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 eligibility finding in partnership with VDSS as well as corrective action plans to address the other two findings.

If you have any questions or require additional information, please do not hesitate to contact the DMAS Internal Audit Director, Susan Smith.

Sincerely,

A handwritten signature in blue ink that reads "Karen Kimsey". The signature is stylized with a large, looped "K" and a trailing flourish.

Karen E. Kimsey



COMMONWEALTH of VIRGINIA

DEPARTMENT OF SOCIAL SERVICES

January 18, 2022

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

Dear Mrs. Henshaw:

The Virginia Department of Social Services concurs with the audit findings including in the 2021 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,

A handwritten signature in black ink, appearing to read "Necole Simmonds".

Necole Simmonds
Deputy Commissioner,
Employee & Organizational Strategy

APA COMMENT ON MEDICAL ASSISTANCE SERVICES' RESPONSE

Medical Assistance Services' response discusses that federal requirements did not allow cancellation of Medicaid coverage for individuals who temporarily relocated to another state during the PHE. We acknowledge this requirement; however, the individual cases and questioned costs cited in our finding entitled "Strengthen Process over Medicaid Coverage Cancellations" are related to individuals who appear to have permanently moved out of state and would potentially no longer be eligible for coverage based on federal requirements.

SECRETARY OF HEALTH AND HUMAN RESOURCES AGENCY OFFICIALS

As of June 30, 2021

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