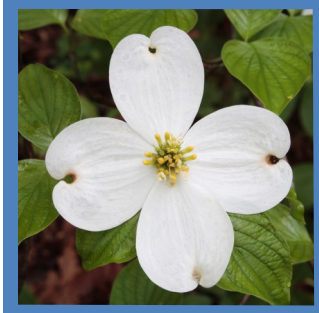


AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2022

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

AUDIT SUMMARY

This report summarizes our fiscal year 2022 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively, these four agencies spent $24.2 billion or 97 percent of the total expenses for agencies within 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, 2022, 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, after Health made adjustments to two attachments for material misstatements as noted in the "Audit Findings and Recommendations" section;

- 57 findings involving internal control and its operation necessary to bring to management's attention. Of these findings, we consider six to be material weaknesses;

- 50 of the 57 findings to be instances of noncompliance with applicable laws and regulations or other matters that are required to be reported, and;

- adequate corrective action with respect to eight audit findings reported in the prior year that we did not include 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). The Risk Alerts are applicable to DBHDS, Health, and Medical Assistance Services. In addition, our report includes one operational matter as a Comment to Management applicable to DBHDS.

-TABLE OF CONTENTS-

COMMENT TO MANAGEMENT

As we have reported previously, there is an operational matter that impacts DBHDS that we continue to highlight in our report given its impact on operations. While agency personnel are aware of this matter and are preparing to meet these challenges, we continue to communicate this issue to encourage continued progress by agency personnel and to ensure there is visibility into their efforts by senior-level management of the agency 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 DBHDS to serve individuals 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 settlement agreement, the Commonwealth was originally 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 mutually agreed with the DOJ to extend the settlement agreement, first to July 1, 2022, and more recently to December 31, 2023. The largest barrier to achieving full compliance is the need for reliable and valid data to support quality and risk management systems for community services. DBHDS continues to improve its existing processes and systems to ensure reliable and valid data is accessible to demonstrate compliance; however, additional improvements are necessary to achieve full compliance that is sustainable.

Over the past year, DBHDS continued to collaborate with all involved parties to prioritize remaining actions needed to exit the settlement agreement. DBHDS also resumed in-person contacts and other community engagements to comply with the settlement agreement. However, 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 to achieve and sustain compliance. 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 sustain 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.

AUDIT FINDINGS AND RECOMMENDATIONS

We have reported our audit findings and recommendations in two different sections below and organized them by agency within each section. The section titled "Internal Control and Compliance Findings and Recommendations" includes current year findings, as well as prior year findings where there the agency has taken limited to no corrective action. The section titled "Status of Prior Year Findings and Recommendations" includes an update on findings from prior years which an agency has not completely resolved, but where the agency has made progress in addressing the issue.

Each individual finding reported includes information on the type of finding, whether the finding is a repeat finding, and the severity classification for the finding, where applicable. The section titled "Independent Auditor's Report" includes more detail on the severity classifications, with a material weakness being the most severe classification. Chart 1 summarizes the total number of findings by agency for fiscal year 2022 including the number of new and repeat findings reported. Of these findings, there were six material weaknesses as follows: Social Services (3), Health (2) and Medical Assistance Services (1).

Summary of Findings by Agency

Chart 1

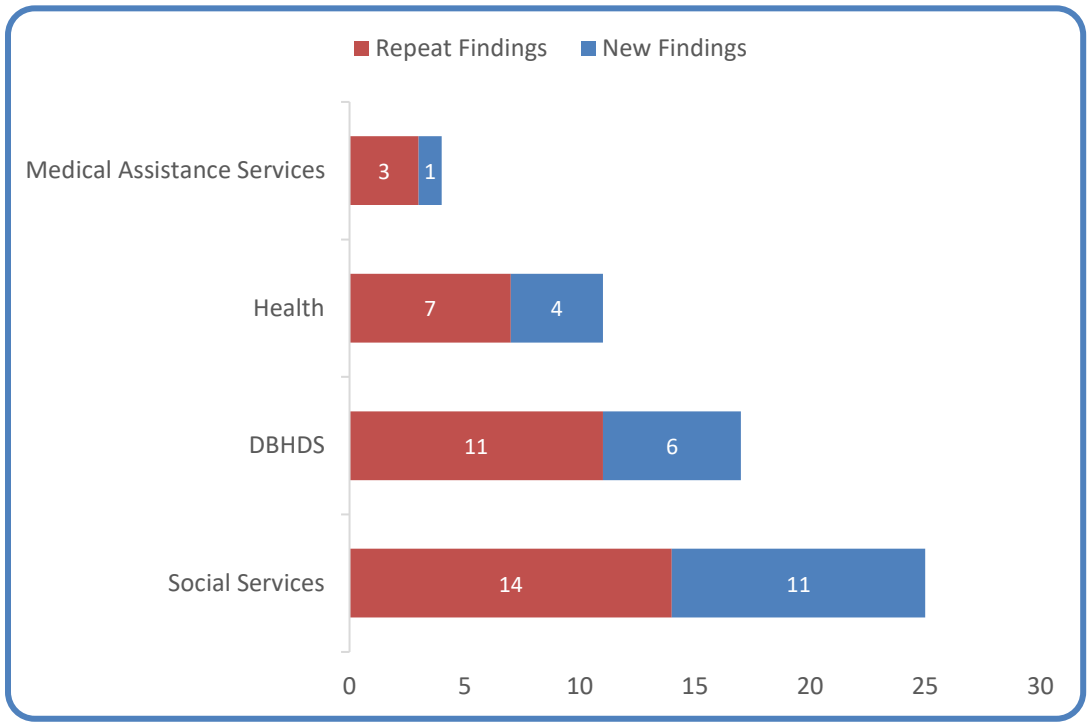
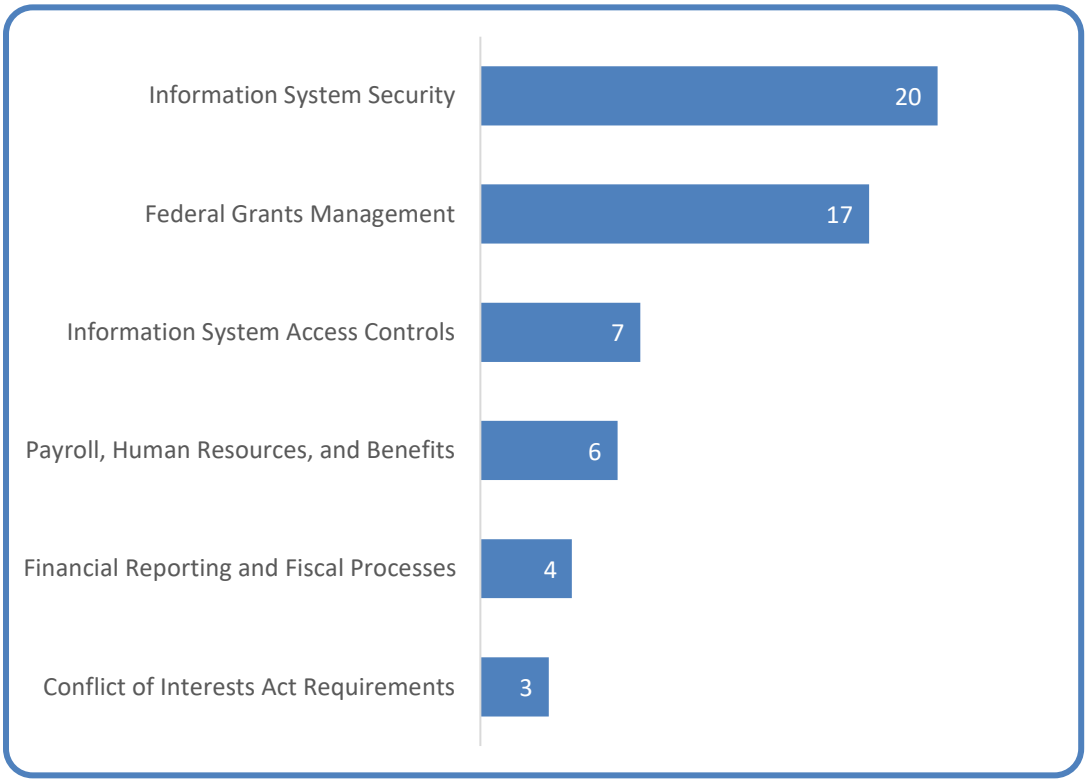


Chart 2 reports the total number of findings by internal control and/or compliance category for fiscal year 2022. As shown below, most findings related to one of two areas, information system security or federal grants management.

Number of Findings by Category

Chart 2



Internal Control and Compliance Findings and Recommendations

Establish a Change Management Process for Information Technology Environment

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS does not have a formal change management policy or process to manage changes affecting all components of its information technology (IT) environment. We communicated the specific weaknesses 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 Commonwealth's Information Security Standard, SEC 501 (Security Standard), requires DBHDS to develop, document, and disseminate a configuration management policy and procedures to facilitate the implementation of the configuration management policy and associated controls. Without a formal change management process, DBHDS cannot track, review, approve, and maintain a record of changes to its IT environment. As a result, DBHDS is at a higher risk for unauthorized changes to its production environment, which could negatively affect the confidentiality, integrity, and availability of its IT systems and data.

DBHDS did not have a formal and consistent change management process due to the Information Security and Information Technology offices operating in a decentralized manner across the Central Office and facilities. Since the current Chief Information Security Officer and Chief Information Officer arrived in 2020 and 2019, respectively, DBHDS has centralized its information security and technology operations, including its change management process. Staffing turnover and limited resources have delayed DBHDS from developing and implementing a formal change management process across its IT environment.

DBHDS should develop and document a formal change management process for all components of its IT environment that aligns with the requirements in the Security Standard. By implementing these controls for the change management process, DBHDS will reduce the risk of unauthorized changes in the environment and will help improve the confidentiality, integrity, and availability of mission-critical and sensitive systems.

Improve Vulnerability Management Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS does not consistently remediate vulnerabilities in its IT environment within the timeframe required in the DBHDS Vulnerability Management Program. 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.

Without remediating vulnerabilities within the required timeframe, DBHDS increases the risk of unauthorized access to the IT environment as well as an increase in likelihood of data breaches. In addition, software vulnerabilities, whether patching or configuration-based, are common flaws used by unauthorized actors to infiltrate a network and initiate an attack and can lead to financial, legal, and reputational damages for DBHDS.

DBHDS implemented the vulnerability management process during fiscal year 2022, and its process continues to mature. Additionally, ongoing resource constraints and other higher priorities, such as remediating prior year findings, caused DBHDS to fall behind in its vulnerability remediation efforts.

DBHDS should improve its vulnerability management process to ensure that it remediates vulnerabilities within the timeline required by the Vulnerability Management Program based on severity. By remediating vulnerabilities timely, DBHDS will reduce data security risk for sensitive and mission critical systems and better protect the confidentiality, integrity, and availability of the data processed by those systems.

Conduct Information Technology Security Audits over Sensitive Systems

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS is not performing timely IT security audits over its sensitive systems in accordance with the Commonwealth's IT Security Audit Standard, SEC 502 (IT Audit Standard). From fiscal years 2019 to 2021, DBHDS completed 16 comprehensive security audits. As of fiscal year 2022, DBHDS identified 140 sensitive systems, many of which do not have a record of receiving an IT security audit.

The IT Audit Standard, Section 1.4, requires IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, to receive an IT security audit at least once every three years. Additionally, the IT Audit Standard, Section 2.2, requires that the IT security auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measures compliance with the applicable Commonwealth IT Risk Management Policies and Standards.

Without conducting IT security audits over all sensitive systems at least once every three years, DBHDS may not detect and mitigate weaknesses affecting its IT environment. Additionally, malicious parties can exploit the unmitigated weaknesses to compromise DBHDS's sensitive systems.

DBHDS Internal Audit has experienced staff turnover since 2019, specifically with its Director of Internal Audit and one of its two IT security auditor positions. The Internal Audit Department currently only has one IT auditor and a new director. The limited staffing has hindered DBHDS from conducting the audits within the three-year requirement.

DBHDS should evaluate potential options to either outsource or hire additional IT auditors to ensure its sensitive systems receive an audit once every three years in accordance with the IT Audit

Standard. This will help to ensure the confidentiality, integrity, and availability of DBHDS's sensitive and mission-critical data.

Complete FFATA Reporting for First Tier SABG Subawards

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS Office of Fiscal and Grants Management (Fiscal and Grants Management) is not completing Federal Funding Accountability and Transparency Act (FFATA) reporting for Community Service Boards (CSB) who received funding from the Substance Abuse Block Grant (SABG) federal grant program. During state fiscal year 2022, DBHDS disbursed approximately $62.2 million in SABG funds to CSBs. This total represents approximately 92 percent of the SABG federal grant program's expenses for state fiscal year 2022.

Title 2 U.S. Code of Federal Regulations (CFR) Part 170 Appendix A requires the non-federal entity to report each obligating action, exceeding $30,000, to the FFATA Subaward Reporting System (FSRS). Fiscal and Grants Management identified the reporting requirements in its policies and procedures for FFATA reporting and completed FFATA reporting for its other subrecipients. However, Fiscal and Grants Management was unable to complete FFATA reporting for CSB's because of staffing shortages. Additionally, Fiscal and Grants Management did not have all the information it needed to complete FFATA reporting because it was still working with the DBHDS Office of Enterprise Management Services (Enterprise Management Services) to ensure the performance contracts with CSBs included all information necessary for FFATA reporting. Not reporting to FSRS could result in a citizen or federal official having a distorted view as to how DBHDS is obligating federal funds from the SABG federal grant program.

Fiscal and Grants Management should dedicate the necessary resources to fulfil its FFATA reporting responsibilities for the SABG federal grant program. Additionally, Fiscal and Grants Management should continue to work with Enterprise Management Services to ensure the performance contracts with CSBs include all required information necessary for FFATA reporting. Finally, Fiscal and Grants Management should evaluate whether it is fulfilling its FFATA reporting responsibilities for DBHDS's other federal grant programs.

Continue to Improve Off-Boarding Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)
Prior Title: Improve Implementation of Off-Boarding Procedures

DBHDS is not properly terminating employees and retaining appropriate documentation to support the completion of off-boarding procedures. Our review of terminated employees included reviewing off-boarding processes at three facilities and Central Office and reviewing system access removals for the entire agency. During fiscal year 2022, Central Office provided all facilities with updated

off-boarding guidance and a termination checklist, which facilities were to incorporate into existing procedures to ensure consistency and proper off-boarding across the agency. When reviewing off-boarding processes, we identified that one facility had not implemented off-boarding procedures nor were they using a termination checklist. During our review, we specifically identified the following deficiencies:

- For all 16 terminated employees tested at one of the DBHDS facilities under review, the facility was unable to provide documentation supporting proper termination and did not have a process to ensure removal of building access and collection of Commonwealth property, such as keys and electronics.

- For five of 19 (26%) terminated employees tested at two DBHDS facilities, the facilities did not remove building access until more than a week after termination.

- Four facilities did not timely remove access to the internal time and leave reporting system for four of 15 (27%) terminated users tested. Access removal for these users ranged from 39 to 236 days after separation or transfer, with the average access removal for the 15 users occurring 38 days after separation or transfer.

- Five facilities did not timely request removal of system access to the internal patient revenue system for six of ten (60%) terminated users tested. Access removal for these users ranged from six to 118 days after separation, with the average access removal for the ten users tested occurring 31 days after 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 remove access to the Commonwealth's retirement benefits system for seven of eight (88%) terminated users at three facilities and Central Office.

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. 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 a high volume of turnover during the period under review. The volume of turnover was a contributing factor to these issues as well as other factors such as, a lack of communication, lack of oversight, competing priorities, and insufficient implementation of policies and procedures. Without proper 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 of unauthorized access to state and internal systems and sensitive information. The decentralization of the agency and secure environment in which facilities operate further increases its exposure to risk.

DBHDS should continue to improve off-boarding policies and procedures across its facilities. These policies and procedures should at a minimum include: the collection of Commonwealth property, timely removal of building access for terminated employees, and timely removal of all information system access in accordance with the CAPP Manual and Security Standard. DBHDS Central Office and management across all facilities should ensure proper implementation and adherence with off-boarding policies and procedures to include retention of supporting documentation and sufficient communication between responsible departments.

Improve Controls over Capital Outlay Voucher Processing
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS should improve controls over the processing of capital outlay invoices. The Architectural and Engineering, Budget and Financial Reporting, and Fiscal offices within DBHDS Central Office are responsible for processing capital outlay invoices for the entire agency. Architectural and Engineering is responsible for the initial receipt and approval of invoices prior to forwarding to Budget and Financial Reporting for approval before Fiscal can process for payment. During fiscal year 2022, the previously referenced offices began assessing and improving controls over the processing of capital outlay invoices, which included implementation of updated policies and procedures.

Our review of 30 capital outlay vouchers processed by DBHDS during fiscal year 2022 found a lack of documentation to support invoice receipt dates, inaccurate recording of the goods and service receipt date, and noncompliance with the prompt payment provisions of the Code of Virginia. Specifically:

- Architectural and Engineering did not have a consistent process for tracking invoice receipt dates and was unable to provide documentation to support the invoice receipt date for ten of 30 (33%) invoices.

- Fiscal inaccurately recorded the goods and service receipt date in the Commonwealth's accounting and financial reporting system for 21 of 30 (70%) vouchers. Fiscal identified and corrected this error during fiscal year 2022 prior to our review.

- Sixteen of 25 invoices (64%) were not in compliance with the prompt payment provisions of the Code of Virginia. The remaining five invoices tested were not subject to the prompt payment provisions.

As outlined in § 2.2-4347 of the Code of Virginia, every state agency that acquires goods or services or conducts any other type of contractual business with nongovernmental, privately-owned enterprises shall promptly pay for the delivered goods and services within 30 days of the receipt of a proper invoice or receipt of the goods and services, whichever is later. As DBHDS did not have a consistent process for tracking invoice receipt dates and was inaccurately recording the goods and service receipt date, there is an increased risk of miscalculated payment due dates, which can contribute to noncompliance with the prompt payment provisions of the Code of Virginia. Additionally, inaccurate

recording of the goods and service receipt date can lead to improper recognition of year-end payables and accruals reported in the Commonwealth's financial statements.

Improper management and oversight of the process for receiving invoices within Architectural and Engineering led to untimely invoice processing and noncompliance with the Code of Virginia. Additional factors, such as a lack of training and miscommunication caused the lack of documentation to support invoice receipt dates and inaccurate recording of the goods and services receipt dates. DBHDS should continue to improve controls over the processing of capital outlay invoices, including increased oversight over the process and additional training, to ensure accurate recording of invoice receipt dates and goods and services receipt dates and ensure compliance with the prompt payment provisions in the Code of Virginia.

Continue to Improve Controls over the Retirement Benefits System Reconciliation
Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)

DBHDS Central Office and individual facilities did not adequately perform and document reconciliations between the Commonwealth's human resource and retirement benefits systems during fiscal year 2022. Individual facilities have taken corrective actions since the prior audits to improve controls over the retirement benefits system reconciliation. However, we noted the following deficiencies during our review of Central Office and three facilities:

- Central Office did not perform a reconciliation of creditable compensation between the Commonwealth's human resource and retirement benefits systems prior to confirming the monthly contribution.

- For one of two months tested (50%), one facility did not retain documentation to support its review of the Commonwealth's human resource system cancelled records report.

- One facility did not address exceptions identified on the automated reconciliation reports.

- Two facilities did not confirm the monthly contribution snapshot within the required timeframe for four of 24 months (17%).

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. CAPP Manual Topic 50410 also describes each of the automated reconciliation reports and the actions agencies should take to promptly clear exceptions on the reports. Additionally, CAPP Manual Topic 50410 requires agencies to confirm retirement contributions by the 10th of the following month. The Payroll Service Bureau (Bureau) processes payroll for Central Office. The Bureau's Scope of Services agreement with Central Office specifically states that Central Office is responsible for reconciling credible compensation prior to confirming the monthly contribution,

reviewing the Commonwealth's human resource system cancelled records report, and actively resolving discrepancies identified during the reconciliation process.

Central Office Payroll and Human Resources departments did not properly perform the reconciliation process as they lacked an adequate understanding of responsibilities. The issues identified at the facilities were a result of a misunderstanding of documentation retention and report review requirements. The untimely confirmations of monthly contributions occurred due to miscommunications between the Payroll and Human Resources departments. Improper reconciliation processes can affect the integrity and accuracy of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire Commonwealth.

Management at Central Office and all DBHDS facilities should ensure that staff adequately perform and document monthly reconciliations of the Commonwealth's retirements benefits system. DBHDS should retain documentation to support their review of the Commonwealth's human resource system cancelled records report. The Payroll and Human Resources departments should communicate during the reconciliation process and provide adequate training to staff to ensure that they know how to properly perform the reconciliation process. Further, when improving controls over the reconciliation of the retirement benefits system, DBHDS should consider the changes in controls that will result from the implementation of the Commonwealth's new human resource and payroll management system, which occurred in fiscal year 2023.

Improve Management of Access to the Retirement Benefits System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Individual DBHDS facilities are not properly managing access to the Commonwealth's retirement benefits system to ensure separation of duties and least privilege access. Seven of 28 (25%) active users across three facilities tested had access to roles that present least privilege and separation of duties issues. These instances allow an individual user to both create and approve transactions or payments.

The Security Standard, Sections AC-5 and AC-6, requires organizations to separate duties of individuals and employ the principle of least privilege as appropriate when granting access. The Virginia Retirement System (VRS) Employer Manual speaks to the role-based security functionality of the retirement benefits system, which allows employers to manage access to the system based on the work an employee performs. When least privilege and separation of duties issues exist, there is an increased risk that users will perform unauthorized transactions, which can compromise data integrity and result in unnecessary exposure to sensitive data. As the VRS actuary uses retirement benefits system data to calculate the Commonwealth's pension liability, inaccurate data due to inappropriate access could result in a misstatement in the Commonwealth's financial statements.

The primary factors that contributed to these issues were an inadequate understanding of role functionalities and a lack of management oversight. Management at the individual facilities should gain an understanding of role functionalities and ensure there is proper oversight and consideration given to

separation of duties and least privilege principles when managing access to the Commonwealth's retirement benefits system. DBHDS should adhere to the Security Standard requirements and VRS guidance when granting access to the retirement benefits system.

Properly Prepare the Schedule of Expenditures of Federal Awards
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

The Office of Financial Management (OFM) did not properly report federal grant expenses in its Attachment 15 - Federal Schedules (Federal Attachment) submitted to the Department of Accounts (Accounts). OFM re-submitted the Federal Attachment to Accounts six different times to address various errors. The initial Federal Attachment omitted $90.4 million of expenses for the Immunization Cooperative Agreements federal program and $149.7 million of Coronavirus State and Local Fiscal Recovery pass-through funds received from the Department of Treasury. Additionally, OFM overstated the Disaster Grants – Public Assistance federal program expenses by approximately $64.0 million because OFM recognized the use of state funding as federal expenses prior to the receipt of federal funding.

Federal regulations known as Uniform Guidance, specifically 2 CFR § 200.510(b), require the Commonwealth to prepare a Schedule of Expenditures of Federal Awards (SEFA). Furthermore, the Single Audit Act, 31 USC Chapter 75 § 7502(h), and Uniform Guidance, 2 CFR § 200.512, require the Commonwealth to submit the SEFA to the federal government. To facilitate the Commonwealth complying with these requirements, Accounts requires state entities with federal funding to complete and submit federal attachments. Accounts compiles the federal attachments and submits the required information to the federal government on behalf of the Commonwealth. Unlike financial statements, the Commonwealth prepares its SEFA using the cash basis of accounting. As a result, the Commonwealth does not report federal expenses on the SEFA until it receives and uses federal funding. To ensure the accuracy of this information, the Comptroller's annual directive requires agencies to ensure controls are in place to avoid material misstatements and/or misclassifications in the federal attachments and other financial information agencies submit to Accounts.

Incorrectly reporting federal information to Accounts may cause the Commonwealth not to comply with the Single Audit Act and Uniform Guidance, which could jeopardize future federal funding. While Accounts corrected the information based on OFM's resubmissions before it submitted the SEFA to the federal government, the misstatements and/or misclassifications required the use of additional resources to detect and correct the errors, which limited the amount of time available to Accounts to complete required tasks before the related federal deadlines.

Several different factors contributed to these errors. OFM has experienced a significant amount of turnover in key positions and hired new staff during the audit period for positions that were historically responsible for completing and submitting the Federal Attachment. Health did not have policies and procedures for preparing the Federal Attachment for the new employees hired into these key roles to use as a resource. In addition, Health has been under stress with the COVID-19 pandemic and its role in statewide health policy, and OFM did not prioritize properly training new employees.

OFM should improve the process for preparing, reviewing, and submitting the Federal Attachment to Accounts including developing adequate policies and procedures so that newly hired

employees have a resource for preparing and submitting financial information. Additionally, OFM should prioritize training new employees in key positions to improve the quality of financial information staff report to Accounts.

Improve Controls over Journal Entries
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

OFM has multiple internal control weaknesses related to journal entry processing. OFM did not retain adequate supporting documentation for two of 25 (8%) journal entries reviewed. In addition, there was no evidence of supervisory approval for three of 25 (12%) journal entries. Lastly, OFM staff were unable to provide an explanation over their tracking process for certain COVID-19 pandemic expenses that staff initially paid with general funds and later moved to federal funds through journal entries.

OFM uses journal entries to record transactions that occur throughout the year as well as to correct and adjust previously recorded entries in the Commonwealth's accounting and financial reporting system. CAPP Manual Topic 20905 states agency management is responsible for instituting internal control over the recording of financial transactions that is designed to provide reasonable assurance regarding the reliability of those records. Reliability of financial records means that management can reasonably make several assertions as to the completeness and accuracy of the financial records. Uniform Guidance, specifically 2 CFR § 200.303(a), requires that Health establish and maintain effective internal control over the federal award that provides reasonable assurance that Health is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Without adequate supporting documentation for journal entries, OFM increases the risk of recording inaccurate information in the accounting records. The lack of adequate supporting documentation could also create questions as to whether the nature of the journal entry is permissible. OFM has experienced a significant amount of turnover in key positions and hired new staff during the audit period for positions that were historically responsible for preparing and reviewing journal entries. In addition, Health has been under stress with the COVID-19 pandemic and its role in statewide health policy and OFM did not prioritize properly training new employees. In response to staffing shortages, Health contracted with a consultant to help OFM monitor and track COVID-19 pandemic related expenses. However, OFM did not document policies and procedures related to the monitoring and tracking of these expenses and staff who oversaw this process no longer work at the agency and were not available to provide an explanation of the process.

OFM should improve internal controls over journal entries to ensure that it retains adequate supporting documentation, including evidence of supervisory approval. Additionally, OFM should ensure it documents policies and procedures over key processes, such as monitoring COVID-19 pandemic-related expenditures. Health should also prioritize training new employees in key positions on preparing and reviewing journal entries.

Strengthen Controls over Overtime Payments
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Health did not pay employees timely for overtime related to the COVID-19 pandemic and, as a result, had to make retroactive payments to employees in fiscal year 2022. Over the last several years, Health employees have worked a significant amount of overtime given their statewide responsibilities related to the COVID-19 pandemic. During the year, Health paid over 1,600 employees for COVID-19 pandemic-related overtime; however, for over half of these employees, Health made lump sum payments because the overtime worked dated back several months or years. These lump sum payments ranged from 30 days to almost two years after the employee earned the overtime. In addition, as of November 2022, there are 169 employees with COVID-19 pandemic-related overtime hours that Health has not paid because it needs additional information on the hours worked.

In response to the public health emergency declaration, Health permitted employees to work overtime beginning in March 2020. To address this need, Health implemented guidelines which required employees to submit an HDP-43 Disaster Labor Record (HDP-43) form to track their overtime related to the COVID-19 pandemic; however, these guidelines did not establish time requirements for employees to submit their overtime hours worked or for managers to approve the time. There was also some confusion as the COVID-19 pandemic evolved as to which staff were eligible for overtime, and Health's guidelines did not clearly address who was eligible for overtime.

The Federal Government provided funding for COVID-19 pandemic-related overtime costs; however, this funding expired at the end of calendar year 2021. In an effort to process overtime costs using the available funds, Health required supervisors to approve and submit all COVID-19 pandemic overtime hours by November 15, 2021. This communication resulted in many employees submitting information related to overtime hours worked in prior months and years and led to lump sum payments.

By not establishing a timeframe for submission or approval of COVID-19 pandemic overtime hours worked, Health processed overtime payments untimely and also increased the risk of employees inaccurately reporting hours worked given the significant reporting delays. Also, Health currently has employees it has not paid for COVID-19 pandemic overtime hours due to issues identified on the employees' HDP-43 forms. The federal funds available to pay this overtime have expired, so Health will have to identify and use other funding sources to pay employees if it determines the overtime hours are valid.

Health should ensure it has adequate policies and procedures in place to pay employees timely, including in emergency situations. As a best practice, agency policies and procedures should be specific and establish a timeframe for submission and approval of information to ensure timely processing. Health should also clearly communicate policies and procedures to staff and supervisors and ensure they adhere to the policies and procedures. Additionally, in emergency situations, Health should regularly update policies and procedures to ensure adequate internal controls are in place.

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Health does not have certain minimum Security Standard controls in place for a sensitive system's database. We communicated the control 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 the implementation of 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 and aligning the database's settings and configurations with best practices, Health cannot ensure the confidentiality, integrity, and availability of data within the database or the information it reports.

Health should implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Improve Third-Party Oversight Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Medical Assistance Services does not have a formal and consistent process for maintaining oversight for three of its IT third-party service providers (providers) that manage and support the Medicaid management system. As a result of an informal and inconsistent process, Medical Assistance Services did not verify or implement three controls required by the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard). We communicated the three 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.

Without a formal and consistent process to maintain oversight of its providers, Medical Assistance Services cannot validate whether its providers implement the security controls that meet the requirements in the Hosted Environment Security Standard to protect the agency's sensitive and mission-critical data. While Medical Assistance Services has a formal IT Third Party and Vendor Compliance Management Policy, effective as of December 31, 2021, the agency experienced turnover in its Information Security Officer (ISO) position in June 2022 before the development of a formal procedure. As a result, Medical Assistance Services did not consistently maintain oversight of its providers in accordance with the Hosted Environment Security Standard.

Medical Assistance Services should dedicate the necessary resources to develop a formal procedure to maintain oversight of its providers in accordance with its policy and the Hosted Environment Security Standard. Medical Assistance Services should also dedicate the necessary resources to implement and consistently perform the formal oversight process, which will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

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

Social Services has an insufficient governance structure to manage and maintain its information security program in accordance with the Security Standard. Specifically, Social Services does not assess information security requirements for its IT projects and prioritize information security and IT resources to ensure its information security program effectively protects sensitive Commonwealth data in accordance with the Security Standard. Social Services uses numerous IT systems to carry out its mission and provide essential services to the public.

The Security Standard, Section 2.4.2, requires the agency head to maintain an information security program that is sufficient to protect the agency's IT systems and to ensure the information security program is documented and effectively communicated. We communicated the internal control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

The internal control weaknesses described in the communication marked FOIAE are the result of Social Services not assessing information security requirements prior to project implementation or prioritizing information security within the IT environment. Not prioritizing IT resources to properly manage its information security program can result in a data breach or unauthorized access to confidential and mission critical data, leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external. Additionally, not dedicating the necessary IT resources to information security has hindered Social Services' ability to remediate findings from management recommendations issued throughout prior audits consistently and timely and bring the information security program in compliance with the Security Standard. Because of the scope of this matter, we consider it to be a material weakness in internal control.

Social Services should evaluate the most efficient and effective method to bring its IT and security program into compliance with the Security Standard. Social Services should also evaluate its IT resource levels to ensure sufficient resources are available and dedicated to prioritizing and implementing IT governance changes and address the internal control deficiencies discussed in the communication marked FOIAE. Implementing these recommendations will help to ensure Social Services protects the confidentiality, integrity, and availability of its sensitive and mission critical data.

Perform Responsibilities Outlined in the Agency Monitoring Plan
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Ensure Appropriate Oversight over Divisions' Monitoring Activities

Social Services' Compliance Division (Compliance) continues to not adhere to its established approach to oversee the agency's subrecipient monitoring activities, as outlined in its Agency Monitoring Plan. During fiscal year 2022, Social Services disbursed approximately $588 million in federal funds from roughly 5,000 subawards. According to Social Services' Organizational Structure Report, Compliance is responsible for agency-wide compliance and risk mitigation that helps to ensure adherence to state and federal legal and regulatory standards, including subrecipient monitoring. During the audit, we noted the following deviations from the Agency Monitoring Plan:

- Compliance has not finalized the Agency Monitoring Plan and, as a result, has not communicated it to Subrecipient Monitoring Coordinators within each division of Social Services. Because of the lack of communication, there were deviations from the Agency Monitoring Plan at the division level. For example, the Agency Monitoring Plan requires each division to monitor subrecipients once every three years. However, the Local Review Team and Child Care Subsidy Program Monitoring Plans did not consider this requirement because the Subrecipient Monitoring Coordinators were unaware of this requirement. We communicated this matter to Social Services through the audit finding titled "Finalize the Agency Monitoring Plan and Communicate Responsibilities to Subrecipient Monitoring Coordinators," which we have included as a separate audit finding in this report.

- Compliance continues to not review division monitoring plans to ensure the divisions implemented a risk-based approach for monitoring subrecipients. The Agency Monitoring Plan states that Compliance will use a monitoring plan checklist to evaluate and determine if all the required elements for subrecipient monitoring are present in each division's plan. As a result of the lack of review, the Division of Benefit Programs' (Benefit Programs) monitoring plan continues to not meet all the requirements outlined in the Agency Monitoring Plan because it does not include a risk-based approach for subrecipient monitoring and does not consider all subrecipients who receive funding from the Temporary Assistance for Needy Families (TANF) federal grant program. We communicated these matters to Social Services through the audit findings titled "Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities" and "Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations," which we have included as separate audit findings in this report.

- Compliance continues to not conduct an analysis of subrecipient monitoring review efforts performed by the divisions. As a result, Compliance has not produced quarterly reports of variances and noncompliance to brief Social Services' Executive Team on the agency's subrecipient monitoring activities. Because of the lack of analysis, Compliance was unaware of deviations from the Agency Monitoring Plan occurring at the divisions. For example,

Benefit Programs only completed 25 of the 67 (37%) scheduled reviews for the Low-Income Home Energy Assistance Program (LIHEAP) federal grant program. Additionally, Benefit Programs did not upload its monitoring review records to Social Services' data repository timely for management review. As a result, Compliance was unaware that Regional Consultants were deviating from Benefit Programs' monitoring plan. We communicated this matter to Social Services through the audit finding titled "Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan," which we have included as a separate audit finding in this report.

Without performing the responsibilities in the Agency Monitoring Plan, Compliance cannot provide Social Services' Executive Team with reasonable assurance that the agency complied with the pass-through entity federal requirements at 2 CFR § 200.332. Title 2 CFR § 200.303(a) requires pass through entities to establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award. Compliance planned to procure a centralized system to strengthen its monitoring activities but has been unsuccessful in its efforts and has not identified alternative approaches for carrying out the responsibilities in the Agency Monitoring Plan and discussed them with Social Services' Executive Team. Because of the scope of this matter, we consider it to be a material weakness in internal control.

Social Services' Executive Team shapes strategies, develops objectives, and collectively resolves issues that are critical to the overall agency performance. Social Services' Executive Team and Compliance should work collaboratively to determine the best approach for carrying out the responsibilities in the Agency Monitoring Plan. Additionally, Social Services' Executive Team and Compliance should hold quarterly meetings to discuss the Agency Monitoring Plan and its activities.

Implement Internal Controls over TANF Federal Performance Reporting
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Benefit Programs does not have adequate internal controls in place to ensure accurate reporting for the Administration for Children and Families (ACF) 199 TANF Data Report (ACF-199) and 209 Separate State Programs-Maintenance-of-Effort (SSP-MOE) Data Report (ACF-209). Social Services submits these reports quarterly and creates them using a fully automated process that extracts data from Social Services' case management system. ACF uses the information in these reports to determine whether the Commonwealth met the minimum work participation requirements for the TANF federal grant program.

Benefit Programs uses a third-party service provider (service provider) to produce the ACF-199 and ACF-209 reports and relies solely on the service provider's internal controls during the data extraction and data reporting process. During our review, we identified the following instances where

the service provider did not report key line information accurately based on the information maintained in Social Services' case management system or the supporting data:

- Ten out of 50 (20%) cases included in the "Receives Subsidized Child Care" key line, four out of 50 (8%) cases included in the "Unsubsidized Employment" key line item, and two out of 50 (4%) cases included in the "Work Participation Status" key line item did not agree to Social Services' case management system.

- Three out of three (100%) of the "Total Number of TANF Families" key line item and three out of three (100%) of the "Total Number of SSP-MOE Families" key line items did not agree to the supporting data.

Title 45 CFR § 265.7(b) requires states to have complete and accurate reports, which means that the reported data accurately reflects information available in case records, are free of computational errors, and are internally consistent. Reporting potentially inaccurate or incomplete information prevents the ACF from adequately monitoring Social Services' work participation rates and the overall performance for the TANF program. In addition, ACF can impose a penalty if it finds Social Services to not be meeting statutory required work participation rates.

Benefit Programs has not developed its own policies and procedures to identify how it obtains assurance over the accuracy of the data included within the submissions. Benefit Programs also relies on the error correction controls of the ACF, performed after report submission, with no secondary review or data validation processes performed within the agency prior to report submission to determine whether the TANF work participation information reported is accurate. Because of the scope of this matter, we consider it to be a material weakness in internal control.

Benefit Programs should implement policies and procedures over the TANF performance reporting process and include a documented secondary review process. Benefit Programs should confirm completion of this review prior to the report submission to ensure accurate reporting of TANF work participation information to ACF in accordance with the ACF-199 and ACF-209 reporting instructions.

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

Social Services continues to not configure a sensitive web application in accordance with the Security Standard. Since the prior audit, Social Services has not remediated any of the previously identified weaknesses. 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 implementing certain internal controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data. Social Services cannot ensure adequate protection of its sensitive and mission-critical data without configuring its sensitive web application in accordance with the Security Standard. Lacking or insufficient procedures and processes to manage the web application contributed to the five weaknesses outlined in the separate FOIAE document. Social Services prioritization of other projects also contributed to the weaknesses persisting.

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

Upgrade End-of-Life Technology

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Social Services uses end-of-life (EOL) technologies in its IT environment and maintains technologies that support mission-essential data on IT systems that its vendors no longer support. We communicated internal control 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 prohibits using software that is end-of-life and which the vendor no longer supports to reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data.

Social Services does not assign an individual or team with the responsibility to track EOL software dates and does not have a formal process to ensure that it upgrades software versions prior to the EOL date, which caused the EOL software to remain in the environment. Social Services use of the EOL software increases the risk that known vulnerabilities will persist in the system without the potential for patching or mitigation. These unpatched vulnerabilities increase the risk of successful cyberattack, exploit, and data breach by malicious parties. Further, vendors do not offer operational and technical support for EOL or end-of-support technology, which affects data availability by increasing the difficulty of restoring system functionality if a technical failure occurs.

Social Services should dedicate the necessary resources to evaluate and implement the internal controls and recommendations discussed in the communication marked FOIAE in accordance with the Security Standard. Minimizing the use of EOL software will help to ensure that Social Services secures its IT environment and systems to protect its sensitive and mission-critical data.

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

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Review and Document Service Organization Control Reports of Third-Party Service Providers

Social Services continues to not have sufficient internal controls for obtaining, reviewing, and documenting System and Organization Control (SOC) reports of service providers. Social Services uses service providers to perform functions such as administering the Electronic Benefit Transfer (EBT) process for public assistance programs, processing public assistance program applications, and performing call center functions. SOC reports, specifically SOC 1, Type 2 reports, provide an independent description and evaluation of the operating effectiveness of a service provider's internal controls over financial processes and are a key tool in gaining an understanding of a service provider's internal control environment and maintaining oversight over outsourced operations. Social Services could not demonstrate that it reviewed service provider SOC reports to identify deficiencies or determined whether the reports provided adequate coverage over operations during the fiscal year.

CAPP Manual Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the service provider's internal control environment. Agencies must also maintain oversight over service providers 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 information technology equipment, systems, and services procured from service providers, and that agencies must enforce the compliance requirements through documented agreements and oversight of the services provided. Finally, 2 CFR § 200.303(a) requires non-federal entities to establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Social Services shares responsibilities for reviewing SOC reports with VITA's Enterprise Cloud Oversight Services (ECOS), based on the type of SOC report. The individuals responsible for obtaining and reviewing SOC 1, Type 2 reports misunderstood the services provided by ECOS, as ECOS does not review SOC 1, Type 2 reports, and did not have clear expectations as to what they should obtain, review, and document during their review of SOC 1, Type 2 reports. As a result, Social Services did not develop policies and procedures related to obtaining, reviewing, and documenting SOC 1, Type 2 reports in relation to our recommendation in the prior audit.

Without adequate policies and procedures over service providers' operations, Social Services is unable to ensure its complementary controls are sufficient to support its reliance on the service providers' control design, implementation, and operating effectiveness. Additionally, Social Services is unable to address any internal control deficiencies and/or exceptions identified in the SOC reports. In effect, Social Services is increasing the risk that it will not detect a weakness in a service provider's

environment by not obtaining the necessary SOC reports timely or properly documenting the review of the reports.

Social Services should develop agency-wide policies and procedures that other divisions can use when obtaining, reviewing, and documenting SOC reports. Policies and procedures should comply with the requirements outlined in the CAPP Manual and Security Standard. These policies and procedures should include, at a minimum, the timeframes for obtaining SOC reports from the service provider, documentation requirements for user entity complementary controls, the steps needed to address internal control deficiencies and/or exceptions found in reviews, and the responsible staff for any corrective actions necessary to mitigate the risk to the Commonwealth until the service provider corrects the deficiency.

Monitor Internal Controls to Ensure Timely Removal of System Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Titles: Improve Timely Removal of System Access; Continue to Improve Access Controls over Child Care System

Social Services did not comply with the Security Standard requirements for removing system access for separated employees. For 13 of the 26 (50%) separations tested from fiscal year 2022, Social Services did not remove system access within 24 hours following each employee's separation date. Untimely removal of access ranged between two and 290 days after each employee's separation date.

Section PS-4 of the Security Standard requires an organization to disable information system access within 24 hours of employment termination. To comply with the Security Standard, Social Services created a policy in Section 2.9 of its State/Local Security Officers Procedures Manual (Manual) that requires supervisors to complete the State Employee Separation and Transfer Checklist (Separation Checklist) at least 48 hours in advance of the employee's separation and submit it to the Division Security Officer. The Division Security Officer must then remove the separated employee from Social Services' access management system, which controls access to its internal systems, within 24 hours following the employee's separation date. Upon completion, the Division Security Officer is responsible for submitting the Separation Checklist to other Divisions, such as the Division of Human Resources (Human Resources) and the Central Security Office (Central Security), to make them aware of the separation.

Social Services does not appear to monitor compliance with internal policies surrounding access removal for separated employees. Of the 13 employees with access removed more than 24 hours after their separation dates:

- We noted four instances where Social Services was unable to provide the Separation Checklist. As a result, Social Services was unable to demonstrate compliance with its internal policies surrounding access removal for separated employees.

- Of the remaining nine employees with completed Separation Checklists, we noted nine instances of untimely or inaccurate supervisor sign-offs. Specifically, there were seven instances where the supervisor did not submit the Separation Checklist to the Division Security Officer at least 48 hours in advance of the employee's date of separation and two instances where the supervisor did not properly sign off and date the Separation Checklist.

Social Services administers numerous public assistance programs that collect personally identifiable information and other protected information from beneficiaries. Social Services places its data and reputation at risk by not removing access timely. Additionally, Social Services could incur a potential financial liability should its information become compromised.

The Security Standard states that the Agency Head is responsible for security of the agency's IT systems and data. Since Human Resources, Central Security, and the Division Security Officers share ownership of the employee separation and access removal processes, Social Services' Executive Team should identify which division in the agency should be responsible for monitoring compliance with internal policies surrounding access removal for separated employees. Social Services' Executive Team should periodically review the monitoring results and take enforcement actions, as necessary, if the agency is not compliant.

Improve Documentation for Separation of Duty Conflicts

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Social Services' Division of Finance (Finance) lacks written documentation for users to justify and authorize conflicting access to its financial accounting and reporting system (financial system). The review of 20 financial system users with access to critical roles identified 14 users (70%) with access to conflicting roles based on Finance's system access policy. While Finance was able to verbally explain the conflicting access and noted that there are compensating controls, it did not maintain documentation explaining the need for certain financial system users to have access to conflicting roles, the compensating controls in place to mitigate separation of duties risks, and management's approval of the conflicting access granted.

Section 8.1 AC-6 of the Security Standard requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks. Additionally, Section 8.1 AC-5 of the Security Standard requires the agency to separate duties of individuals as necessary, document separation of duties of individuals, and define information system access authorization to support the separation of duties.

While Finance has documented which roles in its financial system pose a separation of duties concern, Finance has not updated its policy to require Finance personnel to create written documentation to justify and authorize access to the conflicting roles in the financial system when separation of duty concerns exist. When improper separation of duties exists, there is an increased risk

that users can perform unauthorized transactions in the financial system. Approved documentation of the separation of duties concerns and compensating controls in place provides accountability and assurance that Finance is taking proper consideration of the risks of granting such access to the financial system.

Finance should update its system access policy to require written documentation for users to justify and authorize conflicting access to its financial system. Additionally, Finance should continue to perform reviews of user access to ensure it grants access based on the principle of least privilege and ensure proper separation of duties. If violating the principle of least privilege and causing separation of duties issues is unavoidable, then Finance should document the users with roles that cause separation of duties issues, document the compensating controls in place to mitigate risk, and obtain management approval to achieve compliance with the Security Standard.

Finalize the Agency Monitoring Plan and Communicate Responsibilities to Subrecipient Monitoring Coordinators

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020)
Prior Title: Continue to Communicate Subrecipient Monitoring Responsibilities to the Coordinators

Compliance has not finalized its Agency Monitoring Plan and communicated responsibilities to Subrecipient Monitoring Coordinators, as recommended during the fiscal year 2020 audit. The oversight of Social Services' subrecipient monitoring processes transitioned from the Division of Community and Volunteer Services (Community and Volunteer Services) to Compliance in fiscal year 2019. Community and Volunteer Services created the Agency Monitoring Plan, and it is now the responsibility of Compliance. However, Compliance has not updated the Agency Monitoring Plan to properly reflect agency operations over subrecipient monitoring. In effect, Compliance continues to not communicate the Agency Monitoring Plan to Subrecipient Monitoring Coordinators within each division of Social Services. During fiscal year 2022, Social Services disbursed approximately $588 million in federal funds from roughly 5,000 subawards.

Title 2 CFR § 200.332(d) requires pass-through entities to monitor the activities of subrecipients as necessary to ensure use of the subaward for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Without clearly defining responsibilities and communicating federal requirements, Compliance cannot provide assurance that Social Services adequately monitors all its subrecipients to ensure they are achieving program objectives or complying with federal requirements. Compliance was unable to finalize the monitoring plan and communicate responsibilities to monitoring coordinators because it did not dedicate the resources necessary to implement corrective action.

Compliance should allocate resources to finalize the Agency Monitoring Plan to properly address subrecipient monitoring responsibilities. Additionally, Compliance should communicate the Agency Monitoring Plan to Subrecipient Monitoring Coordinators within each division of Social Services.

Review Non-Locality Subrecipient Single Audit Reports
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Review Non-Locality Subrecipients' Audit Reports and Communicate Results Timely

Compliance continues to not review non-locality subrecipient Single Audit reports as established within its Agency Monitoring Plan. Non-locality subrecipients are subrecipients, who are not local governments, and are mainly comprised of non-profit organizations. During fiscal year 2022, Social Services disbursed approximately $80 million in federal funds to roughly 200 non-locality subrecipients. While reviewing the audit reports for the 27 non-locality subrecipients that received more than $750,000 in federal funds from Social Services, we noted the following:

- Five non-locality subrecipients (19%) did not have a current Single Audit report available in the Federal Audit Clearinghouse (Clearinghouse). Fiscal year 2022 federal disbursements to these non-locality subrecipients totaled approximately $6.5 million.

- Two non-locality subrecipients (7%) had audit findings that affected one or more of Social Services' federal grant programs. As a result of the lack of review over non-locality subrecipient Single Audit reports, Social Services did not issue management decision letters within six months of acceptance of the audit reports by the Clearinghouse to collaboratively resolve audit findings related to Social Services' federal programs.

According to 2 CFR § 200.332(f), all pass-through entities must verify their subrecipients are audited if it is expected that subrecipient's federal awards expended during the respective fiscal year equaled or exceeded $750,000. Additionally, 2 CFR § 200.332(d)(3) requires pass-through entities to issue management decisions for applicable audit findings within six months of acceptance of the audit report by the Clearinghouse.

Without verifying whether non-locality subrecipients received a Single Audit report, Compliance is unable to provide assurance that Social Services met the audit requirements set forth in 2 CFR § 200.332(d)(3) and (f). Additionally, Compliance cannot provide Social Services' Executive Team with assurance that its subrecipient monitoring efforts are adequate without reviewing non-locality Single Audit reports.

Compliance did not review non-locality subrecipient Single Audit reports because it did not dedicate the resources necessary to implement corrective action. In its corrective action plan, Compliance planned to procure a centralized system to support its subrecipient monitoring efforts. However, Compliance was unable to procure a centralized system to support its subrecipient monitoring efforts during the fiscal year and it did not implement an alternative solution to comply with the requirements in 2 CFR § 200.332(d)(3) and (f). Compliance should determine what alternative solutions are available, if it is unable to procure a centralized system, and start reviewing non-locality Single Audit reports to comply with the federal regulations in 2 CFR § 200.332(d)(3) and (f).

Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Benefit Programs does not oversee subrecipient monitoring activities to ensure monitoring activities are conducted in accordance with its monitoring plan. During the fiscal year, Benefit Programs disbursed approximately $312 million in subaward payments from the Supplemental Nutrition Assistance Program (SNAP) and Medicaid Clusters and the LIHEAP and TANF federal grant programs. During the audit, we noted the following deviations from Benefit Program's monitoring plan:

- Benefit Programs created a monitoring plan to comply with Social Services' Agency Monitoring Plan. Regional consultants, who perform subrecipient monitoring activities, created their own subrecipient monitoring schedules that were not consistent with Benefit Program's monitoring schedule.

- Benefit Programs did not confirm that fiscal year 2022 monitoring review records uploaded to its data repository were complete. Some of the missing records included the agency notification letter, case selection sample, and subrecipient monitoring checklist.

- At the beginning of audit fieldwork, the data repository did not contain all subrecipient monitoring reviews performed during the fiscal year. The Subrecipient Monitoring Coordinator subsequently obtained and uploaded the remaining subrecipient monitoring reviews to Benefit Programs' data repository. The data repository only included the following subrecipient monitoring reviews at the time of the audit:

    - 12 of 25 (48%) reviews performed for the LIHEAP federal grant program;

    - 22 of 73 (30%) reviews performed for the SNAP Cluster;

    - 13 of 62 (21%) reviews performed for the Medicaid Cluster; and

    - nine of 62 (15%) reviews performed for the TANF federal grant program.

- Benefit Programs only completed 25 of the 67 (37%) scheduled reviews for the LIHEAP federal grant program.

Benefit Programs did not identify these issues because its monitoring plan did not clearly delineate who was responsible for overseeing subrecipient monitoring activities. As a result, no one in Benefit Programs was overseeing subrecipient monitoring activities. Title 2 CFR § 200.332(d) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure that the pass-through entity uses the subaward for authorized purposes in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Without confirming that program

consultants conduct monitoring activities in accordance with the monitoring plan, Benefit Programs cannot provide assurance that it complied with 2 CFR § 200.332(d).

In March 2022, Benefit Programs created a Subrecipient Monitoring Coordinator position to oversee its monitoring activities. The Subrecipient Monitoring Coordinator is working with Benefit Program's Associate Director for Operations and Support to confirm that Benefit Programs' monitoring plan meets federal requirements. Benefit Programs should continue its efforts to confirm that it conducts monitoring activities in accordance with its monitoring plan.

Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Benefit Programs' monitoring plan does not include all subrecipient programmatic activities for the TANF federal grant program. Benefit Programs' primary programmatic activity for the TANF federal grant program is eligibility determination functions performed by local agencies. However, Benefit Programs also awards various competitive grants to local governments and non-profit organizations to help TANF recipients become self-sufficient. Benefit Programs did not include these programmatic activities in its monitoring plan. During the fiscal year, Benefit Programs disbursed approximately $47 million in TANF competitive grants to roughly 160 organizations.

Title 2 CFR § 200.332(b) requires all pass-through entities 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. Additionally, 2 CFR § 200.332(d) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure that the pass-through entity uses the subaward for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward; and achieves subaward performance goals.

When Benefit Programs developed its monitoring plan, it only focused on eligibility functions performed by local agencies but did not consider other programmatic activities for the TANF federal grant program. Without including the other programmatic activities in the monitoring plan, Benefit Programs cannot provide assurance that subrecipients used TANF federal grant funds for authorized purposes in compliance with federal statutes, regulations, and the terms and conditions of the subaward.

Benefit Programs should update its monitoring plan to include all subrecipient programmatic activities for the TANF federal grant program and ensure each subrecipient is subject to the appropriate risk assessment procedures. Additionally, Benefit Programs should review its awards data for the federal grant programs under its purview to determine if it should include any other subrecipient programmatic activities in its monitoring plan. Benefit Programs' monitoring coordinators should then review the division's monitoring efforts to ensure program consultants conduct them in accordance with the risk assessment.

Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Evaluate Subrecipients' Risk of Non-Compliance

Benefit Programs continues to not evaluate subrecipients' risk of noncompliance with federal regulations related to the administration of the SNAP and Medicaid Clusters and the TANF and LIHEAP federal grant programs. Benefit Programs develops its subrecipient monitoring approach using the size of the subrecipient; however, it does not perform any further risk assessment procedures to determine the monitoring approach. Social Services disbursed approximately $312 million to subrecipients from these federal programs during the fiscal year.

Title 2 CFR § 200.332(b) requires pass-through entities 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. Further, 2 CFR § 200.332(b) suggests that pass-through entities should 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 developed a corrective action plan to perform risk assessment procedures to comply with 2 CFR § 200.332(b); however, Benefit Programs was unable to implement corrective action due to staff turnover. Without performing the proper risk assessment procedures, Benefit Programs cannot demonstrate that it monitored the activities of the subrecipient as necessary to ensure that the pass-through entity used the subaward for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward.

Benefit Programs should continue its corrective action efforts to implement a risk assessment process for subrecipients that is consistent with federal regulations and ensure that its monitoring efforts are consistent with the results of its risk assessment.

Comply with TANF Requirement to Participate in the Income Eligibility and Verification System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Controls over Income Verification for the TANF Program

Social Services continues to work on implementing a process to comply with the Income Eligibility and Verification System (IEVS) requirement for the TANF federal grant program. In August 2020, Social Services completed and implemented the design for the new IEVS process to provide a defined process for working the IEVS matches. However, due to Internal Revenue Service (IRS) security requirements, Local Departments of Social Services (local agency) staff are unable to use IEVS.

Title 45 CFR § 264.10 requires states to meet the requirements of IEVS and request the following information: (1) IRS unearned income; (2) State Wage Information Collections Agency (SWICA) employer quarterly reports of income and unemployment insurance benefit payments; (3) IRS earned income maintained by the Social Security Administration; and (4) immigration status information maintained by the Immigration and Naturalization Service. IEVS requires local agency employees to have background investigations, including Federal Bureau of Investigation (FBI) fingerprinting for employees who can access IEVS, as it contains federal tax information. IRS Publication 1075, Section 2.C.3 Background Investigation Minimum Requirements, states background investigations for any individual granted access to federal tax information must include, at a minimum, FBI fingerprinting, a check of where the subject has lived, worked, and/or attended school within the last five years; and validation of citizenship/residency to ensure the individual is legally eligible to work in the United States.

Virginia law does not require local agency employees to successfully pass a fingerprint background check; therefore, local agencies 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. Social Services drafted a legislative proposal for a fingerprint background check requirement for local agency employees and presented the proposal to the Secretary of Health and Human Resources for consideration during the 2022 General Assembly session. However, the Secretary of Health and Human Resources did not approve this proposal to move forward to the General Assembly.

By not using IEVS when verifying income for TANF participants, Social Services cannot verify that participants in the TANF program have met all eligibility requirements. As a result, per 45 CFR § 264.11, the Commonwealth could incur a two-percent reduction of the adjusted State Family Assistance Grant payable for the immediately succeeding fiscal year, unless the state demonstrates that it had reasonable cause or achieved compliance under a corrective compliance plan.

Social Services will not fully comply with the IEVS federal requirement until the Secretary of Health and Human Resources approves the legislative proposal to move forward to the General Assembly. Social Services should continue to work with the Secretary of Health and Human Resources to propose legislation to the General Assembly to require local agency employees to successfully pass a fingerprint background check. If the General Assembly passes legislation, Social Services should then implement a policy and procedure requiring background checks of local agency employees who access IEVS and ensure the local agencies processing TANF applications properly verify income using IEVS when determining eligibility for TANF.

Strengthen Internal Controls over FFATA Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Finance is not maintaining proper internal controls over FFATA reporting. FFATA reporting helps to provide full disclosure for how entities and organizations obligate federal funding. During the fiscal year, Social Services disbursed approximately $588 million in federal funds from roughly 5,000

subawards. During our audit of the TANF, Adoption Assistance, Foster Care, and Social Services Block Grant (SSBG) federal grant programs, we noted the following deviations from Finance's policy:

- Finance did not complete the required FFATA reporting submissions for the TANF and SSBG federal grant programs.

- Finance did not complete FFATA reporting submissions for three of five (60%) of the subawards sampled for the Adoption Assistance federal grant program. For the two reports tested, Finance could not provide documentation supporting entries into the FSRS. Additionally, Finance submitted these reports nearly three and one-half months after the due date.

- For the five subawards tested for the Foster Care federal grant program, Social Services was unable to provide documentation supporting entries into the FSRS for all subawards. Additionally, Finance submitted these reports nearly three and one-half months after the due date.

Title 2 CFR Part 170 Appendix A requires the non-federal entity to report each obligating action exceeding $30,000 to the FSRS. Further, 2 CFR Part 170 Appendix A requires the non-federal entity to submit subaward information no later than the end of the month following the month in which it made the obligation. Finally, 2 CFR § 200.303(a) states that the non-federal entity must establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Finance did not report this information to FSRS because program personnel did not submit the required information to Finance to report in FSRS. Additionally, Finance was not reviewing Social Services' financial records to ensure program personnel reported all required subaward information. Not uploading obligating actions to FSRS could result in a citizen or federal official having a distorted view as to how Social Services is obligating federal funds.

Finance should remind program personnel to submit required FFATA subaward reporting information as required by its policy. Additionally, Finance should consider periodically checking Social Services' financial records to see if there are instances where program personnel are not submitting the required FFATA subaward reporting information. If so, Finance should collect this information from them promptly to comply with the FFATA reporting requirements.

Perform Analysis to Identify Service Provider Agencies That Perform Significant Fiscal Processes
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Social Services is not performing a comprehensive analysis of service provider agencies during its Agency Risk Management and Internal Control Standards (ARMICS) review to determine if they perform significant fiscal processes. Significant fiscal processes include, but are not limited to, programs or activities that have a high degree of public visibility, represent areas of concern and high risk to mission-critical business processes for agency managers and stakeholders, or have a significant effect on general ledger account balances. Social Services transferred $90 million to other state agencies or institutions from various federal grant programs during the fiscal year to administer certain grants management functions on its behalf.

CAPP Manual Topic 10305 states an agency (primary agency) may use another agency (service provider agency) to perform significant fiscal processes for the primary agency. ARMICS states that decisions about significance should consider not only quantitative, but also qualitative factors, and managers should define any fiscal process as significant if errors or misstatements in the process could have adverse consequences for legal or regulatory obligations. Further, CAPP Manual Topic 10305 states that if a primary agency identifies a service provider agency that performs significant fiscal processes, the primary agency must have adequate interaction with the service provider agency to gain an appropriate understanding of the service provider agency's control environment and obtain assurances from the service provider agency regarding the state of internal control applicable to the significant fiscal processes performed. Finally, 2 CFR § 200.303(a) states that the non-federal entity must establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

During its analysis of service provider agencies, Social Services only considered service provider agencies that have a significant effect on general ledger account balances and not those that have a high degree of public visibility or represent areas of concern or high risk to mission-critical business processes. Without performing a comprehensive analysis of service provider agencies during its ARMICS review, Social Services cannot assure itself that it has obtained adequate coverage over service provider agency operations that are quantitatively or qualitatively significant to its operations.

Social Services should identify all service provider agencies and determine which of them provide significant fiscal processes. Thereafter, Social Services should perform a comprehensive analysis to determine if it has an appropriate understanding of the service provider agency's control environment and obtain assurance from the service provider agency regarding the state of internal control applicable to the significant fiscal processes performed.

Document Process to Collect and Retain Documentation Supporting the SSBG Post-Expenditure Report

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Finance does not have a documented process in place to collect and retain documentation supporting the number of eligible individuals who received services paid for in part or in whole with federal funds under the SSBG, which it reported in its federal fiscal year 2021 SSBG Post-Expenditure Report submission to the ACF in March 2022. ACF requires that states submit an annual Post-Expenditure Report that describes how the state expended SSBG funds for the past year. ACF's Office of Community Services analyzes SSBG expenditure and recipient data reported through the Post-Expenditure Reports to develop the SSBG Annual Report and performance measures for the SSBG program.

Title 45 CFR § 96.74 requires states to report actual numbers of recipients and actual expenditures when this information is available. Additionally, 2 CFR § 200.303(a) requires pass-through entities to establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Finance has a consistent process for obtaining and retaining supporting documentation for financial data reported to the federal government but has not yet documented a process for collecting and retaining performance data showing the number of eligible individuals who received services from SSBG. Without documenting its process and retaining supporting documentation, Finance cannot provide assurance that the data included in the SSBG Post-Expenditure Report is accurate. Finance should document a process to collect and retain all supporting documentation used to complete the SSBG Post-Expenditure Report submitted to ACF to provide assurance that the data included within the Report is accurate.

Monitor Internal Procedures to Ensure Compliance with the Conflict of Interests Act

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Improve Compliance with Conflict of Interests Act

Human Resources is not monitoring compliance with its internal procedures to ensure individuals in positions of trust file the required Statement of Economic Interests (SOEI) disclosure form and complete the required Conflict of Interests Act (COIA) training. Of the 41 employees identified in positions of trust, nine employees (22%) did not file an SOEI form. Three of the nine individuals who did not file an SOEI form held positions with procurement responsibilities. Additionally, of nine randomly selected employees identified in positions of trust, Human Resources was unable to locate the training records for five employees (56%) to demonstrate they completed their required COIA training.

Executive Order Number Eight (2018) requires that the head of each agency, institution, board, commission, council, and authority within the Executive Branch be responsible for ensuring that designated officers and employees file their SOEI form in accordance with § 2.2-3114 of the Code of Virginia. Additionally, § 2.2-3114 and § 2.2-3118.2 of the Code of Virginia state that 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. Further, § 2.2-3130 of the Code of Virginia states orientation training is required to be completed by filers within two months of their hire or appointment and at least once during each consecutive period of two calendar years. Finally, the Virginia Public Procurement Act requires state agencies to adopt the provisions of the COIA to promote ethics in public contracting, and 2 CFR § 200.317 requires states to follow its procurement policies and procedures when procuring property and services with federal funds.

While Human Resources has sufficient policies and procedures in place to ensure compliance with the COIA, it has not monitored compliance with its procedures to ensure all employees in positions of trust file their SOEI forms timely and complete the required training. Human Resources has not been able to monitor compliance with its policy because of turnover within its division.

Without appropriately monitoring individuals in positions of trust, Human Resources cannot ensure that it is fully compliant with the provisions in the COIA. In effect, Social Services could be susceptible to actual or perceived conflicts of interest and limited in its ability to hold employees accountable. These actions could potentially lead to a violation of state or federal laws or regulations. Human Resources should dedicate the resources necessary to monitor all employees designated in a position of trust to ensure they file the required SOEI form and complete the required COIA training.

Reconcile the Commonwealth's Retirement Benefits System

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Human Resources does not sufficiently reconcile retirement contributions before confirming to VRS that retirement data is correct. During the audit, we noted the following deficiencies:

- Human Resources did not perform the required monthly reconciliations between the Commonwealth's retirement benefits system and the Commonwealth's human resource system for eight months (67%) of fiscal year 2022.

- Human Resources did not review the Commonwealth's human resource system cancelled records report.

CAPP Manual Topic 50410 states that agencies should perform a reconciliation of creditable compensation and the approved purchase of prior service agreements between the Commonwealth's human resource and retirement benefits systems monthly before confirming the contribution. Further, CAPP Manual Topic 50410 requires a daily review of the human resource system cancelled records report.

While the Payroll Services Bureau (Bureau) performs certain reconciliation processes on behalf of Social Services, the Bureau's Scope of Services Manual states that agencies must reconcile credible compensation and approved prior purchase of service agreements from human resource data to the retirement benefits system, review the Commonwealth's human resource system cancelled records report, and resolve discrepancies identified during the reconciliation process prior to confirming the contribution snapshot.

Human Resources previously created policies and procedures to reconcile the Commonwealth's retirement benefits system, but experienced turnover in fiscal year 2022, which led to the lack of reconciliations of retirement contributions. Additionally, in April 2022, Social Services transitioned to the Commonwealth's new payroll and human resources system, which affected the internal controls in place over the reconciliation process. Social Services did not update its policies and procedures to reflect this system change due to inadequate staffing.

Insufficient 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 VRS actuary uses retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements. Reviewing and correcting items in the cancelled records report ensures accurate calculation of retirement benefits and proper transmission between the human resource and retirement benefits systems. Untimely certification of retirement contributions impacts the ability of Accounts to process inter-agency transfers for any differences between the amounts confirmed in the Commonwealth's retirement benefits system and the retirement contributions withheld and paid, for all agencies across the Commonwealth.

Human Resources should review CAPP Manual Topic 50410 and the Bureau's Scope of Services Manual to ensure it has an adequate understanding of its responsibilities in relation to reconciling retirement benefits system information. Additionally, Human Resources should update its policies and procedures to reflect its transition to the Commonwealth's new payroll and human resource system. Finally, Human Resources should ensure that it reconciles retirement data timely and in accordance with the CAPP manual prior to confirming the contribution snapshot monthly.

Correctly Report Status of Prior Audit Findings as of Fiscal Year End
Type: Internal Control and Compliance
Severity: Deficiency
Repeat: No

Social Services did not correctly report the status of four of 15 (27%) prior audit findings as of fiscal year end to Accounts. Social Services reported the prior audit findings titled "Improve Compliance with Conflict of Interests Act," "Improve Timely Removal of System Access," "Review and Document Service Organization Control Reports of Third-Party Service Providers," and "Strengthen Process over Medicaid Coverage Cancellations" as "Complete" in its corrective action workplan submitted to Accounts as of June 30, 2022. Accounts, assuming the completed corrective action achieved the desired results, listed the audit finding as "Resolved – corrective action is completed" in its draft Summary Schedule of Prior Audit Findings for the Commonwealth. However, during follow-up testing, we determined that Social Services did not resolve the conditions and causes of these prior audit findings.

CAPP Manual Topic 10205 states that it is the policy of the Comptroller that management should closely monitor corrective actions to ensure that they are timely and achieve the desired results. Additionally, CAPP Manual Topic 10205 notifies state agencies of the inclusion of their responses in the Commonwealth's Single Audit report and that responses should be well documented. Further, 2 CFR § 200.511 requires the Commonwealth to prepare a Summary Schedule of Prior Audit Findings that reports the status of applicable audit findings. The Commonwealth's Comptroller reports each audit finding's status as of June 30th.

Incorrectly reporting a prior audit finding as "Resolved – corrective action is completed" when Social Services has not yet achieved the desired result may cause management to stop deploying resources to correct the condition and cause of the prior audit finding and those charged with governance to believe Social Services has resolved the issue. Further, misrepresenting the status to Accounts may cause the Commonwealth to materially misrepresent the finding's status to the federal government.

Social Services did not correctly report the statuses of the four prior audit findings, referenced above, because of a lack of understanding of the audit finding or confusion with the corrective action reporting timeframes. Compliance monitors the corrective action plans for reasonableness and submits the agency's responses to Accounts. However, Social Services is not testing the operating effectiveness of the internal controls implemented to remediate the findings.

Compliance should provide clear instructions to the individuals responsible for reporting corrective action to make sure it receives accurate information to report to Accounts. Additionally, Social Services' Executive Team should dedicate the resources necessary to ensure the responses provided to Accounts are accurate and to verify that Social Services has implemented the corrective actions and tested that they are operationally effective. Additionally, if not already performed, Social Services should revise its June 30, 2022 corrective action workplan and resubmit to Accounts.

Status of Prior Year Findings and Recommendations

Continue Dedicating Resources to Support Information Security Program

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

DBHDS is making progress to allocate the necessary resources to manage its information security program and IT projects. As of September 2022, DBHDS has reduced its number of sensitive systems and applications from 183 in the prior year to 140 between the Central Office and its facilities. 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.

During the 2022 fiscal year, DBHDS filled an Information Security Analyst position and an Information Security Officer position in the Information Security Department and 11 various positions in the Information Technology Department. However, the Information Security Department is responsible for remediating several prior year findings, in addition to its other primary business functions. DBHDS previously estimated corrective action plans based on having five employees in the Information Security Department, but due to the lack of additional funding to hire the additional three staff, DBHDS has experienced delays in its corrective actions. The lack of resources to implement corrective action has ultimately caused DBHDS to have audit findings repeat for multiple years, specifically the absence of baseline configurations repeated for the seventh year and the IT contingency management documentation repeated for the fifth year.

The Security Standard, Section 2.4.2, states that agency heads are responsible for ensuring that the agency maintains, documents, and effectively communicates a sufficient information security program 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, which can result in a data breach or unauthorized access to confidential and mission-critical data. If a breach occurs and involves Health Insurance Portability and Accountability Act (HIPAA) data, 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 obtain and train additional staff in the Information Security Department. DBHDS should also allocate the additional 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 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 2022 audit, DBHDS created a template to ensure COOPs and DRPs are consistent for each facility and the Central Office and hired two contractors to work full-time on remediation efforts. As of November 2022, the Information Technology Department and Information Security Department are continuing their efforts to finalize COOPs and DRPs for the individual facilities and Central Office to combine into an agency-wide COOP and DRP. DBHDS expects to complete the COOPs and DRPs by the end of the 2022 calendar year and begin annual tests in 2023.

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, Section CP-1, 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 resource shortages within its Information Security Department, leading to the delay of the corrective actions.

DBHDS should dedicate the necessary resources to 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 IT

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

Since the prior year audit, DBHDS reduced its information system environment from 183 to 140 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 System Security Plan (SSP) template that includes a baseline configuration section for each system alongside other risk management documentation. DBHDS was unable to complete baseline configurations for its systems because of staffing shortages and focusing on other higher priorities; however, during the fiscal year DBHDS hired two contractors to work on the project full-time.

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 and manage a baseline configuration for information systems development and test environments that is separate 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 use the new SSP template to complete the baseline configurations for all new and existing systems. DBHDS should also establish a process to 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 Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Improve Database Security

DBHDS still does not secure the database server that supports its financial 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 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 in the communication marked FOIAE. Additionally, DBHDS's continued resource constraints 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. Implementing these controls will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Continue to Improve Risk Assessment Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Improve Risk Assessment Process

DBHDS has made progress in improving its risk assessment process. Since fiscal year 2021, DBHDS developed a new SSP template that includes elements for a system's risk assessment and risk treatment plan as required by the Security Standard and the Commonwealth's Information Technology Risk Management Standard, SEC 520 (Risk Management Standard). However, DBHDS has not completed a SSP for its 140 sensitive systems.

The Security Standard, Sections 6.2 and RA-3, requires DBHDS to conduct and document a risk assessment of the IT system as needed, but not less than once every three years, and conduct and document an annual self-assessment to determine the continued validity of the risk assessment. Additionally, the Risk Management Standard, Section 4.5.5, requires DBHDS to submit a risk treatment

plan for each risk with a residual risk greater than low to the Commonwealth's Chief Information Security Officer within 30 days of the final risk assessment report.

Without conducting risk assessments and risk treatment plans, 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 continues to experience resource shortages within its Information Security Department, leading to delays in corrective actions.

DBHDS should continue to dedicate the necessary resources to complete a risk assessment for each sensitive system. DBHDS should also complete a risk treatment plan for those risks identified with a residual risk greater than low that details the necessary information. Implementing these corrective actions will help DBHDS identify potential risks and implement adequate controls to mitigate risk to its individual systems, IT environments, and business operations.

Continue to Improve Controls over the Calculation of Contractual Commitments

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Improve Controls over the Process for Calculating Contractual Commitments

DBHDS should continue to improve controls over the calculation of contractual commitments that they report to Accounts for inclusion in the Commonwealth's financial statements. Since our prior review, DBHDS improved its processes for calculating contractual commitments to include the creation of policies and procedures. However, the following weaknesses remain.

DBHDS's estimation process does not consider if there are certain non-construction contracts that would not be applicable to an estimation process based on their nature. Further, DBHDS did not compile non-construction contract data timely following fiscal year end as required by its policies and procedures, therefore, data DBHDS used to estimate the non-construction commitment amount did not accurately represent the contract values as of fiscal year end. These weaknesses resulted in DBHDS understating non-construction commitments by $1.9 million. DBHDS also overstated its construction commitment by $4.9 million by including contracts that were complete or cancelled prior to fiscal year end.

Turnover within the Procurement and Architectural and Engineering offices contributed to the identified weaknesses. In addition to the turnover, improper maintenance of DBHDS's capital project management system due to competing priorities contributed to the on-going deficiencies. While these weaknesses did not have a material impact for fiscal year 2022, if left unaddressed, there is an increased risk that DBHDS will report inaccurate commitment amounts that could be misleading to users of the Commonwealth's financial statements. Accounts' Comptroller's Directive No. 1-22 establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the Commonwealth's financial statements 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 must certify the accuracy of the information provided to Accounts.

DBHDS should continue to improve its process for calculating commitments and ensure that all divisions follow the internal policies and procedures over calculating commitments. DBHDS should also ensure there are proper controls in place over estimations and manual processes. Further, DBHDS should ensure there is proper oversight of all divisions to ensure accurate and timely reporting of commitments.

Continue to Implement Compliant Application Access Management Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2018)

DBHDS continues to focus on implementing compliant access management procedures at the facility level that meet the baseline standard defined by the Security Standard. In June 2021, the Information Security Department revised its access management policies and procedures. Due to insufficient personnel and competing priorities within the Information Security Department, DBHDS has yet to confirm that facilities have implemented compliant access management procedures.

DBHDS has been working to reduce and standardize applications across the agency to aid in the implementation of compliant access management procedures. At the end of fiscal year 2022, the Information Security Department began a two-year project working directly with facilities to provide proper training on compliant access management procedures and implement processes to ensure facilities are complying with these procedures. Following the conclusion of the two-year project, the Information Security Department expects that all facilities will have implemented compliant access management 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.

DBHDS should continue to reduce and standardize applications across the agency as necessary. Additionally, the Information Security Department 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 department's baseline procedures and the Security Standard.

Ensure Compliance with the Conflict of Interests Act

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)

In fiscal year 2021, we determined that DBHDS was not properly identifying and tracking individuals in a position of trust to ensure compliance with the COIA requirements. In addition, DBHDS had a process for providing COIA training but did not monitor to ensure applicable individuals complete training. At the end of fiscal year 2022, Central Office Human Resources provided policies and procedures regarding COIA compliance requirements to all DBHDS facilities. However, corrective action remains ongoing and DBHDS continues to improve its processes to ensure compliance with COIA requirements. Due to ongoing corrective action during the period under audit, we did not perform testing of compliance with COIA requirements during the current audit.

Per § 2.2-3114 of the Code of Virginia, 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. Sections 2.2-3128 through 2.2-3131 of the Code of Virginia require 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 limit 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 should continue to 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 to ensure employees complete COIA training timely. Finally, DBHDS should ensure proper implementation of the policies and procedures that Central Office Human Resources developed at the end of fiscal year 2022.

Continue to Improve Controls over Payroll Reconciliations

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020)

DBHDS continues to improve processes and controls over the payroll reconciliation process. In fiscal year 2020, DBHDS facilities 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, however, corrective action remains on-going. In fiscal year 2023, the agency will transition payroll systems, which will affect the controls in place over the payroll reconciliation process. Due to ongoing corrective action during the period under audit and the change in payroll systems, we did not perform a detailed review of the payroll reconciliation process during the current audit.

CAPP Manual Topic 50905 requires agencies to maintain and update key control totals every time the agency processes payroll, 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 change in payroll systems. 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.

Strengthen Controls over Financial Reporting
Type: Internal Control
Severity: Material Weakness
Repeat: Partial (first issued in fiscal year 2021)

OFM needs to strengthen controls over financial reporting information submitted to Accounts and used in the preparation of the Commonwealth's financial statements. There were several instances where attachments OFM submitted to Accounts were late or contained errors requiring resubmission as follows:

- OFM reports information on accounts receivable on Attachment 21. The initial Attachment 21 was over a month late and OFM omitted a $64 million receivable from the Virginia Department of Emergency Management. OFM corrected the information and resubmitted Attachment 21; however, two subsequent revisions were necessary to correct additional errors.

- OFM was late in submitting multiple other items related to year-end reporting. These include Attachment 6A (Leave Liability Statement) which was five days late, Attachment 15 (Federal Schedules) which was 20 days late, Attachment 27 (GASBS No. 33 Federal Fund Analysis – Non-reimbursement Grants) which was 40 days late, Attachment 29 (Government-wide Payables and Other Accruals) which was 11 days late, and Supplemental Item #5 (Adjusted Payables) which was 33 days late.

- OFM did not perform a timely review of monthly reconciliations between Health's internal accounting system and the Commonwealth's accounting and financial reporting system. OFM did not review one of two (50%) monthly reconciliations until two months after the applicable office completed the reconciliation.

Health's financial activity is material to the Commonwealth's financial statements, so it is essential for the agency to have strong financial reporting practices. As a best practice, Health should submit financial reporting information to Accounts by the required due dates and should communicate any expected delays as soon as they are known. OFM's Financial Reconciliation Policy states that each office must submit the monthly reconciliation between Health's internal accounting system and the Commonwealth's accounting and financial reporting system to OFM by the 25th day of the following month. As a best practice, OFM should review these reconciliations in a timely manner.

There are several factors which contributed to these financial reporting issues. OFM has experienced a significant amount of turnover in key positions and hired new staff during the audit period for positions that were historically responsible for completing and submitting attachments as well as reviewing reconciliations. Health did not have policies and procedures on these processes for the new employees hired into these key roles to use as a resource. In addition, the agency has been under stress with the COVID-19 pandemic and the agency's role in statewide health policy, and OFM did not prioritize properly training new employees.

Management should continue working with OFM to fill vacant positions to ensure a more stable and adequate staffing level in this division. It is our understanding that addressing these concerns is currently a priority for OFM, and management is actively taking steps to implement corrective action. As management addresses this issue, they should ensure they have adequate written policies and procedures over key processes in place, as well as identify opportunities for cross-training, to ensure they have adequate measures in place to mitigate the effects of significant turnover in the future. Lastly, OFM should prioritize training new employees in key positions to improve the quality of financial information reported to Accounts.

Follow Eligibility Documentation Requirements for Women, Infants and Children Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)

Local health department eligibility staff did not complete required eligibility documentation for certain recipients under the Women, Infants and Children (WIC) program. For three of 25 (12%) cases, the local health department staff did not obtain acceptable forms of proof of identification or complete an affidavit confirming identity and residence requirements. While performance has significantly improved from the prior year, local health staff still did not follow policies and procedures in these instances.

Local health department staff are primarily responsible for determining eligibility for the WIC program. As a result of the COVID-19 pandemic, the federal government waived the eligibility requirements related to physical presence and allowed states to adopt alternative procedures to verify identity and residence requirements. In June 2020, Health received additional guidance from the United States Department of Agriculture Food and Nutrition Services (FNS), requiring proof of identification through encrypted emails or other approved collection methods. If local health staff are unable to collect this proof of identification, Health's procedures require staff to complete an affidavit to verify identity and residency. Additionally, FNS communicated that Health should have recipients sign a statement as to why they are unable to provide proof of identification or residency.

To address these policy changes, Health developed a Remote WIC Services policy in August 2020; however, the policy did not include the requirement for recipients to sign a statement in cases where the recipient could not provide proof of identification. In response to the prior year finding, Health revised the policy and provided training to local health department staff on the eligibility requirements. Health implemented the revised WIC Remote Services policy in January 2022 and although there has been improvement since the prior year, local health department staff are still adjusting to the revised policy.

When local health department staff do not properly verify identification and residential eligibility for recipients, there is a risk that Health could pay WIC benefits to ineligible recipients. In addition, if local health staff do not complete and keep a record of an affidavit, Health cannot hold recipients accountable for their information. Health central office staff should continue working with local health

department staff to ensure staff adhere to policies and procedures and maintain required documentation for WIC eligibility.

Continue Improving the Disaster Recovery Plan

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

Health made progress to improve the IT disaster recovery plan for its sensitive systems since our prior audit; however, it should continue to address certain processes in the plan to ensure compliance with the Security Standard. Health has not yet addressed through its remediation plan, a previously identified weakness, and we communicated this to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to descriptions of security mechanisms contained within the document.

The Security Standard requires agencies to 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 continued availability of Health's systems. As part of addressing this issue, Health should evaluate current resources available to implement these changes and consider requesting additional resources, if necessary.

Continue Improving Information Technology Change Management Process for a Sensitive System

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2020)

Health made significant progress since our prior audit in implementing a formal change control and configuration management procedure and process. Health completed and implemented the new process in October 2022; however, the new process has not been in production long enough for us to verify these changes. Additionally, Health created a draft Change Management Standard Operating Procedure (SOP) but has not yet completed and approved the SOP.

We communicated the additional issues 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.

Health should complete and approve the Change Management SOP, and ensure it includes all the Security Standard requirements. Health should then implement the established process to ensure staff follow the requirements in the Change Management SOP and the Security Standard. Implementing these improvements will help to ensure that Health's change management process protects the confidentiality, integrity, and availability of sensitive and mission essential data.

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

Health did not remove terminated users' access to certain information systems in a timely manner following the users' separation from the agency. During our review, we found delays in Health removing access from the following information systems:

- Health removed system access untimely for 67 of 106 (63%) financial and patient management system users from two to 254 days after the employees' separation dates.

- Health did not request system access removal timely for three of four (75%) Commonwealth's accounting and financial reporting system users. Health requested the removal of these accounts from seven to 11 business days after the employees' separation dates.

- Health did not request system access removal timely for two of four (50%) Commonwealth's human resources system users. Health requested the removal of these accounts six to 13 days after the employees' separation dates.

- Health did not request system access removal timely for two of five (40%) Commonwealth's payroll system users. Health requested the removal of these accounts two days after the employees' separation date.

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, Health 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.

Overall, Health's untimely removal of system access was primarily the result of management oversight and policies and procedures that are not in compliance with the Security Standard. With regard to the financial and patient management system, Health made some modifications to the access deletion process during the year which integrated termination dates Health entered in its personnel system. These modifications resulted in some improvements in the timeliness of system access deletion; however, several issues remain. Health's policies and procedures do not address a timeframe for access deletion and do not reflect the recent update to the process. As a result, there continue to be instances where Health does not delete access in accordance with the requirements of the Security Standard.

The remaining three systems involved in this issue are statewide systems where Health is responsible for notifying the relevant central agency to terminate the system access. In these cases, Health did not notify the relevant agency in a timely manner due to management oversight. In addition,

Health's policies and procedures are not adequate to ensure compliance with the Security Standard. As an example, for the Commonwealth's human resources system, Health's internal policy states if a user's termination occurs over the weekend, Health should remove access by the next business day. This policy, as written, does not ensure compliance with the Security Standard requirements.

Health should continue to strengthen its policies and procedures over system access to ensure compliance with the Security Standard for terminated employees' access removal. Strengthening the access removal process will improve compliance with the Security Standard and reduce the risk of unauthorized transactions and potential exposure of sensitive data.

Continue Strengthening the Termination Process

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2020)

Health did not properly execute all off-boarding procedures for employees who separated from the agency. Health did not process the final leave payouts for six of 20 (30%) employees in a timely manner. Health made the leave payouts between two and four pay periods after the employees' termination dates.

CAPP Manual Topic 50320 states that "final payments to terminating employees should be issued on the payday following the last period worked." As a result of Health untimely processing employee terminations, the former employees experienced delays in receiving their final payouts. The untimely processing was the result of several different issues, but resource constraints and prioritization of other tasks were contributing factors. In some cases, other departments did not provide required information to OFM timely. There were also instances where Human Resources did not approve leave submitted timely, and there were delays with OFM verifying the payment in the Commonwealth's payroll system.

Health should continue to strengthen the termination process to ensure departments provide all the required information to OFM in a timely manner, and supervisors perform subsequent approvals and reviews timely. Improving this process will reduce the risk of Health not processing leave payouts timely.

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 did not ensure employees occupying a position of trust completed the COIA training within the required timeframe. Nine of 70 (13%) employees designated as required filers did not complete the training. In addition, Health's records for tracking employee COIA training are not up to date. There were several instances where an employee had completed the training, but Health did not document completion in its records.

Section 2.2-3130 of the Code of Virginia requires filers to 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. Because not all of Health's SOEI filers have completed the necessary training even after Health notified them of the training requirement, Health may not be able to rely on its employees to effectively recognize, disclose, and resolve conflicts of interest.

Health is continuing to implement corrective action related to this issue. Health's Office of Human Resources (OHR) is responsible for monitoring employees' COIA training completion status. Health relies on an automated notification system to inform new and existing employees when they must complete certain required trainings and provides them with deadlines for completion. OHR properly notified employees of the training and deadlines but did not follow up to ensure the employee completed the training and met requirements.

OHR should continue to monitor all employees designated in positions of trust to ensure they complete the required COIA training once within each consecutive period of two calendar years and hold the employees accountable for untimely completion. This enhanced monitoring will improve compliance with the COIA and reduce the risk of improper or incomplete conflicts disclosure. Additionally, Health needs to ensure it keeps its records for tracking training up to date and accurate.

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, which the consultant grouped in ten findings. As of the end of fiscal year 2022, Medical Assistance Services resolved one of the ten findings and continues to make progress with nine remaining findings, 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 descriptions of security mechanisms.

Noncompliance with the required security controls increases the risk for unauthorized access to mission-critical systems and data in addition to weakening the agency's ability to respond to malicious attacks to its IT environment. Medical Assistance Services has experienced delays in addressing these findings due to staffing turnover and shortages as well as organizational changes that affected some of its processes. Medical Assistance Services updated its corrective action plan in June 2022, stating corrective actions are still ongoing for all nine findings and estimates it will complete corrective action for eight of the findings by the end of calendar year 2022 and the last finding by June 2023.

Medical Assistance Services should continue to dedicate the necessary resources to ensure timely completion of its corrective action plans and to comply with the Security Standard. These actions will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Continue Strengthening Process over Medicaid Coverage Cancellations

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Strengthen Process over Medicaid Coverage Cancellations
(This finding was also issued to the Department of Social Services)

Medical Assistance Services continues to oversee the review of individuals with an out of state address in the Medicaid claims processing module of the Medicaid management system who may no longer be eligible for Medicaid coverage. Based on data from our prior year finding, Medical Assistance Services, with assistance from Social Services, reviewed cases with an out of state address and subsequently closed approximately 6,700 cases and recouped $40.1 million in Managed Care Organization (MCO) payments. Medical Assistance Services further reviewed additional cases related to fiscal year 2022 and as of November 2022, Medical Assistance Services had identified an additional 8,500 cases for closure and recouped an additional $43.4 million in MCO payments. These efforts are ongoing as research is in progress for over approximately 4,700 cases; however, Medical Assistance Services anticipates completing the review of these cases by December 2022.

Medicaid eligibility is based on several financial and non-financial requirements. Section 12VAC30-40-10 of the Virginia Administrative Code lays out the general conditions of eligibility that an individual must satisfy to enroll in the Medicaid program. One of the non-financial requirements is that the individual be a state resident. In Spring 2020, with the onset of the Public Health Emergency (PHE), the federal government modified the program requirements and based on the Families First Coronavirus Response Act § 6008(b)(3), states cannot cancel Medicaid coverage during the PHE except in the following situations – an individual's death, an individual requests cancellation of coverage, or an individual relocates to another state. To ensure compliance with these requirements, Medical Assistance Services began reviewing coverage cancellation information monthly to ensure cancellations of coverage only occurred 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 reasons. For this process to be effective, Medical Assistance Services was relying on correct cancellation codes in the eligibility system; however, for the cases identified, the eligibility system produced a generic cancellation code causing Medical Assistance Services to reinstate the Medicaid coverage although the individual may have no longer been eligible for coverage.

Medical Assistance Services has undertaken significant efforts to address this issue. Medical Assistance Services staff, along with Social Services and other contracted staff, have performed detailed eligibility reviews of over 17,000 individual cases. In addition to these reviews, Medical Assistance Services has worked with Social Services to ensure it correctly records future coverage cancellations related to relocations to another state in the eligibility system. As of June 2022, Social Services programmed the eligibility system to return a specific cancellation code for relocating out of Virginia instead of a generic cancellation code. While this system change should reduce the number of cases that Medical Assistance Services reinstates when an individual has moved out of state, Medical Assistance Services has also implemented a new quarterly review process to identify individuals who may have relocated out of state and may no longer be eligible for Medicaid coverage. We encourage Medical Assistance Services, along with Social Services, to continue with these efforts to ensure only eligible individuals are receiving Medicaid benefits.

Improve Timely Removal of Critical System Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2017)
Prior Title: Remove Separated Employee Access in a Timely Manner

Medical Assistance Services did not remove access to the claims processing module or the eligibility system timely for individuals who separated from the agency and no longer needed access. For one out of eight (12.5%) users, Medical Assistance Services did not disable system access in the claims processing module within 24 hours of separation. The user retained their system access for 11 days after separation. For three out of 25 (12%) users, Medical Assistance Services did not disable system access in the eligibility system within 24 hours of separation. These three users were contract employees and retained their access to the system between 104 and 123 days after separation.

Medical Assistance Services' Access Control Policy requires that "all user accounts must be disabled immediately upon separation or within 24 hours upon receipt by the Office of Compliance and Security" (Compliance and Security). Failing to disable access timely for web-based mission-critical systems threatens the data integrity of the systems. If separated users retain access to the claims processing module or the eligibility system, users are potentially able to view, copy, and edit sensitive information.

There are several factors contributing to this issue. First, Medical Assistance Services' internal policy is not in compliance with the Security Standard. The Security Standard requires agencies disable access within 24 hours of separation, not within 24 hours of receipt of notification. Additionally, supervisors are not communicating information on separated employees timely. A separating employee's supervisor must initiate an exit clearance workflow for the system to automatically notify Compliance and Security for removal of system access. For the user of the claims processing module, the supervisor requested access termination more than 24 hours after the employee's separation. Finally, for the three users of the eligibility system, Compliance and Security received the access termination request timely but did not terminate access for more than 24 hours after receipt.

In June 2022, Medical Assistance Services implemented several organizational changes, including dissolving Compliance and Security. The responsibility for system access management moved to the division responsible for the system and its applicable business function. Medical Assistance Services is currently updating its internal Access Control policy to ensure it is consistent with the Security Standard and organizational updates. Medical Assistance Services expects to complete the policy and process updates in December 2022. Medical Assistance Services should also train and educate supervisors on the importance of timely notification of separated employees. Finally, Medical Assistance Services should ensure compliance with the Security Standard by removing user access as required.

Continue Developing Record Retention Requirements and Processes for Electronic Records

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

Social Services continues to operate without an adequate data retention process for its case management system. Social Services' case management system authorized over $10 billion in benefit payments from various public assistance programs to beneficiaries during fiscal year 2022. We communicated this 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 fiscal year 2019, Social Services gathered retention requirements from the business divisions. During the fiscal year, Social Services finalized and documented policies with retention requirements. However, Social Services has not developed, documented, and implemented a policy, procedure, and process to operationalize the record retention requirements needed.

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 it preserves, maintains, and makes accessible public-facing records 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. Further, the Security Standard, Section CP-9-COV, requires the agency implement backup and restoration plans for every IT system identified as sensitive relative to availability that address the retention of the data in accordance with the records retention policy.

Without developing, documenting, and implementing a policy, procedure, and process to operationalize record retention requirements, Social Services increases data risk and increases potential exposure to fines, penalties, or other legal consequences. Additionally, Social Services may cause the Commonwealth to spend additional resources to maintain, back up, and protect the information. Social Services should develop and implement a records retention policy and procedure that defines its requirements and processes to ensure that consistent record retention processes can be operationalized across business divisions to ensure compliance with laws and regulations.

Continue Improving IT Risk Management Program

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Social Services continues to not have a formal and effective IT risk management program that aligns with the requirements in the Security Standard. Since we first issued this finding during the fiscal year 2018 audit, Social Services remediated some risk management and contingency planning issues. However, Social Services continues to not:

- accurately verify and validate data and system sensitivity ratings;
- create risk assessments for 50 percent of its sensitive systems;
- create system security plans for 52 percent of its sensitive systems;
- perform annual reviews for 99 percent of its existing risk assessment documentation;
- perform annual reviews for 74 percent of its existing system security plan documentation; and
- implement corrective actions identified in risk assessments.

We communicated the details of these 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.

Due to the magnitude of the project, Social Services has not yet remediated all the weaknesses. Additionally, the requirements documented in the policy and the process documented in the procedure do not align, which contributed to Social Services not consistently completing risk management documentation due to conflicting roles and responsibilities. Without implementing a formal and effective IT risk management program, Social Services cannot assure itself that it is reducing unnecessary risk to the confidentiality, integrity, and availability to its information systems and data.

Social Services should prioritize and dedicate the necessary resources to remediate the weaknesses discussed in the communication marked FOIAE in accordance with the requirements in the Security Standard. Completing its corrective action plan will help to ensure the confidentiality, integrity, and availability of the agency's sensitive systems and mission-essential functions.

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 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 descriptions of security mechanisms. Social Services Change Management Process Guide details the

process Social Services follows to manage changes but does not include all the required elements, which contributed to the weaknesses remaining. Additionally, the change request form does not have the necessary fields to document the required elements.

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. Without doing such, Social Services cannot assure itself that it is reducing unnecessary risk to the confidentiality, integrity, and availability to its information systems and data.

Social Services should 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 Strengthening Process over Medicaid Coverage Cancellations
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2021)
Prior Title: Strengthen Process over Medicaid Coverage Cancellations
(This finding was also issued to Medical Assistance Services)

Medical Assistance Services continues to oversee the review of individuals with an out of state address in the Medicaid claims processing system module of the Medicaid management system who may no longer be eligible for Medicaid coverage. Based on data from our prior year finding, Medical Assistance Services, with assistance from Social Services, reviewed cases with an out of state address and subsequently closed approximately 6,700 cases and recouped $40.1 million in MCO payments. Medical Assistance Services further reviewed additional cases related to fiscal year 2022 and as of November 2022, Medical Assistance Services had identified an additional 8,500 cases for closure and recouped an additional $43.4 million in MCO payments. These efforts are ongoing as research is in progress for over approximately 4,700 cases; however, Medical Assistance Services anticipates completing the review of these cases by December 2022.

Medicaid eligibility is based on several financial and non-financial requirements. Section 12VAC30-40-10 of the Virginia Administrative Code lays out the general conditions of eligibility that an individual must satisfy to enroll in the Medicaid program. One of the non-financial requirements is that the individual be a state resident. In Spring 2020, with the onset of the PHE, the federal government modified the program requirements and based on the Families First Coronavirus Response Act § 6008(b)(3), states cannot cancel Medicaid coverage during the PHE except in the following situations – an individual's death, an individual requests cancellation of coverage, or an individual relocates to another state. To ensure compliance with these requirements, Medical Assistance Services began reviewing coverage cancellation information monthly to ensure cancellation of coverage only occurred 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 reasons. For this process to be effective, Medical Assistance Services was relying on correct cancellation codes in the eligibility system; however, for the cases identified, the eligibility system produced a generic cancellation code causing Medical Assistance Services to reinstate the Medicaid coverage although the individual may have no longer been eligible for coverage.

Medical Assistance Services has undertaken significant efforts to address the issue. Medical Assistance Services staff, along with Social Services and other contracted staff, have performed detailed eligibility reviews of over 17,000 individual cases. In addition to these reviews, Medical Assistance Services has worked with Social Services to ensure it correctly records future coverage cancellations related to relocations to another state in the eligibility system. As of June 2022, Social Services programmed the eligibility system to return a specific cancellation code for relocating out of Virginia instead of a generic cancellation code. While this system change should reduce the number of cases that Medical Assistance Services reinstates when an individual has moved out of state, Medical Assistance Services has also implemented a new quarterly review process to identify individuals who may have relocated out of state and may no longer be eligible for Medicaid coverage. We encourage Medical Assistance Services, along with Social Services, to continue with these efforts to ensure only eligible individuals are receiving Medicaid benefits.

Continue to Strengthen Internal Controls to Ensure Compliance with Federal Employment Eligibility Requirements

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

Human Resources continues to strengthen internal controls over the employment eligibility verification process. Since the prior year, Human Resources has implemented partial corrective action by communicating policies and procedures internally. However, Human Resources' policy manual continues to not include the acceptable forms of documentation necessary to verify employment eligibility. Additionally, Human Resources has not implemented a process to verify the accurate completion of the Employment Eligibility Verification Form (Form I-9). Human Resources has been unable to complete these corrective actions because of turnover in its Benefits Manager position. As a result, we did not perform a detailed review of employment eligibility practices.

The Immigration Reform and Control Act of 1986 requires employers to verify the identity and employment authorization of each person they hire. Additionally, the employer must complete and retain Form I-9 for each employee. Per the United States Citizenship and Immigration Services' Handbook for Employers M-274, employers must retain Form I-9 for a period of at least three years from the date of hire or for one year after the employee's employment termination, whichever is longer. Failure to comply with federal regulations could result in civil fines and/or criminal penalties and debarment from government contracts.

Human Resources should continue to implement corrective action by establishing written procedures to ensure Social Services uses acceptable forms of documentation to validate Form I-9. Additionally, Human Resources should develop an internal review process to ensure accurate completion of Form I-9.

RISK ALERTS

During 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 2022.

Unpatched Software
Repeat: Yes (first issued in fiscal year 2021)
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 continue to rely on contractors procured by VITA for the installation of security patches in their systems that support agency operations. Additionally, these agencies rely on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. At the time of our audit, the ITISP contractors had not applied a significant number of critical security patches to these agencies IT environments, all of which are past the 90-day Security Standard requirement.

The 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. Missing system security updates increase the risk of successful cyberattack, exploit, and data breach by malicious parties.

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 IT infrastructure components at the agencies listed above to remediate vulnerabilities in a timely manner or taken actions to obtain these required services from another source. DBHDS, Health, and Medical Assistance Services are working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Additionally, our separate audit of VITA's contract management will continue to report on this issue.

Access to Audit Log Monitoring Tool
Repeat: No
Applicable to: DBHDS, Health, and Medical Assistance Services

DBHDS, Health, and Medical Assistance Services rely on the Commonwealth's ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, the agencies listed above 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, Health, 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 ratifying the ITISP contracts in 2018, over the last three years VITA has attempted to compel the ITISP contractor to grant agencies, such as DBHDS, Health, and Medical Assistance Services access to the monitoring tool and audit log information. However, as of October 2022, VITA and the ITISP contractor have not been able to grant access to individual agencies due to delays in configuring a new centralized monitoring tool that is replacing the original product. VITA is overseeing the ITISP contractor's current efforts to implement a new system to grant these agencies access to monitor audit log information. VITA estimates the agencies will have limited access to the monitoring tool by the end of the 2022 calendar year while other expected features do not have an estimated delivery date.

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. VITA not being able to enforce the deliverable requirements from the ITISP contractor increases the risk associated with the Commonwealth's data confidentiality, integrity, and availability.

DBHDS, Health, and Medical Assistance Services are working with VITA and VITA's ITISP contractor 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's contract management will continue to address this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2022

The Honorable Glenn Youngkin
Governor of Virginia

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, 2022. 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, 2022. 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/or attachments submitted to the Department of Accounts (Accounts); reviewed the adequacy of each agency's 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 have 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 significant cycles, classes of transactions, and account balances at the following agencies:

Department of Behavioral Health and Developmental Services

Commonwealth's retirement benefit system
Federal revenues, expenses, and compliance for:
    Prevention and Treatment of Substance Abuse Block Grant
Information system security (including access controls)
Institutional revenues
Licensing behavioral health providers
Operational expenses, including payroll expenses

Department of Health

Accounts payable
Accounts receivable
Collection of fees for services
Commonwealth's retirement benefit system
Federal revenues, expenses, and compliance for:
    Special Supplemental Nutrition Program for Women, Infants and Children
    Coronavirus Relief Fund Program
    Immunization Cooperative Agreements
Information system security (including access controls)
Inventory
Operational Expenses, including payroll expenses and small purchase charge card expenses
Revenue related to Cooperative Agreements between Health and local governments

Department of Medical Assistance Services

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

Department of Social Services

Budgeting and cost allocation
Child Support Enforcement assets, additions, and deletions
Commonwealth's retirement benefit system
Contract procurement and management
General Fund expenses
Federal revenues, expenses, and compliance for:
- Adoption Assistance
- Child Care and Development Fund (CCDF) Cluster
- Foster Care
- Low-Income Home Energy Assistance Program (LIHEAP)
- Medicaid Cluster
- Social Services Block Grant (SSBG)
- Supplemental Nutrition Assistance Program (SNAP) Cluster
- Pandemic Electronic Benefit Transfer (P-EBT) Administrative Costs
- Temporary Assistance for Needy Families (TANF)

Financial reporting
Human resources
Information system security (including access controls)

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. However, we audited select federal programs for agencies listed below with an "*" in support of the Commonwealth's Single Audit and we will separately report the results of those audits.

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 six findings in the sections titled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations" to be material weaknesses.

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 50 findings in the sections titled "Internal Control and Compliance Findings and Recommendations" and "Status of Prior Year Findings and Recommendations" to be significant deficiencies.

In addition to the significant deficiencies, we detected a deficiency in internal control that is not significant to the Commonwealth's Annual Comprehensive Financial Report and Single Audit but is of sufficient importance to warrant the attention of those charged with governance. We have identified one finding in the "Status of Prior Year Findings and Recommendations" to be a deficiency.

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 the Department of Accounts, after Health made adjustments to two attachments for material misstatements as noted in the "Audit Findings and Recommendations" section.

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, 2022. The Single Audit Report will be available at www.apa.virginia.gov in February 2023.

Exit Conference and Report Distribution

We discussed this report with management for the agencies included in our audit at an exit conference as we completed our work on each agency. Government Auditing Standards require the auditor to perform limited procedures on management's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Responses." Management's response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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

NELSON SMITH
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 06, 2023

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, 2022. We concur with the findings and our corrective action plan will be 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 recognize staffing challenges, evaluating risks we face due to decentralization, 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 during the past few fiscal years, 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 Divya Mehta, Director of Internal Audit, if you have any questions regarding our corrective action plan.

Sincerely,

Nelson Smith

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

Colin M. Greene, MD, MPH
State Health Commissioner

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

January 18, 2023

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

Dear Ms. Henshaw:

We have reviewed your report on our audit for the year ended June 30, 2022. We concur with the findings and our corrective action plan will be provided in accordance with the Department of Accounts guidelines.

We appreciate your team's efforts and constructive feedback. Please contact Tasha Owens, Internal Audit Director, at tasha.owens@vdh.virginia.gov or 804-864-7450, if you have any questions regarding our corrective action plan.

Sincerely,

Colin M. Greene, MD, MPH
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH
To protect the health and promote the well-being of all people in Virginia.

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CHERYL J. ROBERTS
DIRECTOR

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

January 10, 2023

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, 2022. We concur with the audit findings assigned to DMAS and will submit a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the work plans for corrective actions that DMAS will take to address the audit findings.

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

Sincerely,

Cheryl J. Roberts
Director

COMMONWEALTH of VIRGINIA
DEPARTMENT OF SOCIAL SERVICES
Office of the Commissioner

Danny TK Avula MD, MPH
Commissioner

January 19, 2023

Auditor of Public Accounts
James Monroe Building
101 North 14th Street 8th Floor
Richmond, VA 23219

Dear Mrs. Henshaw:

The Virginia Department of Social Services concurs with the audit findings included in the 2022 review conducted by the Auditor of Public Accounts.

Should you require additional information, please do not hesitate to contact Ross McDonald, Director of Compliance, via e-mail at ross.l.mcdonald@dss.virginia.gov or by telephone at (804) 380-5408.

Sincerely,

Danny TK Avula

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

SECRETARY OF HEALTH AND HUMAN RESOURCES AGENCY OFFICIALS

As of June 30, 2022

John Littel, Secretary of Health and Human Resources

Department of Behavioral Health and Developmental Services
Nelson Smith – Commissioner

Department of Health
Colin Greene, MD, MPH – Commissioner

Department of Medical Assistance Services
Cheryl J. Roberts, J.D. – Acting Director

Department of Social Services
Dr. Danny TK Avula – Commissioner