AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

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

AUDIT SUMMARY

This report summarizes our fiscal year 2023 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively, these four agencies spent $28.2 billion or 98 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, 2023, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and financial reporting system, each agency's internal accounting and financial reporting system, and supplemental information and attachments submitted to the Department of Accounts, after Health and Social Services made adjustments to their attachments for material misstatements as noted in the section titled "Internal Control and Compliance Findings and Recommendations;"

- 55 findings involving internal control and its operation necessary to bring to management's attention; six of which are considered to be material weaknesses;

- 46 of the 55 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 16 prior audit findings and recommendations identified as complete in the Findings Summaries included in the Appendix.

We identified the Low-Income Household Water Assistance Program (LIHWAP) and the Temporary Assistance for Needy Families (TANF) federal grant programs as high-risk major federal programs at Social Services and included them within the Commonwealth's Single Audit scope. We conduct our audits under the assumption that management has designed, implemented, and maintained internal controls that provide reasonable assurance that it managed the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

During the LIHWAP audit, we determined that management did not implement internal controls to comply with the federal regulations at Title 2 U.S. Code of Federal Regulations (CFR) § 200.303(a) and 2 CFR § 200.501(g), which require Social Services to maintain internal controls to provide reasonable assurance over contractor compliance. Due to the significance of the matters described in the finding titled "Obtain Reasonable Assurance Over Contractor Compliance with Program Regulations" in the "Internal Control and Compliance Findings and Recommendations" section of our report, we were unable to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on compliance for the LIHWAP federal grant program. As a result, we issued a disclaimer of opinion for the

LIHWAP federal grant program in the Commonwealth's Single Audit report for the year ended June 30, 2023.

For our audit of the TANF federal grant program, the Office of Management and Budget's (OMB) Compliance Supplement requires us to audit Social Services' 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) report submissions. During the audit, we determined that Social Services had not implemented internal controls to comply with the federal regulations at 45 CFR § 265.7(b), which require States to have complete and accurate reports that accurately reflect information available in case records are free of computational errors and are internally consistent. As a result, we communicated this matter to Social Services' management through the audit finding titled "Implement Internal Controls over TANF Federal Performance Reporting," which is included in the section of our report titled "Internal Control and Compliance Findings and Recommendations." Additionally, we issued a qualified opinion on the reporting type of compliance requirement for the TANF federal grant program because Social Services did not materially comply with the provisions at 45 CFR § 265.7(b), as compliance with this requirement is necessary for the Commonwealth to materially comply with the reporting compliance requirement applicable to the program.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

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. 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-

AUDIT FINDINGS AND RECOMMENDATIONS

We have reported our audit findings and recommendations below and organized them by agency within each section. The section titled "Internal Control and Compliance Findings and Recommendations" includes all current year findings, followed by risk alerts and a comment to management. The section titled "Findings Summaries" is a comprehensive list of findings by agency and includes the status of current and prior year findings.

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 2023 including the number of new and previously reported, but ongoing findings reported. Of these findings, there were six material weaknesses as follows: Social Services (4), Health (1) and Medical Assistance Services (1).

Summary of Findings by Agency

Chart 1

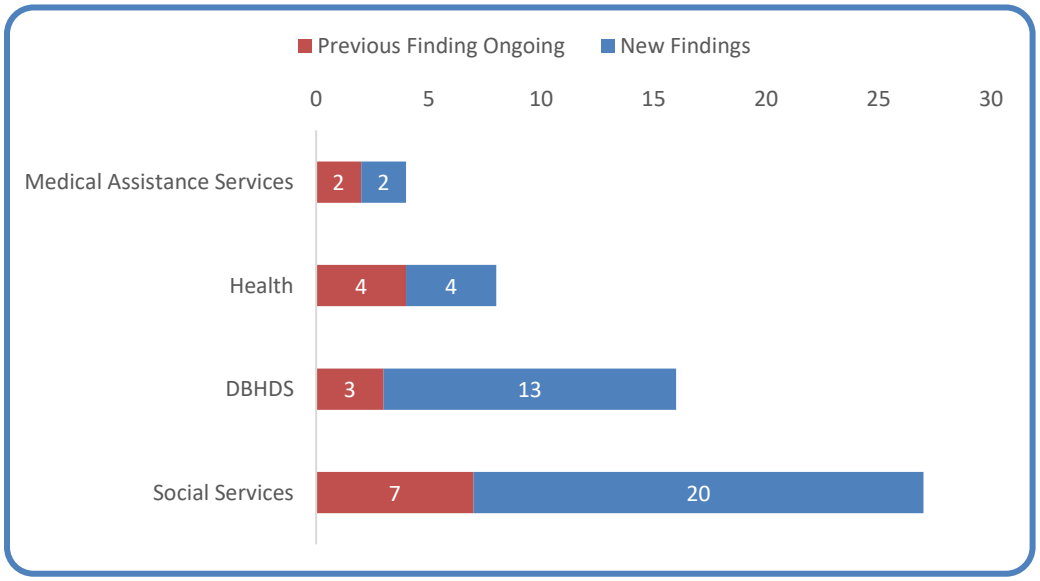
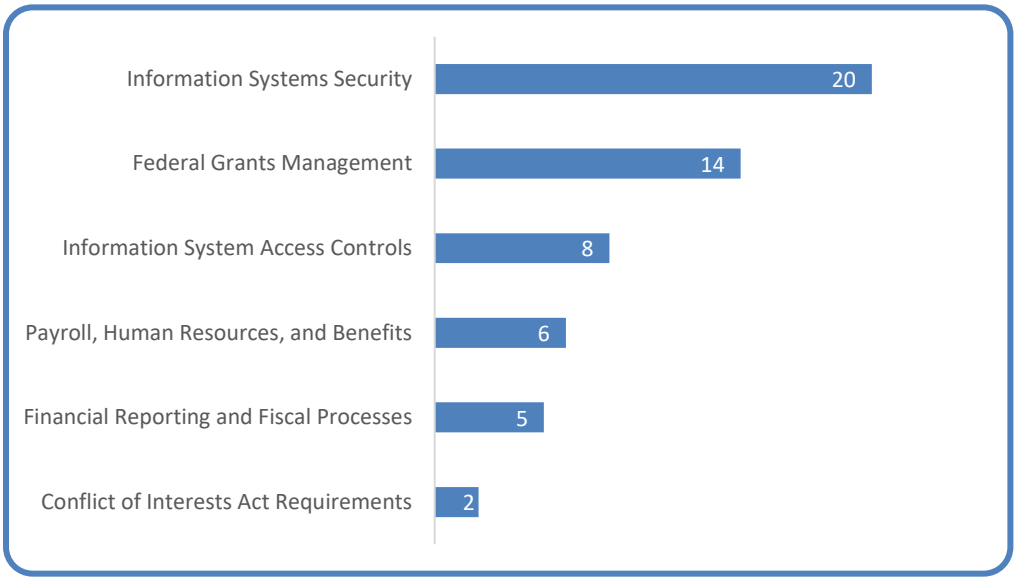


Chart 2 reports the total number of findings by internal control and/or compliance category for fiscal year 2023. As shown below, most findings related to one of two areas, information system security or federal grants management.

Number of Findings by Category

Chart 2



INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Vulnerability Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

DBHDS continues to not consistently remediate vulnerabilities in its information technology (IT) environment within the timeframe required by DBHDS's Vulnerability Management Program and the Commonwealth's Information Security Standard, SEC 501 (Security Standard). As of September 2023, DBHDS identified 2,828 high-risk vulnerabilities, of which 2,522 (89%) remained unmitigated beyond the Vulnerability Management Program's 30-day requirement. Of those 2,522 high-risk vulnerabilities, 30 vulnerabilities (1%) existed in DBHDS's IT environment beyond the 90-day requirement outlined in the Security Standard. Additionally, DBHDS does not obtain an approved exception for delays with its vulnerability remediation from the agency's Chief Information Security Officer (CISO) or the Commonwealth's CISO.

DBHDS's Vulnerability Management Program requires DBHDS to remediate vulnerabilities classified as high-risk within 30 days of the vulnerability discovery date or obtain an exception signed by the agency's CISO. Additionally, the Security Standard requires DBHDS to remediate legitimate vulnerabilities within 90 days in accordance with an organizational assessment of risk. The Security Standard also requires DBHDS to request for approval to deviate from a specific requirement in any related information security standard, if compliance would adversely impact a business process of the agency, by submitting an exception request to the Commonwealth's CISO (*Vulnerability Management Program, Sections Vulnerability Remediation Responsibilities and Vulnerability Exception Request; Security Standard, Sections RA-5 Vulnerability Scanning and 1.5 Exceptions to Security Requirements*).

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, which can lead to financial, legal, and reputational damages for DBHDS. Issues confirming vulnerabilities classified as false positives in the vulnerability management software led to confusion in DBHDS's vulnerability remediation efforts. Despite DBHDS's more stringent requirements, it completed several remediation tickets later than anticipated, extending the amount of time the vulnerabilities existed in the environment.

DBHDS should continue to improve its vulnerability management process to ensure it remediates all vulnerabilities within the timeline required by its Vulnerability Management Program based on severity. DBHDS should also ensure it identifies and removes false positive vulnerabilities from the scan to provide an accurate description of DBHDS's vulnerability landscape. If DBHDS must deviate from requirements outlined in its Vulnerability Management Program or the Security Standard, DBHDS should file for and receive an approved exception from the agency's CISO and the Commonwealth's CISO. By remediating legitimate 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
First Issued: Fiscal Year 2022

DBHDS continues not to perform timely IT security audits over its sensitive systems in accordance with the Commonwealth's IT Security Audit Standard, SEC 502 (IT Audit Standard). DBHDS planned to conduct 11 IT security audits during fiscal year 2023, based on the calendar year 2023 IT Audit Plan submitted in December 2022, but only completed nine audits as of fiscal year end. The IT Audit Plan includes both sensitive system audits and facility audits, and 109 of the 143 sensitive systems and facilities listed in DBHDS's IT Audit Plan do not have a record of receiving an IT security audit.

The IT Audit Standard requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Additionally, the IT Audit Standard 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 Resource Management Policies and Standards *(IT Audit Standard, Sections 1.4 Scope and Frequency of IT Security Audits and 2.2 IT Security Audit Scope*).

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's previous IT auditor left the agency at the end of calendar year 2022, and DBHDS filled the vacancy in August 2023. DBHDS did not consider outsourcing the IT security audits during the seven-month vacancy due to budget constraints. Limited staffing also continues to hinder DBHDS from completing its IT security audits within the three-year requirement.

DBHDS should allocate the necessary resources to either outsource or hire additional IT auditors to ensure it audits its sensitive systems 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.

Develop Baseline Configurations for Information Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2015

DBHDS is making progress to document baseline configurations for its sensitive systems' hardware and software requirements. Baseline security configurations are essential controls in information technology environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems.

Since the prior year audit, DBHDS reduced its information system environment from 140 to 90 sensitive systems and applications across the Central Office and 12 facilities, with some containing Health Insurance Portability and Accountability Act (HIPAA) data, social security numbers, and Personal Health Information data. Additionally, DBHDS developed a baseline configuration for seven of its 90 sensitive systems during fiscal year 2023.

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

- Develop, document, and maintain a current baseline configuration for information systems.
- Review and update the baseline configurations on an annual basis, when required due to environmental changes, and during information system component installations and upgrades.
- Maintain a baseline configuration for information systems development and test environments that it manages separately from the operational baseline configuration.
- Apply more restrictive security configurations for sensitive systems, specifically systems containing HIPAA data.
- Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

The absence of baseline configurations increases the risk that these systems will not meet the minimum-security requirements to protect data from malicious access attempts. If a data breach occurs to a system containing HIPAA data, DBHDS can incur large penalties, up to $1.5 million. The limited progress made in the last year is due to DBHDS's ongoing resource constraints and focusing on other higher priorities.

DBHDS should assign the necessary resources to continue its efforts to complete baseline configurations for the remaining systems as well as new systems implemented in the future. 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
First Issued: Fiscal Year 2021

DBHDS has made progress to 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).

Since the prior year audit, DBHDS has remediated three out of four identified weaknesses and while it has made progress to address the fourth weakness, DBHDS did not verify the database's configuration aligns with its baseline configuration or document justifications for deviating from the baseline. Additionally, DBHDS has not obtained an approved exception request from the Commonwealth's CISO for continuing to deviate from controls required by the Security Standard and as a result, it has not configured three settings in accordance with the Security Standard and CIS Benchmark. We communicated the remaining 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 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.

DBHDS works with an external vendor to manage the financial system. While the external vendor has provided verbal justifications in prior years for needing to deviate from certain controls required by the Security Standard or recommended by industry best practices, DBHDS did not verify, approve, and document the deviations and justifications in its baseline configuration, nor did DBHDS enforce the baseline's expected configuration.

DBHDS should work with its external vendor to review the deviations between the baseline configuration document and the database's configuration. For deviations that DBHDS verifies and approves, DBHDS should update its baseline configuration to reflect the deviation and business justification. For those it does not approve, DBHDS should enforce its baseline configuration and Security Standard requirements to ensure the database aligns with the agency's expected configuration settings. Additionally, if DBHDS must deviate from security controls required by the Security Standard, DBHDS should file for and receive an approved exception that includes a description of compensating controls that will reduce the risks to its environment.

Continue to Improve Offboarding Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2014

DBHDS is not properly offboarding employees, retaining appropriate documentation to support the completion of offboarding procedures, and removing system access for employees timely. Our review of terminated employees included reviewing offboarding processes at five different facilities and reviewing system access removals for the entire agency. When reviewing offboarding processes, we identified that four out of the five facilities tested were not consistently completing an offboarding checklist for terminated employees. During our review, we specifically identified the following deficiencies:

- For 15 of 26 (58%) employees tested at four DBHDS facilities under review, the facilities did not complete an offboarding checklist.

- For 12 of 26 (46%) terminated employees tested at three DBHDS facilities, the facilities did not remove building/system access in a timely manner.

- For ten of 26 (38%) terminated employees tested at three DBHDS facilities, the facilities could not provide supporting documentation showing the employees returned state property prior to their termination.

- For six of 29 (21%) terminated employees tested, DBHDS did not remove access to the Commonwealth's accounting and financial reporting system within 24 hours of the employee's separation.

- For six of ten (60%) terminated employees tested, DBHDS did not remove access to the internal patient revenue system timely, within 24 hours of the employee's separation.

DBHDS's Central Office has provided facilities with offboarding guidance and a termination checklist, which the facilities were to incorporate into their existing procedures. 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, job abandonment, and insufficient implementation of policies and procedures. Without sufficient and documented internal controls over terminated employees that ensure the return of Commonwealth property and removal of all access privileges, DBHDS is increasing the risk that terminated employees may retain physical access to Commonwealth property and unauthorized access to state and internal systems and sensitive

information. The decentralized nature of the agency and the secure nature in which the facilities operate further increases the exposure risk.

DBHDS should continue to improve offboarding 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 Security Standard. Furthermore, these procedures should address unique situations such as job abandonment. DBHDS Central Office and management across all facilities should ensure proper implementation and adherence with offboarding policies and procedures to include retention of supporting documentation and sufficient communication between responsible departments.

Improve Controls over the Payroll Certification Process

Type: Internal Control

Severity: Significant Deficiency

DBHDS should improve controls over the payroll certification process. Of the five facilities tested, four (80%) did not have evidence that the appropriate personnel reviewed the necessary pre- and post-certification reports or have documentation showing who prepared and reviewed payroll prior to certification. In addition, the facilities did not maintain proper documentation supporting any changes made to the payroll during the certification process. During the fiscal year under audit, the Commonwealth implemented a new payroll system. Formal guidance related to payroll certifications for the new system was issued late in the fiscal year and as a result DBHDS has not updated its policies and procedures to reflect the new payroll system. The exceptions noted were due to staff turnover, as well as not having updated policies and procedures to reflect the new payroll system.

Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 50800 – Payroll Confirmation details the required procedures that agencies must perform as part of the pre- and post-certification process related to payroll, and the supporting documentation that agencies must maintain. Additionally, CAPP Manual Topic 50800 states that there must be evidence of review such as initials or signatures, as well as the date of the review. By not following the proper payroll certification procedures, DBHDS increases the risk that inaccurate, unauthorized, or fraudulent payroll transactions could go undetected.

DBHDS Central Office should ensure that all facilities develop and implement policies and procedures for the payroll certification process that are specific to the new payroll system and in accordance with the CAPP Manual. Management should train employees responsible for the payroll certification process on the new policies and procedures and retain adequate documentation to provide evidence that employees followed the proper procedures including evidence of reports reviewed and supervisory review prior to certifying payroll, as well as support for any changes made to payroll.

Continue to Improve Controls over Payroll Reconciliations

Type: Internal Control
Severity: Significant Deficiency
First Issued: 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 payroll reconciliations. 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. This area was not subject to audit during the last two audits due to ongoing corrective action and DBHDS transitioning to a new payroll system in fiscal year 2023, which affected the controls in place over the payroll reconciliation process. During fiscal year 2023, no DBHDS facilities reviewed performed reconciliations over tax deductions and withholdings by pay period or monthly. Furthermore, the facilities did not perform a reconciliation of the new payroll system to the financial system by pay period or monthly as required. Formal guidance related to payroll reconciliations for the new system was issued late in the fiscal year and as a result DBHDS has not updated its policies and procedures to reflect the new payroll system.

CAPP Manual Topic 50905 requires agencies to maintain key control totals and update them every time the agency processes payroll to facilitate the tax deduction and withholding reconciliations. This topic also requires a monthly reconciliation over the control totals, tax deductions, and withholdings 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. Additionally, performing a reconciliation of the payroll system to the financial system provides assurance that the agency is processing the correct amount of payroll and recording payroll in the appropriate funds and accounts.

DBHDS should continue to improve controls over the payroll reconciliation process, including performing all necessary reconciliations to ensure that payroll is accurate. Management should develop and distribute payroll reconciliation policies and procedures to facilities based on the new payroll system that meet the newly established CAPP Manual requirements.

Continue to Implement Compliant Application Access Management Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 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 fiscal year 2023, DBHDS required more applications to use its multi-factor authentication procedures and began to develop the necessary access management training. Additionally, DBHDS began removing applications that are not compliant with its new process, reducing noncompliance. However, due to insufficient

personnel and competing priorities within the Information Security Office, DBHDS has yet to confirm that all 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 Office began a two-year project working directly with facilities to provide proper training on compliant access management procedures and implement processes to ensure facilities comply with these procedures. This project is ongoing as of the end of fiscal year 2023 and DBHDS expects to continue the project through the end of fiscal year 2024. Following the conclusion of the two-year project, the Information Security Office 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. 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 Office should continue to work with facilities to set reasonable deadlines, provide proper training, and monitor actions to ensure that application access management procedures at the facility level align with DBHDS's baseline procedures and the Security Standard.

Improve IT Contingency Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2017

DBHDS has made limited progress to complete updated Continuity of Operations Plans (COOP) and IT Disaster Recovery Plans (DRP) for its 12 facilities and DBHDS Central Office. In addition, the DBHDS Central Office and facilities are not performing annual tests of the COOPs or DRPs. Since the fiscal year 2022 audit, DBHDS has completed a COOP and DRP document for three facilities and drafted a document for another two facilities that it has not finalized. Additionally, DBHDS continues to participate in the annual Commonwealth-wide disaster recovery test for its servers.

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

By not having current COOPs and DRPs for all 12 facilities and the DBHDS Central Office, 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's lack of communication and coordination between the central Information Technology and Emergency Planning Departments and individual facilities have caused delays in its corrective actions.

DBHDS should ensure there is adequate communication and coordination among departments and continue its efforts to update the contingency management program for the DBHDS 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 DBHDS Central Office. Once the contingency documents are complete, DBHDS should conduct tests, on at least an annual basis, to ensure the DBHDS Central Office and facilities can restore mission-critical and sensitive systems in a timely manner in the event of an outage or disaster.

Continue to Improve Risk Assessment Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

DBHDS has made limited progress in conducting risk assessments over its sensitive systems in accordance with the Security Standard and the Commonwealth's Information Technology Risk Management Standard, SEC 520 (Risk Management Standard). Since the fiscal year 2022 audit, DBHDS completed risk assessments for four out of its 90 (4%) sensitive systems and of those four, DBHDS completed risk treatment plans for three of them.

The Security Standard 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 (*Security Standard, Section 6.2 Risk Assessment*). Additionally, the Risk Management Standard requires DBHDS to submit a risk treatment plan for each risk with a residual risk greater than low to the Commonwealth's CISO within 30 days of the final risk assessment report (*Risk Management Standard, Section 4.5.5 Reporting IT Risk Assessment Results (Findings)*).

Without conducting risk assessments and risk treatment plans for all systems, 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's Information Security Department hired two contractors to assist with completing corrective actions for ongoing findings, including risk assessments and risk treatment plans. However,

due to the number of systems within DBHDS's environment and the system documentation required for each, DBHDS did not make as much progress as it originally planned.

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

Continue Dedicating Resources to Support Information Security Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2019

DBHDS is making progress to allocate the necessary resources to manage its information security program and IT projects. As of September 2023, DBHDS has reduced its number of sensitive systems and applications from 140 in the prior year to 90 between the DBHDS 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.

Since the prior year audit, DBHDS's Information Security Department obtained one additional Information Security Officer (ISO) position, totaling six ISO positions that report to the agency's CISO. Additionally, the Information Security Department hired two contractors to assist its staff with corrective actions for several ongoing recommendations. However, vacancies for two ISO positions during fiscal year 2023 and the extensive number of corrective actions DBHDS must complete has ultimately caused DBHDS to repeat some audit findings for the eighth year, specifically the absence of baseline configurations.

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 (*Security Standard, Section 2.4.2 Agency Head*). Not having sufficient IT resources to manage the sensitive systems for the DBHDS Central Office and facilities increases the risk that certain controls may not exist, resulting in a data breach or unauthorized access to confidential and mission-critical data. If a breach occurs and involves HIPAA data, the agency can incur large penalties, as much as $1.5 million per year.

DBHDS should conduct an analysis of its current resource allocation to determine where gaps may exist to accomplish its outstanding corrective action plans. DBHDS should use the resource analysis to obtain and dedicate additional resources, if needed, to resolve the ongoing management recommendations and maintain its information security program in accordance with the Security Standard. Additionally, DBHDS should continue its efforts to reduce its sensitive system inventory.

Improve Change Management Process for Information Technology Environment

Type: Internal Control and Compliance

Severity: Significant Deficiency

DBHDS does not consistently follow its formal change control and configuration management process nor meet certain requirements in the Security Standard. DBHDS has two change and configuration management processes, one for its health records system and the second for all other changes to its IT environment. The following weaknesses exist for the IT environment configuration management process:

- DBHDS inconsistently documents the types of changes that users can request between its IT Change Management Process Guide (Process Guide) and its Change Management FAQ Presentation (FAQ Presentation). As a result, DBHDS does not consistently follow the workflows described in its Process Guide for the change types. DBHDS's IT Configuration Management Policy, which aligns with the Security Standard, requires DBHDS to determine the types of changes to the information system that are configuration controlled. By not consistently identifying and documenting the types of change that users can request, DBHDS increases the risk of implementing changes to production without obtaining the proper approvals and conducting the appropriate level of testing (*IT Configuration Management Policy Section B: Configuration Change Control; Security Standard, CM-3 Configuration Change Control*).

- DBHDS does not formally close all change request tickets for its IT environment. DBHDS classifies changes as resolved after implementing the change to production prior to formally assessing the change as closed. For DBHDS to formally consider a change as closed, the user must confirm the change's functionality in production and DBHDS conducts a post-implementation review. Out of 50 changes completed between January 2023, which is when DBHDS implemented the process, and June 2023, DBHDS did not formally close 14 (28%) of the changes. The Process Guide requires DBHDS to resolve and close changes after 30 calendar days (*Process Guide, Section 3.3: Activities*). By not formally closing the change requests, DBHDS risks having change tickets open for extended periods without confirming a successful change implementation.

- DBHDS does not annually review and revise, as needed, its IT Configuration Management Policy, which it last reviewed in December 2021. The Security Standard requires DBHDS to review and update the configuration management policy on an annual basis or more frequently if required to address an environmental change. By not performing annual policy reviews, DBHDS cannot ensure it properly communicates, implements, and enforces new security control and process requirements, which increases the risk for unauthorized changes to be implemented in the IT environment (*Security Standard, CM-1 Configuration Management Policy and Procedures*).

DBHDS's CISO is responsible for reviewing the agency's policies and procedures, but due to other competing priorities, the CISO was unable to review and update the IT Configuration Management Policy. Additionally, due to the recent implementation of the change management process for IT environment changes, DBHDS continues to enhance its documentation, train personnel, and enforce its policy requirements.

DBHDS should annually review its IT Configuration Management Policy, Process Guide, and FAQ Presentation to ensure it consistently documents the expectations for the change management process and it continues to align with the Security Standard. Additionally, DBHDS should train to its personnel to accurately classify the type of change, consistently follow the applicable process workflow based on the type of change requested, and formally close all change tickets in accordance with the agency's IT Configuration Management Policy, Process Guide, and the Security Standard. Maintaining an effective change management process will help to protect the confidentiality, integrity, and availability of sensitive and mission essential data.

Improve Security Awareness Training Program
Type: Internal Control and Compliance
Severity: Significant Deficiency

DBHDS does not administer its security awareness training program in accordance with its IT Security Awareness and Training Policy (Security Awareness Policy), the Security Standard, and the Commonwealth's Security Awareness Training Standard, SEC 527 (Security Awareness Training Standard). An established security awareness training program is essential to protecting agency IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the agency. Specifically, the following weaknesses exist with DBHDS's security awareness training program:

- DBHDS does not provide role-based training to all users with designated security roles, such as System Owners, Data Owners, System Administrators, Agency Head, and security personnel. While DBHDS developed some role-based training modules in its training platform, the agency has not finalized all role definitions applicable to the agency to include all necessary modules, causing DBHDS to delay its implementation of role-based training. DBHDS's Security Awareness Policy, which is based on the Security Standard, requires that the agency provide role-based security training commensurate with the user's level of expertise (*Security Awareness Policy, Section: B. Role-Based Training; Security Standard, Section AT-3 Role-Based Security Training; Security Awareness Training Standard, Section 3.5 Standards Alignment*). The lack of adequate role-based training increases the risk that users will be unaware or unequipped to perform their assigned security-related functions, resulting in an increased data security risk.

- DBHDS does not consistently monitor and enforce employee compliance with the new employee and annual refresher security awareness and training requirements. Specifically, out of 576 users assigned to new employee training between January and May 2023, 23 (4%)

users did not complete training within the required 30-day period and DBHDS did not disable access for 18 of those 23 (78%) users. Additionally, 18 out of 233 (8) users did not complete annual refresher training in calendar year 2022 and DBHDS did not disable access for 15 (83%) of those users for noncompliance. DBHDS's Security Awareness Policy designates each manager as responsible for ensuring their employees complete mandatory security awareness training. Additionally, the Security Awareness Policy requires all new DBHDS employees and business partners to complete security awareness training within the first 30 days of commencing work and repeat the training at least on an annual basis afterward, and states that the CISO or designee may revoke account rights until the employee or business partner completes mandatory security awareness training (*Security Awareness Policy, Section A. General Security Awareness Training; Security Standard, Sections AT-2 Security Awareness and AT-4 Security Training Records; Security Awareness Training Standard, Section 2.2 Information Security Officer (ISO)*). Without a process to consistently ensure that all users complete security awareness training at-hire and regularly thereafter, DBHDS increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

- DBHDS does not perform an annual review of its Security Awareness Policy, which DBHDS last reviewed in June 2021, and as a result, it does not reflect the additional security awareness training requirements outlined in the Security Awareness Training Standard. The Security Standard requires DBHDS to review and update the security awareness and training policy on an annual basis or more frequently if required to address an environmental change (*Security Standard, Section AT-1 Security Awareness and Training Policy and Procedures*). By not performing annual policy reviews, DBHDS cannot ensure that it communicates, implements, and enforces new security control and process requirements, which increases the risk for malicious users to exploit the potential gaps in the IT environment.

DBHDS's focus on other higher priorities, such as performing corrective actions for other ongoing management recommendations, and staffing turnover resulted in the above weaknesses occurring. DBHDS should dedicate the necessary resources to conduct annual reviews and revise the Security Awareness Policy, as necessary, to ensure its policy requirements align with those outlined in the Security Standard and Security Awareness Training Standard. Additionally, DBHDS should finalize and administer role-based training to users with designated security roles. DBHDS should also improve its monitoring and enforcement process to ensure all users complete IT security awareness training in accordance with its Security Awareness Policy, the Security Standard, and Security Awareness Training Standard. Improving the security awareness training program will help protect the agency from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive information.

Continue to Improve Controls Over the Retirement Benefits System Reconciliation

Type: Internal Control
Severity: Significant Deficiency
First Issued: Fiscal Year 2014

Individual DBHDS facilities did not adequately perform and document reconciliations between the Commonwealth's human resource and retirement benefits systems during fiscal year 2023. DBHDS has taken corrective actions since the prior audit to improve controls over the Commonwealth's retirement benefits system reconciliation, such as completing a reconciliation of creditable compensation. However, we noted the following deficiencies during our review of five facilities.

- Two facilities did not regularly review or address errors on the Centralized State Systems – Cancelled Records Report.

- Four facilities did not review the Commonwealth's human resource and payroll management billing exception reports for both months reviewed.

- Four facilities did not confirm the monthly contribution timely for 13 of 60 months (22%).

The facilities did not regularly review or address errors on the Centralized State Systems – Cancelled Records Report or review the Commonwealth's human resource and payroll management billing exception reports due to the implementation of the new payroll system. DBHDS has not developed policies and procedures specific to the new system. Guidance over the new payroll system was not available until late in the fiscal year, which caused confusion over the requirements and led to the facilities not reviewing these reports or confirming the monthly contribution timely. 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.

CAPP Manual Topic 50470 states that agencies must review and clear transactions on the Cancelled Records Report in the Commonwealth's retirement benefits system. Additionally, CAPP Manual Topic 50470 states that it is important to resolve exceptions on the Commonwealth's human resource and payroll management billing exception report as the automated transactions result in a charge to the agency for the employee's portion. The Code of Virginia prohibits employers from paying the employee portion. CAPP Manual Topic 50470 also requires agencies to confirm retirement contributions by the 10th of the following month.

Management at DBHDS facilities should ensure that staff adequately perform and document monthly reconciliations of the Commonwealth's retirements benefits system, confirm the information timely, and retain documentation to support their review of the necessary reports. Further, management should develop detailed policies and procedures and provide adequate training to payroll and human resource staff to ensure that they know how to properly perform the reconciliation process.

Ensure Compliance with the Conflict of Interests Act

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

In fiscal year 2021, DBHDS did not properly identify and track individuals in a position of trust to ensure compliance with the Conflict of Interests Act (COIA) requirements. In addition, DBHDS did not ensure the required employees completed the mandatory training. DBHDS has since provided policies and procedures regarding COIA compliance requirements to all DBHDS facilities. DBHDS Central Office Human Resources is now in the process of monitoring all DBHDS facilities to ensure they meet all necessary training requirements within the two-year required timeframe; however, corrective action remains ongoing and DBHDS continues to improve its processes to ensure compliance with all 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. Section 2.2-3130 of the Code of Virginia requires that each employee within a position of trust complete COIA training within two months of their hire date and at least once every two years after the initial training.

Without appropriately identifying employees in positions of trust and ensuring completion of required training, DBHDS could be susceptible to actual or perceived conflicts of interest and may 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 monitor all DBHDS facilities to ensure that employees within positions of trust file the appropriate disclosures upon hire or promotion, and subsequently at each annual filing period. In addition, DBHDS should continue to monitor employees to ensure they complete the required COIA training timely.

Continue to Improve Controls over the Calculation of Contractual Commitments

Type: Internal Control
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

DBHDS should continue to improve controls over the calculation of contractual commitments which they report to the Department of Accounts (Accounts) for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). DBHDS did not compile and calculate its contractual commitments accurately for fiscal year 2023. DBHDS's process for calculating the commitments disclosure incorrectly included negative amounts for completed contracts and included errors in the

calculation process. These weaknesses resulted in an overall understatement of contractual commitments of approximately $2.4 million.

DBHDS experienced turnover in the positions that are responsible for contractual commitment calculations, including positions within the Procurement, Architectural and Engineering, and Budget Offices which contributed to the identified weaknesses. In addition to the turnover, DBHDS does not have sufficiently detailed procedures for how DBHDS should compile and calculate the commitments disclosure. While these weaknesses did not have a material impact for fiscal year 2023, if left unaddressed, there is an increased risk that DBHDS will report inaccurate commitment amounts which could be misleading to users of the Commonwealth's ACFR. Accounts' Comptroller's Directive No. 1-23 establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the ACFR as required by the Code of Virginia. Accounts requires state agencies to submit information as prescribed in the Comptroller's Directives and individuals preparing and reviewing the submissions must certify the accuracy of the information provided.

DBHDS should continue to improve its process for calculating commitments and ensure that detailed procedures exist that outline all necessary steps required for calculating commitments. Further, DBHDS should ensure there is proper oversight of the process to ensure accurate reporting of commitments.

Strengthen Controls over Financial Reporting

Type: Internal Control
Severity: Material Weakness
First Issued: Fiscal Year 2021

The Office of Financial Management (OFM) needs to strengthen controls over financial reporting information submitted to the Department of Accounts (Accounts) and used in preparation of the Commonwealth's financial statements. There were several instances where information submitted to Accounts was late or contained errors and had to resubmitted as follows:

- OFM reports information on accounts receivable to Accounts on Attachment 21. The initial Attachment 21 included a $32 million receivable for the Coronavirus State and Local Recovery Fund, which OFM should not have included. OFM corrected the information and resubmitted the Attachment 21; however, three subsequent revisions were necessary to correct additional errors.

- OFM improved its timeliness over submitting required attachment and supplemental items related to year-end reporting to Accounts when compared to the previous fiscal year; however, there were still a few late submissions for fiscal year 2023. OFM submitted Attachment 6B (Leave Liability Statement) seven days late, Attachment 15 (Federal Schedules) five days late, and Attachment 27 (GASBS No. 33 Federal Fund Analysis – Non-reimbursement Grants) 19 days late.

- OFM does not have adequate policies and procedures for preparing reconciliations between its internal accounting system and the Commonwealth's accounting and financial reporting system. The policies and procedures do not require proper clearing for reconciling items or signature and date of the preparer or the reviewer. Three of three (100%) reconciliations did not include sign-off by preparer or reviewer.

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 associated due dates and should communicate any expected delays as soon as they are known. In addition, OFM should have a financial reconciliation policy that requires evidence of a preparer and reviewer of the reconciliations to ensure adequate segregation of duties. The policy should also specify actions to take in the case of reconciling differences between the internal accounting system and the Commonwealth's accounting and financial reporting system.

There are several factors contributing to these financial reporting issues. OFM has experienced a significant amount of turnover in key positions, particularly since January 2021. Health recruited new staff during the audit period for positions that were historically responsible for completing and submitting attachments to Accounts and preparing reconciliations; however, there were not adequate policies and procedures for the new employees to use as a resource.

Management should continue working with OFM to fill vacant positions to ensure a more stable and adequate staffing level. It is our understanding that this is currently a priority, as OFM is actively taking steps to address staffing needs. As OFM fill vacant positions, it should ensure it has adequate written policies and procedures over key processes in place, as well as identify opportunities for cross-training, to ensure there are 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 it reports to Accounts.

Improve Controls Over Journal Entries
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

OFM has multiple internal control weaknesses related to journal entry processing. OFM did not retain adequate supporting documentation or evidence of supervisory approval for three of 30 (10%) journal entries reviewed. OFM uses journal entries to record transactions that occur throughout the year or 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. Additionally, CAPP Manual Topic 20410 states that the entry approver should review the supporting documentation to ensure the entry contains proper coding for the adjustment. Federal regulations known as Uniform Guidance, specifically, 2 CFR § 200.303(a), require that Health establish and maintain effective internal control over federal awards that provides reasonable assurance that Health is managing federal awards in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Without adequate supporting documentation for journal entries, OFM increases its risk of recording inaccurate information and management may not be able to determine if accounting records are complete and accurate. 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 during the last two fiscal years. Health had vacancies and recruited new staff during the audit period for positions that were historically responsible for preparing and reviewing journal entries as well as retaining supporting documentation. However, Health did not properly train new staff in preparation of and documentation of journal entries. Health also did not have policies and procedures to help staff ensure proper documentation for journal entries is retained.

Health should prioritize training of employees in key positions on preparing and reviewing journal entries. OFM should improve internal controls over journal entries to ensure staff retain adequate supporting documentation, including evidence of supervisory approval. Additionally, OFM should ensure they document policies and procedures over key processes which will help ensure proper documentation of journal entries.

Follow Eligibility Documentation Requirements for Women, Infants and Children Program

Type: Internal Control and Compliance
Severity: Deficiency
First Issued: 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. While Health transitioned back to its in-person eligibility policy in August 2023, the local health staff did not follow the remote policies and procedures that were in effect during fiscal year 2023. For five of the 25 (20%) cases sampled, the local health department staff did not obtain acceptable forms of proof of identification or complete an affidavit confirming identity and residence requirements.

Local health department staff are primarily responsible for determining eligibility for the WIC program. As a result of the COVID-19 global pandemic, Health only verified eligibility for the WIC program remotely during the fiscal year. Based on guidance from the United States Department of Agriculture Food and Nutrition Services (FNS), proof of identification through encrypted emails or other approved collection methods was necessary. If local health staff were unable to collect this proof of identification, Health's procedures required 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 were unable to provide proof of identification or residency. Health addressed the guidance from FNS by creating a Remote WIC Services policy and procedure in August 2020. Health made several revisions to the policy and provided training to local health department staff on the eligibility requirements and retention of affidavits. Health implemented the revised policy in January 2022; however, local health staff overlooked the requirement to obtain affidavits when proof of identification for recipients was unable to be collected.

Not verifying identification and residential eligibility for recipients increases the risk that Health could pay WIC program benefits to ineligible recipients. In addition, if local health staff do not complete and keep on record an affidavit, Health cannot hold recipients accountable for their information. As Health transitions back to in-person WIC services in August 2023, Health central office staff should continue working with local health department staff to ensure they adhere to policies and procedures and maintain required documentation for WIC eligibility.

Improve Vulnerability Management

Type: Internal Control and Compliance
Severity: Significant Deficiency

Health does not consistently remediate vulnerabilities for software that is under Health's purview within the timeframe required in Health's Vulnerability Management Process and the Security Standard. The Virginia Information Technologies Agency (VITA) is responsible for remediating vulnerabilities related to servers and endpoints, but Health is responsible for remediating vulnerabilities for applications. Health and VITA work together to scan Health's systems for vulnerabilities using various tools. After obtaining and reviewing quarterly vulnerability scan reports, Health identifies the

vulnerabilities in the reports that it is responsible for remediating and assigns technical staff to remediate each identified vulnerability. However, Health does not ensure that it remediates each vulnerability within the timeframe required in Health's Vulnerability Management Process and that it remediates all legitimate vulnerabilities within 90 days. Additionally, Health does not ensure that the same vulnerabilities are not present in subsequent vulnerability scans.

Health's Vulnerability Management Process states that critical-risk vulnerabilities must be remediated within 15 days, high-risk vulnerabilities must be remediated within 30 days, medium-risk vulnerabilities must be remediated within 60 days, and low-risk vulnerabilities must be remediated within 90 days. The Security Standard requires Health to remediate legitimate vulnerabilities within 90 days (*Security Standard, Sections RA-5 and RA-5 COV).* Without remediating vulnerabilities within the required timeframes, Health increases the risk of unauthorized access to its 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, which can lead to financial, legal, and reputational damages for Health.

Resource constraints in the Information Security Office hindered effective end-to-end vulnerability management. Additionally, competing priorities, including operational duties, within the Office of Information Management (OIM) contributed to the increased time from discovery to remediation of legitimate vulnerabilities. The Information Security Officer (ISO) and OIM should closely collaborate to complete their respective tasks to improve Health's processes and remediate vulnerabilities within the timelines required by the Vulnerability Management Process and the Security Standard. Health should assess each element of the process to ensure its effectiveness for remediating all vulnerabilities within 90 days. Health should also ensure that the same vulnerabilities are not present in subsequent vulnerability scans. By remediating vulnerabilities timely, Health 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

Type: Internal Control and Compliance
Severity: Significant Deficiency

Health does not conduct a comprehensive IT security audit on each sensitive system at least once every three years that assesses whether IT security controls are adequate and effective. Specifically, Health developed an audit plan indicating 18 audits planned for fiscal year 2023. However, Health did not conduct nine of the 18 planned audits. Additionally, Health has not conducted an IT security audit over 16 other sensitive systems in the last three years.

The Security Standard, Section 7, requires that each IT system classified as sensitive undergo an IT security audit as required by and in accordance with the current version of the IT Audit Standard. The IT Audit Standard, Section 1.4, requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall 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 use criteria that, at a minimum, assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Security Standard.

Without conducting full IT security audits that cover all applicable Security Standard requirements for each sensitive system every three years, Health increases the risk that IT staff will not detect and mitigate existing weaknesses. Malicious parties taking advantage of continued weaknesses could compromise sensitive and confidential data. Further, such security incidents could lead to mission-critical systems being unavailable. The Office of Internal Audit (OIA) Administrative Procedures – Subject 6: IT Security Audits (OIA Procedures) tasks OIA with performing IT security audits. However, the OIA's Senior IT Auditor position has remained vacant since 2019, which contributed to Health being unable to complete the required audits. Budgetary constraints contributed to OIA's delay in recruiting a Senior IT Auditor qualified to perform technical audits of sensitive systems or procuring an external auditor to complete the required audits.

Management should evaluate potential options and develop a formal process for conducting IT audits over each sensitive system at least once every three years that tests the effectiveness of the IT security controls and compliance with Security Standard requirements. Health should then complete the planned IT security audits, either through its internal audit function or through the acquisition of external third-party services. Compliance with the IT Audit Standard will help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Continue Strengthening the System Access Removal Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2014

Health did not remove terminated employees' access to critical information systems in a timely manner following the employees' separation from the agency. During our review, we found that Health did not remove system access timely for 119 of 205 (58%) terminated users of Health's patient management system. Health removed these accounts two to 180 days after the employees' termination dates.

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. Untimely termination of system access increases the risk of terminated employees retaining unauthorized access to state systems and sensitive information and increases the risk of inappropriate transactions and exposure to sensitive data. Since the prior audit, Health updated its internal termination process to ensure proper communication between responsible offices. Health made some modifications to the access deletion process which integrated termination dates Health enters into its personnel system. This modification resulted in improvements with removing system access within Health's financial management system. However, Human Resources did not enter termination dates timely to communicate the need to remove access to Health's patient management system after employee termination.

Health administers public assistance programs that collect personally identifiable information and other protected information from beneficiaries. Health places its data and reputation at risk by not removing access timely. Additionally, Health could incur a potential financial liability should its information become compromised. Health should continue strengthening its internal process over system access to ensure Human Resources enters and approves employee termination dates timely to ensure access is removed in compliance with the Security Standard. This will reduce the risk of unauthorized transactions and potential exposure of sensitive data.

Improve Internal Controls over Employee Offboarding Process
Type: Internal Control
Severity: Significant Deficiency

Health does not have adequate internal controls over the terminated employee offboarding process. As a result, we identified the following deficiencies:

- The Office of Human Resources (Human Resources) did not enter three of 25 (12%) employees' termination dates within the Commonwealth's human resource and payment management system within 24 hours of the termination date.

- Human Resources was unable to confirm the collection of Commonwealth property for four of the 25 (16%) terminated employees sampled by the employees' termination dates.

- Supervisors did not submit timely notification of employees' termination to Human Resources for five of 25 (20%) terminated employees sampled to ensure timely removal of system access to Health's critical information systems.

- Human Resources was unable to locate the completed offboarding checklist for three of the 25 (12%) terminated employees sampled.

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. Additionally, Health's internal policy states that a separation checklist must be performed upon employee termination. Performing separation checklists immediately upon employee separation provides confirmation of the collection of all Commonwealth property assigned to the employees, increases the likelihood that termination dates are entered into the System within 24 hours, and ensures proper removal of access to Health's critical information systems. Not adequately completing the separation checklist increases the risk of misappropriation of Commonwealth assets.

Health's internal policy does not define specific timeframes for the completion of the separation checklist, which includes correspondence between Human Resources, OFM, and OIM, nor does it define a timeframe for system access removal. This lack of specificity makes it difficult to enforce adherence to the policy and ensure timeliness of completion. Health should review its current termination practices to ensure its policy is reasonable and internal controls are operating effectively. Improving the policy and associated controls will enable Human Resources to better monitor the timely completion of the employee separation checklist and access removal, which will ultimately reduce rates of noncompliance with the Security Standard and ensure Health collects Commonwealth property prior to termination.

Improve System Access Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency

Health lacks written documentation specifying the business need for access roles to its financial management system and patient management system, as well as the approval of those roles. As a result, we identified the following deficiencies:

- For six of 14 (43%) sampled financial management system users and nine of 25 (36%) patient management system users granted access during the current fiscal year, OIM was unable to provide supporting documentation that supervisors properly approved assigned roles and the assigned roles agree to the access request.

- For seven of 14 (50%) sampled financial management system users and five of 25 (20%) patient management system users granted access during the current fiscal year, we identified access roles that we consider to be separation of duties conflicts. These roles violate the principle of least privilege and OIM was unable to provide compensating control documentation to ensure system access is appropriate.

Section 8.1 AC-6 of the Security Standard requires the agency to employ the principle of least privilege, only allowing 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. When improper separation of duties exists, there is an increased risk that users can perform unauthorized transactions in the financial management system and patient management system. Approved documentation of the separation of duties concerns and compensating controls to mitigate risk provides accountability and assurance that Health is properly considering the risks of granting such access to its critical information systems. Lastly, not ensuring that system users have and retain appropriate access to Health's critical information systems increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of Health's transactions within its systems.

While Health has documented system access procedures, Health has not identified conflicting roles and does not have written documentation to justify and authorize access to the conflicting roles within its critical information systems when separation of duties concerns exist. Health should update its system access policies to require written documentation for users to justify and authorize conflicting access to its critical information systems. If violating the principle of least privilege and causing separation of duties issues is unavoidable, then Health 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. Lastly, Health should ensure supervisors properly authorize all access roles.

Improve Information Security Program and Controls
Type: Internal Control and Compliance
Severity: Material Weakness
First Issued: Fiscal Year 2020

Medical Assistance Services continues to address weaknesses in its IT general controls originally identified in a 2020 audit and confirmed in a 2023 audit covering the same IT general controls conducted by Medical Assistance Services' Internal Audit division. The 2020 audit tested 100 controls required by the Security Standard and identified 71 individual control weaknesses grouped into ten findings. Internal Audit conducted an audit in 2023 of 105 controls based on the current Security Standard requirements and identified 61 individual control weaknesses, a 58 percent noncompliance rate. Medical Assistance Services addressed one finding in fiscal year 2022 and an additional two findings during fiscal year 2023, which Internal Audit's review confirmed. However, Internal Audit issued one new finding to Medical Assistance Services in addition to the seven repeat findings, covering the following control areas:

- IT Security Governance
- Access Management
- System Security Plans
- IT Security Policies and Procedures
- Incident Response
- Penetration Testing and Vulnerability Assessments
- Third Party Vendor Management
- Security Awareness and Training (new)

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 ongoing staffing shortages, as well as lingering effects from organizational changes that affected some of its processes. Medical Assistance Services updated its corrective action plan for the seven repeat findings in June 2023, stating corrective actions are still ongoing with an estimated completion date of September 2023.

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

Obtain and Review Information Security Audit
Type: Internal Control and Compliance
Severity: Significant Deficiency

Medical Assistance Services has not obtained the required biennial automated data processing (ADP) risk analyses and system security audit of the Medicaid claims processing module of the Medicaid management system (claims processing module). The last audit of the claims processing module occurred during October 2020 and Medical Assistance Services received the report in January 2021. The Medicaid program is highly dependent on extensive and complex computer systems that include controls for ensuring the proper payment of Medicaid claims. These controls reside with the agency as well as with one of Medical Assistance Services' service providers.

As required by 42 CFR § 95.621, Medical Assistance Services must review its claims processing module on a biennial basis. At a minimum, the review must include an evaluation of physical and data security operating procedures and personnel practices. Additionally, the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard) states that agency heads remain accountable for maintaining compliance with the Hosted Environment Security Standard for IT equipment, systems, and services procured from service providers and must enforce the compliance requirements through documented agreements and oversight of the services provided.

Without the biennial audit, Medical Assistance Services cannot ensure the service provider has adequately designed and implemented the controls over the claims processing module and whether the controls are operating effectively. Although Medical Assistance Services maintains a high degree of interaction with the service provider, not obtaining and reviewing the biennial audit increases the Commonwealth's risk that it will not detect a weakness in the service provider's environment, which could negatively impact the Commonwealth. Due to the highly sensitive, mission-critical nature of the data and controls within the claims processing module, Medical Assistance Services is also compromising system integrity and increasing the risk of unauthorized system access.

Medical Assistance Services' contract with the service provider includes a biennial audit as a term of the contract. However, Medical Assistance Services did not ensure that the service provider completed the audit timely. In June 2023, the service provider communicated to Medical Assistance Services that the next audit would begin in July 2023 and in October 2023 the service provider communicated that it would deliver the report in December 2023.

Medical Assistance Services should ensure that the service provider completes the required biennial audit and that future audits meet the timing and other requirements in the contract. In addition, Medical Assistance Services should use the results of these audits to ensure its service provider complies with the requirements in the Hosted Environment Security Standard, Code of Federal Regulations, and contract with the Commonwealth. If the required audit discloses weaknesses, Medical Assistance Services should implement compensating controls to mitigate the risk to the Commonwealth until the service provider corrects the deficiency.

Improve Third-Party Oversight Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Medical Assistance Services has made progress to document and implement a formal process for maintaining oversight for three of its IT third-party service providers that manage and support the Medicaid management system. However, Medical Assistance Services continues to not verify that one of its three service providers performs two controls as required by the Hosted Environment Security Standard. We communicated the two weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

VITA's Enterprise Cloud Oversight Service (ECOS) confirms the two controls as part of its service for two of the three service providers; however, ECOS does not review the third service provider, and it is Medical Assistance Services' responsibility to verify the provider performs the required controls. Medical Assistance Services did not ensure the individuals responsible for monitoring the service providers are confirming these specific controls and processes within the required timeframe. Without maintaining appropriate oversight of its service providers, Medical Assistance Services cannot validate whether its service providers implement the required security controls to protect the agency's sensitive and mission-critical data.

Medical Assistance Services should improve its process by ensuring individuals tasked with monitoring service providers confirm the controls per the Hosted Environment Security Standard. Medical Assistance Services should ensure the individuals responsible for monitoring service providers implement and consistently perform formal oversight processes in a timely manner, which will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

Perform Annual System Access Reviews
Type: Internal Control and Compliance
Severity: Significant Deficiency

Medical Assistance Services has not performed an annual access review for two of three user groups of the claims processing module of the Medicaid management system since June 2022. Medical Assistance Services completed an annual access review of Medical Assistance Services' employees but did not perform an annual review of the Social Services' and contractors' user groups. The Social Services and contractor user groups represent almost ninety percent of the total users of the system.

The Security Standard, Section 8.1 AC-2, requires the agency to review accounts for compliance with account management requirements on an annual basis. Medical Assistance Services encountered issues after the implementation of the Medicaid management system including lack of staff and budgetary constraints, causing management to defer the review process.

By not reviewing access on an annual basis, Medical Assistance Services cannot verify that each user's access is appropriate based on job functions; does not violate the principles of least privilege or separation of duties; and is configured appropriately. Lack of an annual access review increases the risk that a user retains inappropriate access, which could lead to unauthorized access to sensitive information. Medical Assistance Services should perform an annual review of Social Services' and contractors' access to identify unnecessary access due to terminations or changes in responsibilities.

Improve Information Security Program and IT Governance

Type: Internal Control and Compliance
Severity: Material Weakness
First Issued: Fiscal Year 2022

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 information technology resources to ensure its information security program effectively protects sensitive Commonwealth data in accordance with the Security Standard.

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 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 control weaknesses described in the communication marked FOIAE are the result of Social Services not assessing information security requirements prior to project implementation and prioritizing information security within the IT environment. Social Services has hindered its ability to consistently and timely remediate findings from management recommendations issued throughout prior year audits and bring the information security program in compliance with the Security Standard by not dedicating the necessary IT resources to information security. Not prioritizing information technology 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. Because of the scope of this matter and the magnitude of Social Services' information system security responsibilities, we consider these weaknesses collectively to create a material weakness in internal controls over compliance.

In July 2023, the Governor appointed a Chief Deputy Commissioner, who is responsible for overseeing Social Services' information technology and security functions. 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 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
First Issued: Fiscal Year 2018

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. 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 fiscal year 2023, Social Services disbursed approximately $619 million in federal funds through roughly 5,400 subawards from 35 federal grant programs. During the audit, we noted the following deviations from the Agency Monitoring Plan:

- While Compliance has updated and finalized the Agency Monitoring Plan, it has not communicated it to Subrecipient Monitoring Coordinators in divisions with subrecipient monitoring responsibilities. 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 did not consider this requirement because Compliance did not communicate the Agency Monitoring Plan to Subrecipient Monitoring Coordinators. The Local Review Team did, however, implement a risk-based approach to monitoring subrecipients as required by the Agency Monitoring Plan.

- Compliance continues to not review division monitoring plans to ensure the divisions implement 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. Because of the lack of review, the Division of Benefit Programs' (Benefit Programs) fiscal year 2023 monitoring plan did not meet all the requirements outlined in the Agency Monitoring Plan because it did not include a risk-based approach for subrecipient monitoring and did not consider all subrecipients who receive funding from the Temporary Assistance for Needy Families (TANF) federal grant program. Additionally, while the Office of New Americans has adequate subrecipient monitoring processes, it does not have a written monitoring plan as required by the Agency Monitoring Plan.

- Compliance continues to not analyze each division's subrecipient monitoring activities. 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 Compliance's lack of analysis and communication, the Executive Team was unaware of the deviations noted above.

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. Without performing the responsibilities in the Agency Monitoring Plan, Social Services cannot provide reasonable assurance that the agency has complied with pass-through entity federal requirements at 2 CFR § 200.332. Because of the scope of this matter and the magnitude of Social Services' subrecipient monitoring responsibilities, we consider these weaknesses collectively to create a material weakness in internal control over compliance.

Since the prior audit, Compliance and Social Services' Executive Team have worked together to discuss solutions to address this audit finding. Social Services is considering procuring a grants management system and Compliance has worked with the agency's Division of Information Technology to determine whether it can utilize this system to fulfil its subrecipient monitoring responsibilities. Compliance has also discussed the need for additional staff to assist with subrecipient monitoring oversight with the Executive Team. However, Compliance has not implemented these corrective actions as of the end of fiscal year 2023 because of the level of effort and considerations involved with these corrective actions. Therefore, Compliance should continue to work with the Executive Team to make sure that it has the appropriate level of resources to fulfil its responsibilities in the Agency Monitoring Plan.

Implement Internal Controls over TANF Federal Performance Reporting
Type: Internal Control and Compliance
Severity: Material Weakness
First Issued: Fiscal Year 2022

Benefit Programs does not have adequate internal controls in place to ensure accurate reporting in 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). ACF requires Social Services to submit this data to ACF quarterly, and ACF uses the data 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 to produce and submit 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 other supporting data and Benefit Programs did not detect or correct these errors before the service provider submitted the data to ACF:

- Benefit Programs did not confirm that the reported information agreed to supporting data for three out of six (50%) of the "Total Number of TANF Families" key line items tested during the audit.

- Benefit Programs did not confirm that the reported information agreed to supporting data for two out of six (33%) of the "Total Number of SSP-MOE Families" key line items tested during the audit.

- Benefit Programs did not accurately report on the "Receives Subsidized Child Care" key line item for 14 out of 120 (12%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Number of Months Countable Toward Federal Time Clock" for six out of 120 (5%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Unsubsidized Employment" key line item for five out of 120 (4%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Work Participation Status" key line item for five out of 120 (4%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Hours of Participation" key line item for four out of 120 (3%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Work Eligible Individual Indicator" key line item for one out of 120 (<1%) cases tested during the audit.

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 federal grant program. In addition, ACF can impose a penalty if it finds Social Services did not meet statutory required work participation rates.

Since the prior audit, Benefit Programs has worked with its service provider to analyze the reporting errors to determine the cause and appropriate actions to resolve these errors. However, because of its ongoing efforts to analyze and correct the reporting errors, Benefit Programs continues to rely on the error correction controls of the ACF, performed after report submission, and has not developed and implemented its own internal controls to obtain assurance over the accuracy of the data included within the service provider's submissions. Because of the scope of this matter and errors noted above, we consider it to be a material weakness in internal control. Additionally, we believe this matter represents material noncompliance since Social Services did not fully comply with the provisions at 45 CFR § 265.7(b).

Benefit Programs should implement internal controls over the TANF performance reporting process and include a documented secondary review process of the service provider's data. Benefit Programs should complete this review prior to the report submission to ensure accurate reporting of TANF work participation data to ACF in accordance with the ACF-199 and ACF-209 reporting instructions.

Obtain Reasonable Assurance over Contractor Compliance with Program Regulations
Type: Internal Control and Compliance
Severity: Material Weakness

Social Services cannot provide reasonable assurance that its contractor administered the Low-Income Household Water Assistance Program (LIHWAP) in compliance with federal statutes, regulations, and the terms and conditions of the federal award. Reasonable assurance is a high, but not absolute, level of assurance that the entity and its contractors have complied with federal laws and regulations.

The United States Department of Health and Human Services awarded approximately $25 million to Social Services to administer the LIHWAP federal grant program. The objective of the LIHWAP federal grant program is to meet unprecedented water services needs that arose during the COVID-19 pandemic and provide quick intervention to help the people facing high water or wastewater costs compared to their income in resuming and/or maintaining their home water or wastewater services.

Social Services partnered with a for-profit contractor to administer the program on its behalf due to resource limitations and the need to provide this assistance to individuals as quickly as possible. Through its contractual agreement, Social Services assumed ultimate responsibility for program compliance and incorporated certain measures into its contractual agreement to maintain compliance with federal laws and regulations. Specifically, Social Services was to agree on performance self-assessment criteria with the contractor within 30 calendar days of the execution of the project start date, then have the contractor prepare a monthly self-assessment to report on such criteria. Social Services then had ten business days, after the receipt of the contractor's self-assessment, to audit the results of the contractor's service level obligations and performance requirements and discuss any discrepancies with the contractor to determine if invoice or payment adjustments were necessary.

Because of the fast-paced nature of the program and the need to provide the assistance to individuals as quickly as possible, Social Services was unable to agree on the performance criteria with the contractor. As a result, Social Services did not receive the monthly self-assessments from the contractor and audit them in accordance with the contractual agreement. While Social Services did have on-going discussions with the contractor about program compliance and did perform periodic reviews of applicant records, these reviews did not follow a systematic process that provides reasonable assurance over the contractor's compliance with program regulations.

Title 2 CFR § 200.501(g) states that the auditee is responsible for reviewing the contractor's records to determine program compliance. Additionally, 2 CFR § 200.303(a) states that non-federal entities 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. Since Social Services has not implemented the contractual provisions related to the vendor's self-assessment reporting and performance auditing, we are unable to audit Social Services' compliance for the LIHWAP federal grant program and must disclaim an opinion on compliance for the program in the Commonwealth's Single Audit report. We also believe this matter represents a material weakness in internal control over

compliance because there is a reasonable possibility that material noncompliance with a compliance requirement will not be prevented, or detected and corrected, on a timely basis.

The contract between Social Services and the contractor ends on December 31, 2023. Thereafter, the contractor will transfer program records to Social Services within the subsequent months. Social Services has until June 2024 to close out the LIHWAP federal grant program and should fulfill its responsibilities for auditing the contractor's records for compliance before it closes the LIHWAP grant with the United States Department of Health and Human Services. Therefore, Social Services should implement an audit process that provides reasonable assurance that the contractor administered the LIHWAP federal grant program in accordance with federal statutes, regulations, and the terms and conditions of the federal award before it closes the grant award. Additionally, Social Services' Executive Team should oversee the implementation of the audit process.

Continue Improving IT Risk Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: 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. As a result, Social Services does not complete various IT risk management documentation nor maintain an accurate list of sensitive systems. IT risk management documentation identifies the types of data stored and processed within its environment, the sensitivity classification of that data, potential risks and threats to the systems, and risk mitigating controls that Social Services should implement.

Since we first issued this finding in 2018, Social Services has made progress to remediate the issues identified. However, Social Services continues to not comply with the following Security Standard requirements:

- Social Services does not verify and validate the data and system sensitivity ratings of its systems to ensure proper IT system sensitivity ratings. Social Services' systems list includes 89 systems. Social Services classifies 77 of the 89 systems (87%) as sensitive systems based on the sensitive data handled by each system. Social Services classifies four of the 89 systems (4%) as nonsensitive systems. Social Services does not rate eight of the 89 systems (9%). However, five of the eight unrated systems transmit, process, or store sensitive data sets or support critical business processes and therefore, Social Services should consider these to be sensitive systems. The remaining three of the eight unrated systems do not transmit, process, or store sensitive data sets or support critical business processes and therefore Social Services should consider these nonsensitive systems. The Security Standard defines sensitive systems as systems that transmit, process, or store sensitive data sets or support sensitive business processes. Without a process to maintain an updated sensitive systems list and verify and validate IT system and data sensitivity, Social Services increases the risk of not properly defining all sensitive systems within its IT environment. Failure to identify sensitive systems increases the likelihood of Social Services inadequately addressing risks, vulnerabilities, and

remediation techniques necessary to protect sensitive IT systems and data. (*Security Standard, Section 4.2.6 IT System and Data Sensitivity Classification*)

- Social Services does not create or annually review risk assessments and system security plans (SSP) for every sensitive system. Social Services' systems list indicates 77 systems classified as sensitive systems, and the systems list includes five additional systems without a sensitivity classification that process and store sensitive data and therefore should be classified as sensitive systems. Several of these systems have no or only partial risk assessment and SSP documentation. Specifically:

  - Risk assessment documentation does not exist for 64 (78%) systems.

  - Annual review documentation does not exist for 82 (100%) of the existing risk assessments.

  - SSP documentation does not exist for 45 (55%) systems.

  - Annual review documentation does not exist for 82 (100%) of the existing SSPs.

- The Security Standard requires the agency to conduct and document a risk assessment for each IT system classified as a sensitive system at least once every three years. The Security Standard also requires the agency to develop and distribute to appropriate organization-defined personnel a security plan for the information system. Without completing risk assessments and SSPs for all sensitive systems, Social Services may not appropriately secure its systems against known vulnerabilities that can affect the confidentiality, integrity, and availability of sensitive and mission-critical data. (*Security Standard, Sections 6.2 Risk Assessment Requirements, RA-3 Risk Assessment and PL-2 System Security Plan)*.

- The Security Standard requires Social Services to review, and update completed risk assessments annually or when changes occur that may impact the security state of the system, and to review and update each SSP on an annual basis or more frequently to address environmental changes. Without conducting an annual review and update of the risk assessment and SSP for each IT system classified as sensitive, Social Services may not adequately secure its sensitive systems against new vulnerabilities that can affect data confidentiality, integrity, and availability. (*Security Standard, Sections RA-3 Risk Assessment and PL-2 System Security Plan*)

- Social Services does not implement corrective actions to mitigate risks in its sensitive systems' risk assessments. The Security Standard requires Social Services to prepare a report of each risk assessment that includes major findings and risk mitigation efforts (*Security Standard, Section 6.2.3 Risk Assessment*). While Social Services documents a list of risk remediation plans and a schedule within its risk assessments, Social Services does not have a process to establish effective corrective action plans to mitigate findings identified during the risk assessments. Without properly establishing and implementing corrective actions, Social

Services opens its systems to possible risks and vulnerabilities that could compromise the agency's sensitive information.

Without documenting risk management information for all its sensitive systems and reviewing the documentation at least annually, Social Services may not consistently and effectively manage its IT risk management program. An effective IT risk management program is essential to help protect IT systems and data from potential risks. Specifically, Social Services cannot prioritize information security controls to implement or determine if proper information security controls are in place. Ineffective security controls could lead to a breach of data or unauthorized access to sensitive and confidential data.

Social Services' Information Security Risk Management (ISRM) oversees the risk management program on behalf of business owners and hired an IT Risk Manager in 2020. ISRM has prioritized completing risk assessments and SSPs for new systems; however, due to the magnitude of the project, ISRM has not yet completed the project. Additionally, the risk assessment requirements documented in the risk assessment policy and the risk assessment process documented in the risk assessment procedure do not align, which contributed to Social Services not consistently completing risk management documentation due to conflicting roles and responsibilities.

Social Services should develop a plan and prioritize resources to complete risk management documentation for its sensitive systems and review those documents annually to validate that the information reflects the current environment. Additionally, Social Services should implement security controls to mitigate the risks and vulnerabilities identified in its risk assessments. Improving the IT risk management program will help to ensure the confidentiality, integrity, and availability of the agency's sensitive systems and mission essential functions.

Continue Developing Record Retention Requirements and Processes for Electronic Records

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2018

Social Services continues to operate without an adequate data retention process that ensures consistent compliance with retention requirements for its case management system and adherence to federal regulations and the Code of Virginia. Specifically, Social Services does not have data retention policies and procedures that define its requirements and processes to consistently ensure data retention compliance and destruction. Social Services' case management system stores several types of federal benefit program records with varying retention requirements supporting ten programs and services, such as Medicaid, TANF, and the Supplemental Nutrition Assistance Program (SNAP). Social Services' case management system authorized over $17 billion in public assistance payments to beneficiaries from these federal programs during fiscal year 2023.

Since fiscal year 2019, Social Services gathered retention requirements from the business divisions that support the federal programs and services. In fiscal year 2022, Social Services finalized and documented policies with retention requirements for the data sets handled by each of the ten programs and services supported by its case management system. However, Social Services has not developed,

documented, and implemented procedures and processes to operationalize the records retention policies for each of the programs and services to ensure consistent retention and destruction of records in compliance with regulations and laws.

Title 45 CFR § 155.1210, governs record retention for Medicaid and requires state agencies to maintain records for ten years. Additionally, the Virginia Public Records Act outlined in § 42.1-91 of the Code of Virginia makes an agency responsible for ensuring that it preserves, maintains, and makes accessible public 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. Furthermore, the Virginia Public Records Act in § 42.1-86.1 of the Code of Virginia details requirements for the disposition of records including that records created after July 1, 2006, and authorized to be destroyed or discarded, must be discarded in a timely manner and in accordance with the provisions of Chapter 7 of the Virginia Public Records Act. Records that contain identifying information as defined by subsection C of § 18.2-186.3 of the Code of Virginia shall be destroyed within six months of the expiration of the records retention period. Finally, the Security Standard requires agencies to implement backup and restoration plans that address the retention of the data in accordance with the records retention policy for every IT system identified as sensitive relative to availability (*Security Standard, Section CP-9-COV Information System Backup*).

Without implementing records retention requirements, Social Services increases the risk of a data or privacy breach. Additionally, destroying documents that should be available for business processes or audit, or keeping data longer than stated, could expose Social Services to fines, penalties, or other legal consequences. Further, Social Services may not be able to ensure that backup and restoration efforts will provide mission essential information according to recovery times. Finally, Social Services spends additional resources to maintain, back up, and protect information that no longer serves a business purpose.

Social Services determined that the retention requirements for all ten programs and services supported by its case management system are not feasible as a single release due to the risk and complexity of the project, as well as changes to federal requirements, since its initial analysis. Therefore, Social Services plans to use a phased delivery approach including multiple releases, beginning with Release 1 in February 2024. Further, Social Services is working on a revised timeline to complete each additional phase for the remaining releases.

Social Services should continue to develop and implement records retention procedures that define its requirements and processes to ensure that consistent records retention processes can be operationalized across business divisions to comply with applicable with laws and regulations.

Improve Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2019

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

Lacking and insufficient procedures and processes to manage the web application contributed to the five weaknesses outlined in the separate FOIAE document. Additionally, Social Services prioritizing other projects also contributed to the weaknesses persisting. Not configuring web applications in accordance with the Security Standard increases the risk of successful cyberattack, exploit, and data breach by malicious parties.

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. Proper configuration of the web application will help Social Services to protect its sensitive and mission-critical data.

Continue Improving IT Change and Configuration Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: 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. The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data.

Social Services' 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. Not aligning IT change management processes with the Security Standard increases the risk of 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.

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.

Upgrade End-of-Life Technology

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Social Services uses end-of-life (EOL) technologies in its IT environment and maintains technologies that support mission-essential data on IT systems running software 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 agencies from using software that is EOL 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. Using EOL technologies increases 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. Dedicating the necessary resources to minimize the use of EOL technologies will help to ensure that Social Services secures its IT environment and systems to protect its sensitive and mission critical data.

Conduct Information Technology Security Audits

Type: Internal Control and Compliance
Severity: Significant Deficiency

Social Services does not conduct a comprehensive IT security audit on each sensitive system at least once every three years that assesses whether IT security controls are adequate and effective. Specifically, Social Services has not conducted an IT security audit in the last three years over 29 of the 70 sensitive systems (41%) due for an IT security audit.

The Security Standard, Section 7, requires that each IT system classified as a sensitive system undergo an IT security audit as required by and in accordance with the current version of the IT Audit Standard. The IT Audit Standard, Section 1.4, requires that IT systems containing sensitive data, or

systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall 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, assesses the effectiveness of the system controls and measures compliance with the applicable requirements of the Security Standard.

Social Services does not have an internal audit function but does employ an IT Audit Manager. However, any audits conducted by the IT Audit Manager cannot be peer reviewed due to Social Services not having an internal audit function or Chief Audit Executive, and thus, these audits do not meet Government Auditing Standards requirements. Therefore, Social Services procures an external auditor to complete all the required IT Security Audits using funds allocated from the Virginia General Assembly, as well as funds allocated to Information Technology Services. Social Services tasks the IT Audit Manager with coordinating the audits and tracking Social Services' remediation of audit findings. However, the IT Audit Manager relies on the collaboration of the business divisions, Information Technology Services, and Information Security Risk Management, as well as the oversight of the Executive Team to effectively schedule and conduct the audits. Social Services did not perform the IT security audits in accordance with the Security Standard because of a lack of governance over IT security.

Without conducting full IT security audits that cover all applicable Security Standard requirements for each sensitive system every three years, Social Services increases the risk that IT staff will not detect and mitigate existing weaknesses. Malicious parties taking advantage of continued weaknesses could compromise sensitive and confidential data. Further, such security incidents could lead to mission-critical systems being unavailable.

Social Services should evaluate potential options and develop a formal process for conducting IT audits over each sensitive system at least once every three years that tests the effectiveness of the IT security controls and compliance with Security Standard requirements. Social Services should then complete the planned IT security audits and implement adequate governance processes to ensure it is meeting the Security Standard requirements. Compliance with the IT Audit Standard will help to ensure the confidentiality, integrity, and availability of sensitive and mission-critical data.

Monitor Internal Controls to Ensure Timely Removal of System Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2018

Social Services continues to implement internal controls to monitor the timely removal of system access. The Security Standard, Section PS-4, requires the organization to disable information system access within 24 hours of employment termination. In prior audits, we identified instances where Social Services did not remove separated employee access in accordance with the Security Standard.

In response to the prior audit recommendations, Social Services formed an agency-wide working group to determine the exact processes needed to implement the internal controls necessary to address the audit recommendations. Additionally, Social Services' ISRM function and the Division of Human

Resources (Human Resources) have worked together to discuss implementing new reporting and interface processes between its internal human resources system and the Commonwealth's human resources system. However, because of the extent of its corrective actions, Social Services was not able to implement all of them by the end of fiscal year 2023.

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 potential financial liabilities should its information become compromised. Therefore, Social Services should continue its corrective action efforts to implement internal controls to monitor the timely removal of system access.

Improve Documentation for Separation of Duty Conflicts

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Social Services' Division of Finance (Finance) continues to lack written documentation for users to justify and authorize conflicting access to its financial accounting and reporting system (financial system) as of the end of fiscal year 2023. Since the prior year's audit, Finance has developed additional internal controls to document and authorize conflicting access in its financial system including creating a conflicting responsibilities report to monitor user accounts with separation of duty conflicts and updating its access request form to provide only temporary access for users with separation of duty conflicts and including a justification field in the form that requires the Chief Financial Officer's approval. However, Finance did not implement these internal controls as of the end of fiscal year 2023 because of the time needed to create and implement these additional resources.

The Security Standard, Section 8.1 AC-6, requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks. 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. When improper separation of duties exists, there is an increased risk that users can perform unauthorized transactions in the financial system. Approval of the separation of duty concerns and adequate compensating controls provides accountability and assurance that Finance is properly considering the risks of granting such access to the financial system.

Finance should continue to develop and implement its corrective actions and monitor them to ensure that they are operationally effective. By implementing these corrective actions and monitoring them, Social Services will be able to provide reasonable assurance that it adequately safeguards its financial system in accordance with the Security Standard.

Evaluate Separation of Duty Conflicts within the Case Management System
Type: Internal Control and Compliance
Severity: Significant Deficiency

Social Services has not performed nor documented a conflicting access review for its case management system to identify the combination of roles that could pose a separation of duties conflict and ensure compensating controls are in place to mitigate risks arising from those conflicts. Social Services uses the case management system to determine applicant eligibility and authorize benefit payments for the Medicaid Cluster, Child Care and Development Fund Cluster, SNAP Cluster, TANF, and Low-Income Household Energy Assistance (LIHEA) federal grant programs. Social Services' case management system authorized over $17 billion in public assistance payments to beneficiaries from these federal programs during fiscal year 2023.

The Security Standard, Section 8.1 AC-5, 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. Social Services, in collaboration with its service provider, has documented role-based security access. However, due to lack of management oversight, the documentation did not include a review of conflicting role access and Social Services has not properly updated the documentation even though the case management system has undergone multiple changes and upgrades since its initial release over ten years ago. By not performing and documenting a conflicting access review, Social Services does not know which combinations of roles pose a separation of duties conflict and could potentially create opportunities for users to exploit vulnerabilities in the case management system.

Social Services should perform and document a conflicting access review for the case management system to identify the combinations of roles that could pose separation of duties conflicts and ensure compensating controls are in place to mitigate risks arising from those conflicts. Additionally, Social Services should update the role-based security access documentation to reflect all system changes from prior case management system related releases.

Perform Annual Review of Case Management System Access
Type: Internal Control and Compliance
Severity: Significant Deficiency

Social Services did not perform the required annual access review for its case management system during fiscal year 2023. Social Services uses the case management system to determine applicant eligibility and authorize benefit payments for the Medicaid Cluster, Child Care and Development Fund Cluster, SNAP Cluster, TANF, and LIHEA federal grant programs. Social Services' case management system authorized over $17 billion in public assistance payments to beneficiaries from these federal programs during fiscal year 2023.

The Security Standard, Section 8.1 AC-2(j), requires the agency to review accounts for compliance with account management on an annual basis. Additionally, Social Services' policies and procedures require an annual review of user accounts to verify access privileges of active employees for every role-

based access system and this review must be completed within 364 days of the last completion of access review. The annual access review for the case management system was not performed during fiscal year 2023 due to staff turnover. By not performing this annual access review, Social Services increases the risk of improper or unnecessary access to sensitive systems, which could result in a breach in data security. Social Services should perform an annual access review of user accounts for the case management system as required by the Security Standard and the agency's policies and procedures.

Review Non-Locality Subrecipient Single Audit Reports

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2018

Compliance continues to not review non-locality subrecipient Single Audit reports as established within the Agency Monitoring Plan. Non-locality subrecipients are subrecipients who are not local governments and are mainly comprised of non-profit organizations. During fiscal year 2023, Social Services disbursed approximately $87 million in federal funds to roughly 205 non-locality subrecipients. While reviewing the audit reports for the 26 non-locality subrecipients that received more than $750,000 in federal funds from Social Services, we noted the following:

- Seven non-locality subrecipients (27%) did not have a Single Audit report available in the Federal Audit Clearinghouse (Clearinghouse) for the most recent audit period. Social Services disbursed approximately $10 million in federal funds to these entities during fiscal year 2023.

- A non-locality subrecipient (4%) had audit findings that affected one of Social Services' federal grant programs. As a result of the lack of review over the non-locality subrecipient's Single Audit report, Social Services did not issue a management decision within six months of acceptance of the audit report by the Clearinghouse.

According to 2 CFR § 200.332(f), all pass-through entities must verify their subrecipients are audited if it is expected that the 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 a management decision within six months of acceptance of the audit report by the Clearinghouse. A management decision is Social Services' written determination, provided to its subrecipient, of the adequacy of the subrecipient's proposed corrective actions to address the audit findings, based on Social Services' evaluation of the audit findings and proposed corrective actions.

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

In its corrective action plan as of the end of fiscal year 2023, Compliance indicated that it has worked with Social Services' Executive Team to put forth a budget request to procure a grants management system to assist with its subrecipient monitoring efforts. Additionally, Compliance is

considering implementing a manual system where it will review non-locality Single Audit reports until it implements a permanent solution. However, Compliance was unable to procure a grants management system to support its subrecipient monitoring efforts during the fiscal year and it did not implement a manual system to comply with the requirements in 2 CFR § 200.332(d)(3) and (f) because of a lack of available resources.

Compliance should continue to work with Social Services' Executive Team to determine which solution(s) would be the most beneficial to the organization to comply with these federal requirements. Additionally, Compliance should consider using the query functionalities in the Clearinghouse to determine whether any of its non-locality subrecipients have audit findings that warrant a management decision.

Communicate Responsibilities to Subrecipient Monitoring Coordinators

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2020
Prior Title: Finalize the Agency Monitoring Plan and Communicate Responsibilities to Subrecipient Monitoring Coordinators

Compliance has not communicated responsibilities to subrecipient monitoring coordinators, as required by the Agency Monitoring Plan. Compliance's Agency Monitoring Plan serves as a guide in the development, implementation, and coordination of division monitoring plans and aims to address accountability and provide consistency in monitoring activities across all Social Services' divisions and offices. During fiscal year 2023, Social Services disbursed approximately $619 million in federal funds from roughly 5,400 subawards.

Title 2 CFR § 200.332(d) requires pass-through entities to monitor the activities of subrecipients as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Further, 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.

Since the prior audit, Compliance has updated and finalized the Agency Monitoring Plan but has been unable to communicate it to the subrecipient monitoring coordinators because of a lack of available resources. Without communicating responsibilities to subrecipient monitoring coordinators, 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 should continue to work with Social Services' Executive Team to obtain the appropriate resources so that it can communicate responsibilities to subrecipient monitoring coordinators.

Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

Benefit Programs did not evaluate subrecipients' risk of noncompliance with federal regulations related to the administration of the TANF federal grant program and the Medicaid Cluster during fiscal year 2023. Benefit Programs only considered the size of the subrecipient when determining the extent of monitoring necessary. Social Services disbursed approximately $178 million to roughly 270 subrecipients from these federal programs during the period under review.

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, the subrecipient's prior experience with the same or similar subawards, and whether the subrecipient has new personnel or new or substantially changed systems. 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.

As part of its corrective action, Benefit Programs created a new monitoring plan in April 2023 that includes a risk assessment tool that conforms with federal regulations. However, Benefit Programs did not place the new risk assessment tool into operation until after fiscal year 2023 because of the communication and training that needed to occur on the new monitoring plan. Benefit Programs should continue its corrective action efforts and confirm that program consultants are completing the risk assessment tool properly.

Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Benefit Programs fiscal year 2023 monitoring plan did 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.

According to 2 CFR § 200.322(b) all pass-through entities are required to evaluate each subrecipient's risk of noncompliance with federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring. Additionally, 2 CFR § 200.332(d) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure it uses the subaward for authorized purposes, which comply with federal statutes,

regulations, and the terms and conditions of the subaward; and that the subrecipient achieves subaward performance goals. Without including all 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.

In response to the prior year's audit recommendation, Benefit Programs' management analyzed all its programmatic activities and verified that they were incorporated into its fiscal year 2024 monitoring plan. As part of its corrective action, Benefit Programs' management mandated that home office staff monitor subrecipients receiving TANF competitive grants once every three years and complete risk assessment procedures in other years to verify that there have not been any changes in the subrecipient's risk profile. Benefit Programs was unable to fully implement corrective action in fiscal year 2023 because of the efforts involved with creating and implementing a new monitoring plan and dedicating the resources to provide proper oversight. Benefit Programs should continue its corrective action efforts to confirm that it includes all programmatic activities within its monitoring plan and that it conducts monitoring activities in accordance with the monitoring plan.

Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Benefit Programs did not oversee subrecipient monitoring activities to ensure they were conducted in accordance with its monitoring plan. During fiscal year 2023, Benefit Programs disbursed approximately $173 million in subaward payments from the TANF federal grant program and Medicaid Cluster. During the audit, we noted the following deviations from Benefit Programs' monitoring plan:

- Benefit Programs created a monitoring plan for fiscal year 2023 to comply with Compliance's Plan. Regional consultants, who perform subrecipient monitoring activities, created their own subrecipient monitoring schedules that were not consistent with Benefit Programs' monitoring plan. As a result, Benefit Programs only completed 35 of the 63 (56%) scheduled reviews for the TANF federal grant program and Medicaid Cluster. Regional consultants completed 28 additional reviews which Benefit Program did not originally included in its monitoring plan.

- Benefit Programs did not confirm that fiscal year 2023 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.

Title 2 CFR § 200.332(d) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure that it uses the subaward authorized purposes, which are in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Without confirming that monitoring activities are conducted in accordance with the monitoring plan, Benefit Programs cannot provide assurance that it complied with the provisions at 2 CFR § 200.332(d).

In response to the prior year's audit recommendation, Benefit Programs created a new monitoring plan in April 2023 to address the deficiencies noted above. As part of its corrective action, Benefit Programs' subrecipient monitoring coordinator will be responsible for tracking regional consultants' monitoring activities, verifying that all relevant monitoring documents are uploaded to its data repository, creating desk tools for regional consultants, and providing training on the new monitoring plan. Benefit Programs was unable to fully implement corrective action in fiscal year 2023 because of the efforts involved with creating and implementing a new monitoring plan and dedicating the resources to provide proper oversight. Benefit Programs should continue its corrective action efforts to confirm that monitoring activities are conducted in accordance with the monitoring plan.

Monitor Case Management System Records to Ensure Compliance with TANF Eligibility Requirements

Type: Internal Control and Compliance
Severity: Significant Deficiency

Social Services did not comply with certain federal eligibility requirements for the TANF federal grant program, resulting in known questioned costs of $12,275. The TANF federal grant program provided over $120 million in assistance to approximately 28,000 needy families during fiscal year 2023. During the audit, we reperformed the eligibility determinations for all needy families that received assistance during the fiscal year and identified 30 instances (<1%) where the facts in the recipient's case record did not support the eligibility determination. Specifically:

- For sixteen payments, staff did not properly assign to the state the rights the family member may have for child support. In 12 instances, Social Services underpaid benefit amounts to recipients, and in two instances, Social Services improperly denied benefits to the recipient due to manually entering child support payments beyond the acceptable timeframe. Staff incorrectly keyed the remaining two instances into the system but did not result in an adverse financial effect to the recipient or Social Services. Title 42 United States Code (USC) 608(a)(3) mandates that the State shall require that, as a condition of providing assistance, a member of the family assigned to the state the rights the family member may have for support from any other person and this assignment may not exceed the amount of assistance provided by the State.

- For eight payments, staff did not properly evaluate the income eligibility. Title 45 CFR § 263.2(b)(2) defines financially "needy" as financially eligible according to the state's quantified income and resource criteria, which Social Services quantifies through its TANF Manual as maximum income charts in Section 305, Appendix 1.

- For two payments, staff did not properly evaluate the extended absence of a child or adult to determine the effect on household eligibility. Title 42 USC 608(a)(10) mandates that a state may not provide assistance to an individual who is a parent (or other caretaker relative) of a minor child who fails to notify the state agency of the absence of the minor child from the

home within five days of the date that it becomes clear to that individual that the child will be absent for the specified period of time.

- Staff did not properly reduce or terminate two payments for individuals not complying with the Commonwealth's work requirements for TANF recipients. Title 45 CFR §261.13 mandates that if an individual in a family receiving assistance refuses to engage in required work without good cause, a state must reduce assistance to the family, at least pro rata, with respect to any period during the month in which the individual refuses or may terminate assistance.

- Staff did not properly evaluate the qualified alien status for one payment as required by 8 USC § 1611.

- One recipient had a failed eligibility determination yet received a payment from the case management system. Title 45 CFR § 206.10(a)(8) requires that each decision regarding eligibility or ineligibility to be supported by facts in the applicant's or recipient's case record.

Social Services relies on its case management system to properly determine eligibility, correctly calculate benefits payments, and achieve the federal requirements of the TANF federal grant program. Of the exceptions noted above, 16 of the 30 (53%) were the result of local agency eligibility workers mistakenly reporting child support payments as unearned revenue beyond the acceptable timeframe instead of assigning these payments to the Commonwealth for referral to the Division of Child Support Enforcement, as required by the CFR. The remaining 14 exceptions (47%) resulted from local agency eligibility workers manually overriding the eligibility determination made by the case management system and not including sufficient documentation to justify the rationale for the override. Social Services provides local agency eligibility workers with elevated access to the case management system so they can exercise their judgement during the applicant intake process. However, Social Services does not appear to monitor the use of manual overrides to ensure they are documented appropriately and that local agency eligibility workers are not using them excessively. In effect, Social Services places itself at risk of having to repay grant funds to the federal government if it does not comply with federal laws and regulations.

Social Services should provide additional training to local agency eligibility workers on how to properly determine and document eligibility determinations in the case management system. Additionally, Social Services should consider monitoring local agency eligibility worker's use of manual overrides to confirm that they properly document eligibility determinations in the case management system. By providing additional training and implementing additional internal controls, Social Services will be able to ensure that sufficient documentation supports each eligibility decision in its case management system in the applicant's or recipient's case record.

Implement Internal Controls over TANF Federal Special Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency

Benefit Programs does not have adequate internal controls in place to ensure reasonably accurate reporting in the ACF Annual Report on State Maintenance-of-Effort (MOE) Programs (ACF-204) for the TANF federal grant program. ACF requires Social Services to submit this data to ACF annually and ACF uses this information in reports to Congress about how TANF programs are evolving, in assessing State and Territory MOE expenditures, and in assessing the need for legislative changes. During our review, we identified the following:

- Benefit Programs could not produce evidence to support a reasonable estimate for four out of six (66%) of the "Total number of families served under the program with MOE funds" key line items.

- Benefit Programs appeared to use an estimation process that did not have a sound basis for two out of six (33%) of the "Total number of families served under the program with MOE funds" key line items.

Title 2 CFR § 200.303(a) requires the non-federal entity 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. Further, 45 CFR § 75.361 requires that financial records, supporting documents, statistical records, and all other non-federal entity records pertinent to a federal award must be retained for a period of three years from the date of submission.

The ACF-204 Reporting Instructions allow states the flexibility to use reasonable estimates with a sound basis when actual numbers are not available. However, Benefit Programs has not dedicated the resources to implement appropriate internal controls and document its estimation and retention processes to demonstrate that it uses reasonable estimates with a sound basis to support the amounts reported in the ACF-204 report. Reporting potentially inaccurate information prevents the ACF from adequately monitoring Social Services' MOE programs and the overall performance for the TANF federal grant program. Therefore, Benefit Programs should dedicate the necessary resources to implement internal controls over the TANF special reporting process and include documented estimation and retention processes to ensure reasonably accurate reporting of TANF MOE Programs to ACF in accordance with the ACF-204 reporting instructions.

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

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

Social Services continues to not have sufficient internal controls over System and Organization Controls (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 service providers' 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 did not obtain, review, or document its review of service provider SOC reports to identify deficiencies or determine whether the reports provided adequate coverage over operations during state fiscal year 2023.

The 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 ECOS based on the type of SOC report. VITA obtains and reviews SOC 2 reports, which provide information on controls at service providers relevant to information system security, availability, processing integrity, and confidentiality or privacy. SOC 1 reports provide information on controls at the service providers relevant to Social Services' internal control over financial reporting. Designated staff in Social Services programmatic areas, who the service provider's services affect, should obtain and review SOC 1, Type 2 reports. Designated staff should communicate any complementary user entity controls to the Agency Risk Management and Internal Controls Standards (ARMICS) coordinator to ensure Social Services has properly designed and implemented the relevant controls. Additionally, designated staff should document their review of the SOC 1, Type 2 reports, noting if there were any deviations in controls, perform a review of the service provider management's response to any exceptions noted, and document Social Services' consideration of the significance of any deviations and their impact on Social Services' operations.

Social Services did not assign responsibility to a resource within the agency, knowledgeable of SOC reporting requirements, to develop an agency-wide policy to communicate expectations related to

obtaining, reviewing, and documenting SOC 1, Type 2 reports for agency personnel to use when carrying out their programmatic responsibilities. As a result, the individuals responsible for obtaining and reviewing SOC 1, Type 2 reports misunderstood the services provided by ECOS, as ECOS does not obtain or review SOC 1, Type 2 reports, and did not have clear expectations as to what should be considered during their review of SOC 1, Type 2 reports.

Without adequate policies and procedures over service providers' operations, Social Services is unable to ensure its complementary user entity controls are sufficient to support their 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. 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 its review of the reports.

Social Services should obtain, review, and document SOC 1, Type 2 reports for its service providers that significantly affect its financial activity. As part of its corrective action, Social Services should assign responsibility to a knowledgeable resource within the agency to develop an office-wide policy that other divisions can use when reviewing and documenting SOC reports. Policies and procedures should comply with the requirements outlined in the CAPP Manual and Security Standard and include, but not be limited to, 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. After developing an agency-wide policy, Social Services should communicate it to all individuals responsible for overseeing service provider operations to ensure compliance with federal and state regulations.

Strengthen Internal Controls over FFATA Reporting

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Finance does not maintain adequate internal control over Federal Funding Accountability and Transparency Act (FFATA) reporting. FFATA reporting is intended to provide full disclosure of how entities and organizations are obligating federal funding. During fiscal year 2023, Social Services disbursed approximately $619 million in federal funds from roughly 5,400 subawards. During our audit of the TANF, Refugee and Entrant Assistance State/Replacement Designee Administered Programs (Refugee Assistance), and Crime Victim Assistance federal grant programs, we noted the following deviations from Finance's policy:

- Finance did not complete FFATA reporting submissions for 106 of 205 (52%) of the grant year 2023 TANF subawards that spent $30,000 or more during fiscal year 2023. Social Services disbursed approximately $7.9 million from these subawards during the fiscal year. Finance

did not report TANF subawards to FFATA Subaward Reporting System (FSRS) because program personnel did not submit the required information to Finance to report in FSRS.

- Finance did not complete FFATA reporting submissions for three of 17 (18%) of the grant year 2023 Refugee Assistance subawards that spent $30,000 or more during fiscal year 2023. Social Services disbursed approximately $126,000 from these subawards during the fiscal year. Finance did not report Refugee Assistance subawards to FSRS for these three subawards because the initial subaward amount was less than $30,000 and program personnel did not inform Finance that subsequent subaward modifications increased the subaward value to over $30,000.

- Finance did not complete FFATA reporting submissions for grant year 2023 Crime Victim Assistance subawards during fiscal year 2023. Social Services disbursed approximately $3.5 million from 129 subawards during the fiscal year. Social Services did not report this information to FSRS because it inadvertently assumed that it was a subrecipient of the Department of Criminal Justice Services and did not need to complete FFATA reporting as required by the Crime Victim Assistance Grant Special Conditions document.

Title 2 CFR Part 170 Appendix A requires the non-federal entity to report each obligating action exceeding $30,000 to the FSRS. Further, Title 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.

The decentralized nature of Social Services' grants management practices and the volume of subawards elevates the risk that Finance will not report all subaward information to FSRS. Although Finance sent periodic email reminders to program staff responsible for submitting FFATA data to Finance for submission to FSRS, program personnel overlooked a significant percentage of these submissions because of turnover and a lack of familiarity with FFATA reporting requirements. Additionally, Finance did not have a compensating internal control in place to detect subawards that it did not report to FSRS.

When Social Services does not upload all obligating actions meeting the reporting threshold to FSRS as required, a citizen or federal official may have a distorted view as to how Social Services is obligating federal funds. Therefore, Finance should continue to remind program personnel to submit required FFATA subaward reporting information to them and revise its policy to reflect any changes in its processes. Additionally, Finance should consider periodically checking Social Services' financial records to determine 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.

Strengthen Internal Controls over Financial Reporting of Non-Reimbursement Grants
Type: Internal Control
Severity: Significant Deficiency

Finance did not accurately report the year-end balances for non-reimbursement grants to the Department of Accounts (Accounts) in its Attachment 27 (Non-Reimbursement Grants) submission. Accounts uses this information to adjust the federal trust fund balance in the Commonwealth's ACFR to ensure that it appropriately represents the fund's net position as of fiscal year end. While auditing Social Services' Attachment 27 submission, we identified the following errors:

- Finance used incorrect data to calculate the year-end cash balance for each federal grant program in its Federal Cash Flow Statement workbook, which resulted in a $72.6 million overstatement in its calculated year-end federal cash balance. Finance uses the amounts in this workbook to complete the Attachment 21 (Receivables) and Attachment 27 submissions to Accounts. Finance resubmitted Attachments 21 and 27 to Accounts due to this misstatement.

- Finance did not include all non-reimbursable federal grant program cash balances in its initial Attachment 27 submission to Accounts, which resulted in a $24.7 million understatement of the modified accrual ending balance.

Finance experienced turnover in its financial reporting positions during the fiscal year and it did not identify these errors during its review of the Attachment 27 submission. Additionally, Finance does not have documented procedures outlining its process for preparing the Attachment 27 submission. Accounts' Office of the Comptroller Directive No. 1-23 states that an agency must ensure that it has internal controls in place to avoid material misstatements and/or misclassifications in the attachments and other financial information submitted to Accounts for inclusion in the Commonwealth's ACFR. Without implementing adequate internal controls over financial reporting, Social Services cannot reasonably assure itself that the financial information it submits to Accounts for inclusion in the Commonwealth's ACFR is free of material misstatements.

Finance should develop and implement procedures outlining its process for preparing the Attachment 27 submission. Additionally, Finance should perform a thorough review of its Attachment 27 submission before submitting it to Accounts. Implementing these internal controls will help Social Services reasonably assure itself that the financial information it submits to Accounts for inclusion in the Commonwealth's ACFR is free of material misstatements.

Reconcile the Commonwealth's Retirement Benefits System
Type: Internal Control
Severity: Significant Deficiency
First Issued: Fiscal Year 2022

Human Resources does not sufficiently reconcile retirement contributions before confirming to the Virginia Retirement System that retirement data is correct. Specifically, Human Resources continues

to not perform reconciliations between the Commonwealth's retirement benefits system and the Commonwealth's human resource and payroll management system and not review the Commonwealth's human resource and payroll management 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 payroll management and retirement benefits systems monthly before confirming the contribution. Further, the CAPP Manual Topic requires a daily review of the human resource and payroll management system cancelled records report.

Social Services transitioned to the human resources and payroll management system in April 2022 and its corrective action is dependent on obtaining an updated Scope of Services Manual from the Payroll Service Bureau to reflect the use of the human resource and payroll management system. Social Services contacted the Payroll Service Bureau in August 2023 to obtain an updated Scope of Services Manual; however, it was not available at that time and was informed that it was expected to be available within the next few months. Additionally, Human Resources initiated a process change to include a comparison of transactions keyed to the human resource and payroll management system and the Commonwealth's retirement benefits system. Finally, Human Resources implemented a new method to track changes, compare transactions between the two systems at least monthly, and make corrections as needed in July 2023.

Because of the extent of its corrective actions, Human Resources was not able to complete its corrective actions as of the end of fiscal year 2023. Human Resources plans to complete its corrective action efforts by April 1, 2024. Insufficient reconciliation processes can affect the integrity of the information in the Commonwealth's retirement benefits system, which the Virginia Retirement System uses for pension liability calculations for the Commonwealth's agencies and institutions. Therefore, Human Resources should continue its corrective action efforts to ensure that it sufficiently reconciles retirement contributions before confirming to the Virginia Retirement System that retirement data is correct.

Monitor Internal Procedures to Ensure Compliance with the Conflict of Interests Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2021

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 orientation training in accordance with the Code of Virginia. As part of its corrective action efforts, Human Resources is taking the following steps to ensure that it complies with Virginia's State and Local Government Conflict of Interests Act (COIA) and its internal procedures:

- Human Resources transitioned conflict of interests related processes to its Compliance unit in January 2023.

- Human Resources is updating the field used in the Commonwealth's human resources and payroll management system to identify positions of trust for newly added or removed positions.

- Social Services' Conflict of Interests Coordinator is working with division directors to review conflict of interest criteria and identify positions by title and responsibility that require compliance with the COIA.

- Social Services' Conflict of Interests Coordinator is reviewing Social Services' new hire/transfer report two times a month to identify newly created or re-established positions that may not have been captured with the correct conflict of interest status.

- Social Services' Conflict of Interests Coordinator is reviewing conflict of interest training records for all identified positions, employees, and board members. Any employee or board member who is not in compliance with conflict of interests training requirements will be asked to complete the required training and completion dates will be monitored and tracked in a conflict of interests tracking spreadsheet. Social Services' Conflict of Interests Coordinator will review the conflict of interests tracking spreadsheet twice monthly and contact employees and board members whose training is nearing expiration.

Section 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, the § 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 their procurement policies and procedures when procuring property and services with federal funds.

Because of the extent of its corrective actions, Human Resources was not able to complete its corrective actions as of the end of fiscal year 2023. Human Resources plans to complete its corrective action efforts by April 1, 2024. Without appropriately monitoring individuals in positions of trust, Social Services cannot assure itself that it is fully compliant with the provisions in the COIA. In effect, Social Services could be susceptible to actual or perceived conflicts of interests and may be limited in its ability to hold employees accountable. These actions could potentially lead to a violation of state or federal laws or regulations. Therefore, Human Resources should continue its corrective action efforts to ensure that it complies with the provisions of the COIA.

Comply with TANF Requirement to Participate in the Income Eligibility and Verification System
Type: Internal Control and Compliance
Severity: Deficiency
First Issued: Fiscal Year 2018

Social Services continues to develop and propose legislation to fully comply with the Income Eligibility and Verification System (IEVS) requirements 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, local agency employees are still unable to access IEVS because they have not satisfied all Internal Revenue Service (IRS) security requirements.

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 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 that 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. Title 45 CFR § 264.11 states that 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 to not participate in the IEVS or achieved compliance under a corrective compliance plan. To date, the Commonwealth has not demonstrated that it has reasonable cause to not participate in the IEVS and has not achieved compliance under a correction compliance plan.

The Secretary of Health and Human Resources has accepted Social Services proposal to require local agency employees to have fingerprint background checks and participate in IEVS and has submitted this legislation to the Governor for consideration in the Commonwealth's 2025 – 2026 biennial budget. Assuming the Governor accepts this legislative proposal, it will then be presented to the General Assembly for an official vote to determine if it will be adopted into state law.

RISK ALERTS

During the course of our audit, we encountered two 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 2023.

Unpatched Software
First Issued: 2021
Applicable to: DBHDS, Health, and Medical Assistance Services

VITA contracts with various 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 systems that support operations at DBHDS, Health, and Medical Assistance Services. Additionally, DBHDS, Health, and Medical Assistance Services rely on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of November 2023, the ITISP contractors had not applied a significant number of critical security patches to the IT environment at DBHDS, Health, and Medical Assistance Services, all of which are past the 90-day update window allowed by the Security Standard.

The Security Standard 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 (Security Standard, Section SI-2 Flaw Remediation). Missing system security updates increase the risk of successful cyberattack, exploitation, 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 DBHDS, Health, and Medical Assistance Services 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
First Issued: 2022
Applicable to: DBHDS, Health, and Medical Assistance Services

DBHDS, Health, and Medical Assistance Services rely on the ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, DBHDS, Health, and Medical Assistance Services rely on contractors

procured by VITA to provide DBHDS, Health, and Medical Assistance Services access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in the agencies' IT environments so agency personnel can review logged activity. Additionally, DBHDS, Health, and Medical Assistance Services 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, VITA tried to compel the ITISP contractor to grant agencies, such as DBHDS, Health, and Medical Assistance Service, access to the monitoring tool and audit log information for the last four years. As of October 2023, the MDR Dashboard went live for agencies to request access to the tool. However, VITA and the ITISP contractor did not formally communicate to all agencies, including DBHDS, Health, and Medical Assistance Services that it was available and how to request access to the tool. Also, while the MDR Dashboard is in production, it does not include all audit log information to allow agencies to adequately monitor their IT environments. Additionally, VITA and the ITISP contractor have not provided training to agencies on how to use the MDR Dashboard.

The Security Standard requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity (*Security Standard, Section AU-6 Audit Review, Analysis, and Reporting*). VITA not enforcing the deliverable requirements from the ITISP contractors increases the risk associated with the Commonwealth's data confidentiality, integrity, and availability. DBHDS, Health, and Medical Assistance Services are working with VITA and the ITISP contractors to obtain access to the audit log information within the MDR Dashboard to ensure the agencies can review the activities occurring in their IT environment in accordance with the Security Standard. Additionally, our separate audit of VITA, which is ongoing, will continue to address this issue.

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

First Issued: Fiscal Year 2016

In January 2012, the Commonwealth of Virginia and the United States (U.S.) 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 original settlement agreement, the Commonwealth was expected to demonstrate full compliance by June 30, 2020, and sustain a full year of compliance to exit court oversight of the agreement in 2021. The Commonwealth has not yet achieved full compliance and mutually agreed with the DOJ to extend the settlement agreement, first to July 1, 2022, then to December 31, 2023, and most recently to December 31, 2024. The largest barrier to achieving full compliance is not having the proper capacity for individuals with the most complex needs, specifically focusing on developing capacity around nursing, behavioral services, and access to dental services. DBHDS continues to work on these areas, however, additional improvements are necessary to achieve full compliance that is sustainable.

Over the past year, DBHDS has improved its project management activities to increase compliance with the settlement agreement, completed root cause analyses on indicators that are not yet in compliance, and improved the reliability and validity of the Commonwealth's data used for compliance reporting. However, there is further risk of noncompliance if DBHDS does not receive adequate funding at the appropriate time for provider rates, 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 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, the General Assembly, and the Administration to work together to ensure that DBHDS has the funds and support it needs to continue to comply with the settlement agreement and provide services to individuals in the appropriate setting.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

John Littel
Secretary of Health and Human Resources

Dr. Karen Shelton, MD, Commissioner
Department of Health

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

Dr. Danny TK Avula, Commissioner
Department of Social Services

Nelson Smith, Commissioner
Department of Behavioral Health and
Developmental Services

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, 2023. 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' 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, 2023. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, each agency's financial system, 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 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:
    Coronavirus State and Local Fiscal Recovery Funds
Information system security (including access controls)
Institutional revenues
Licensing behavioral health providers
Operational expenses, including payroll expenses

Department of Health

Accounts receivable
Collection of fees for services
Commonwealth's retirement benefit system
Cooperative agreements between Health and local governments, including:
    Accounts payable
    Aid to and reimbursement from local governments
    Cost allocations
Eligibility for:
    Special Supplemental Nutrition Program for Women, Infants and Children Program
Federal revenues, expenses, and compliance for:
    Child and Adult Care Food Program
    Coronavirus State and Local Fiscal Recovery Funds
Information system security (including access controls)
Inventory
Payroll expenses
Rescue squad support

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
- Children's Health Insurance Program
- Coronavirus State and Local Fiscal Recovery Funds

Provider assessment revenues and expenses
Information system security (including access controls)

Department 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:
- Child Support Enforcement
- Crime Victim Assistance
- Low-Income Household Water Assistance Program
- Medicaid Cluster
- Refugee Assistance and Entrant Assistance
- Temporary Assistance for Needy Families

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 the agency listed below with an "*" in support of the Commonwealth's Single Audit and we will separately report the results of that audit.

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

We performed audit tests to determine whether the agencies' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the agencies' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

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

Our consideration of internal control over financial reporting and federal compliance (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the section titled "Internal Control and Compliance 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, which are described in the section titled "Internal Control and Compliance 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 47 findings, which are described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

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

Conclusions

We found that the agencies, 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 system, and supplemental information and attachments submitted to the Department of Accounts, after Health and Social Services made adjustments to two attachments for material misstatements as noted in the "Audit Findings and Recommendations" section.

The results for the Commonwealth's Single Audit for the year ended June 30, 2023, are contained in a separate report, which will be available on our website at www.apa.virginia.gov in February 2024.

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 section titled "Internal Control and Compliance Findings and Recommendations."

The agencies have taken adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summaries included in the Appendix.

Since the findings noted above include those that have been identified as material weaknesses and/or 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, 2023. The Single Audit Report will be available at www.apa.virginia.gov in February 2024.

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 the agencies' responses to the findings identified in our audit, which are included in the accompanying section titled "Agency Responses." The agencies' responses were not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the responses.

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

JDE/clj

FINDINGS SUMMARIES

Department of Behavioral Health and Developmental Services

Finding Title	Status of Corrective Action	First Issued
Improve Controls over Capital Outlay Voucher Processing	Complete	2022
Improve Management of Access to the Retirement Benefits System	Complete	2022
Establish a Change Management Process for Information Technology Environment	Complete	2022
Improve Vulnerability Management Process	Ongoing	2022
Conduct Information Technology Security Audits over Sensitive Systems	Ongoing	2022
Develop Baseline Configurations for Information Systems	Ongoing	2015
Continue to Improve Database Security	Ongoing	2021
Continue to Improve Offboarding Procedures	Ongoing	2014
Improve Controls over the Payroll Certification Process	Ongoing	2023
Continue to Improve Controls over Payroll Reconciliations	Ongoing	2020
Continue to Implement Compliant Application Access Management Procedures	Ongoing	2018
Improve IT Contingency Management Program	Ongoing	2017
Continue to Improve Risk Assessment Process	Ongoing	2021
Continue Dedicating Resources to Support Information Security Program	Ongoing	2019
Improve Change Management Process for Information Technology Environment	Ongoing	2023
Improve Security Awareness Training Program	Ongoing	2023
Continue to Improve Controls over the Retirement Benefits System Reconciliation	Ongoing	2014
Ensure Compliance with the Conflict of Interests Act	Ongoing	2021
Continue to Improve Controls over the Calculation of Contractual Commitments	Ongoing	2021
Complete FFATA Reporting for First Tier SABG Subawards	Deferred*	2022

*This audit finding originated from the fiscal year 2022 audit of the Substance Abuse Block Grant federal grant program. This federal grant program is not in cycle for the Commonwealth's 2023 Single Audit, and as such, we limited our audit procedures to confirming the accuracy of the corrective action status in the Commonwealth's Summary Schedule of Prior Audit Findings. Per our inquiry with DBHDS, we determined that corrective action was ongoing as of June 30, 2023.

Department of Health

Finding Title	Status of Corrective Action	First Issued
Continue Addressing Compliance with the Conflict of Interests Act	Complete	2019
Continue Improving the Disaster Recovery Plan	Complete	2019
Continue Strengthening the Termination Process	Complete	2020
Continue Improving Information Technology Change Management Process for a Sensitive System	Complete	2020
Properly Prepare the Schedule of Expenditures of Federal Awards	Complete	2022
Strengthen Controls over Overtime Payments	Complete	2022
Improve Database Security	Complete	2022
Strengthen Controls over Financial Reporting	Ongoing	2021
Improve Controls over Journal Entries	Ongoing	2022
Follow Eligibility Documentation Requirements for Women, Infants and Children Program	Ongoing	2021
Improve Vulnerability Management	Ongoing	2023
Conduct Information Technology Security Audits	Ongoing	2023
Continue Strengthening the System Access Removal Process	Ongoing	2014
Improve Internal Controls over Employee Offboarding Process	Ongoing	2023
Improve System Access Procedures	Ongoing	2023

Department of Medical Assistance Services

Finding Title	Status of Corrective Action	First Issued
Improve Timely Removal of Critical System Access	Complete	2017
Continue Strengthening Process over Medicaid Coverage Cancellations	Complete	2021
Improve Information Security Program and Controls	Ongoing	2020
Obtain and Review Information Security Audit	Ongoing	2023
Improve Third-Party Oversight Process	Ongoing	2022
Perform Annual System Access Reviews	Ongoing	2023

Department of Social Services

Finding Title	Status of Corrective Action	First Issued
Continue to Strengthen Internal Controls to Ensure Compliance with Federal Employment Eligibility Requirements	Complete	2018
Continue Strengthening Process over Medicaid Coverage Cancellations	Complete	2021
Document Process to Collect and Retain Documentation Supporting the SSBG Post-Expenditure Report	Complete	2022
Correctly Report Status of Prior Audit Findings as of Fiscal Year End	Complete	2022
Improve Information Security Program and IT Governance	Ongoing	2022
Perform Responsibilities Outlined in the Agency Monitoring Plan	Ongoing	2018
Implement Internal Controls over TANF Federal Performance Reporting	Ongoing	2022
Obtain Reasonable Assurance over Contractor Compliance with Program Regulations	Ongoing	2023
Continue Improving IT Risk Management Program	Ongoing	2018
Continue Developing Record Retention Requirements and Processes for Electronic Records	Ongoing	2018
Improve Web Application Security	Ongoing	2019
Continue Improving IT Change and Configuration Management Process	Ongoing	2019
Upgrade End-of-Life Technology	Ongoing	2022
Conduct Information Technology Security Audits	Ongoing	2023
Monitor Internal Controls to Ensure Timely Removal of System Access	Ongoing	2018
Improve Documentation for Separation of Duty Conflicts	Ongoing	2022
Evaluate Separation of Duty Conflicts within the Case Management System	Ongoing	2023
Perform Annual Review of Case Management System Access	Ongoing	2023
Review Non-Locality Subrecipient Single Audit Reports	Ongoing	2018
Communicate Responsibilities to Subrecipient Monitoring Coordinators	Ongoing	2020
Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations	Ongoing	2021
Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities	Ongoing	2022
Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan	Ongoing	2022

Monitor Case Management System Records to Ensure Compliance with TANF Eligibility Requirements	Ongoing	2023
Implement Internal Controls over TANF Federal Special Reporting	Ongoing	2023
Obtain, Review, and Document System and Organization Controls Reports of Third-Party Service Providers	Ongoing	2021
Strengthen Internal Controls over FFATA Reporting	Ongoing	2022
Strengthen Internal Controls over Financial Reporting of Non-Reimbursement Grants	Ongoing	2023
Reconcile the Commonwealth's Retirement Benefits System	Ongoing	2022
Monitor Internal Procedures to Ensure Compliance with the Conflict of Interests Act	Ongoing	2021
Comply with TANF Requirement to Participate in the Income Eligibility and Verification System	Ongoing	2018
Perform Analysis to Identify Service Provider Agencies That Perform Significant Fiscal Processes	Deferred*	2022

*This audit finding originated from the fiscal year 2022 audit of the Social Services Block Grant federal grant program. This federal grant program is not in cycle for the Commonwealth's 2023 Single Audit, and as such, we limited our audit procedures to confirming the accuracy of the corrective action status in the Commonwealth's Summary Schedule of Prior Audit Findings. Per our inquiry with Social Services, we determined that corrective action was ongoing as of June 30, 2023.

COMMONWEALTH of VIRGINIA

NELSON SMITH
COMMISSIONER

VIRGINIA 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 10, 2024

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, 2023. We concur with the findings and our corrective action plans have been provided separately.

The Department of Behavioral Health and Developmental Services (DBHDS) has made significant progress to close several findings from prior year audits, and we appreciate that this report reflects the progress made to date on those corrective actions. We also greatly appreciate the audit team's interest and effort to recognize staffing crisis in our agency, 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 this fiscal year, we are proud of our staff for their incredible efforts to face those challenges while remaining committed to enhancing our operations and system of care.

We appreciate your team's efforts, constructive feedback, and acknowledgement of progress made by the agency despite facing many challenges in the past year. Please contact Divya Mehta, Director of Internal Audit if you have any questions regarding our corrective action plan.

Sincerely,

Nelson Smith
Commissioner

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

Karen Shelton, MD
State Health Commissioner

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

February 1, 2024

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, 2023. 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,

Karen Shelton, MD
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH

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 8, 2024

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 FY23 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, 2023. We concur with the audit findings and will submit a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the work plans for corrective actions that DMAS will take to address the audit findings.

We appreciate the audit team's work and feedback. If you have any questions or require additional information, please 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, 2022

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

Dear Ms. Henshaw:

The Virginia Department of Social Services concurs with the audit findings included in the 2023 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

5600 Cox Road · Glen Allen, VA 23060
www.dss.virginia.gov · 804-726-7011 · TTY Dial 711