


VIRGINIA DEPARTMENT OF SOCIAL SERVICES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

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

AUDIT SUMMARY

Our audit of the Virginia Department of Social Services (Social Services) for the fiscal year ended June 30, 2024, found:

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

- 25 matters involving internal control and its operations necessary to bring to management's attention; 24 of which represent instances of non-compliance with applicable laws and regulations or other matters that are required to be reported; and

- adequate corrective action with respect to five prior audit findings identified as "Complete" in the Findings Summary included in the Appendix.

We identified the Temporary Assistance for Needy Families (TANF) federal grant program as a high-risk major federal program at Social Services and included it within the Commonwealth's Single Audit scope. The Office of Management and Budget's Compliance Supplement requires an audit of Social Services' Administration for Children and Families (ACF) 199 TANF Data Report (ACF-199) and 209 Separate State Programs – Maintenance-of-Effort (MOE) Data Report (ACF-209) submissions. During the audit, we determined that Social Services did not implement internal controls to comply with the provisions at 45 Code of Federal Regulations (CFR) § 265.7(b), which require States to have complete and accurate reports that 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 compliance requirement for the TANF federal grant program because Social Services did not materially comply with the provisions at 45 CFR § 265.7(b).

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 Accounts in Topic 10205 – Agency Response to Auditor of Public Accounts Audit of the Commonwealth Accounting Policies and Procedures (CAPP) Manual. Those corrective actions may include additional items beyond our recommendation.

In fiscal year 2023, we included the results of our audit over Social Services in the report titled "Agencies of the Secretary of Health and Human Resources for the year ended June 30, 2023."

-TABLE OF CONTENTS-

COMMENT TO MANAGEMENT

A Comment to Management is an issue that came to our attention during the audit that we want to bring to management's attention for their consideration. We do not consider this issue an internal control weakness or a compliance finding for the agency.

Dedicate Resources to Adequately Monitor Corrective Actions for Audit Findings

Social Services has not dedicated the necessary resources to adequately monitor whether staff are performing corrective actions to address prior audit findings in a timely manner and if the corrective actions achieve the desired results. As a result, Social Services did not take adequate corrective action to resolve 22 of the 27 (81%) internal control and/or compliance deficiencies we communicated to management in prior audits. We have included findings and recommendations addressing the continuing internal control and/or compliance deficiencies, along with four new findings, in the report section titled "Internal Control and Compliance Findings and Recommendations." We found the internal control and/or compliance deficiencies are the most pervasive in the following areas of the agency:

- Social Services continues to not secure its sensitive information technology (IT) systems in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard). We identified 12 instances where Social Services did not comply with the Security Standard, including 11 (92%) that we included in prior reports. These audit findings are the result of Social Services having an insufficient governance structure to manage and maintain its information security program in accordance with the Security Standard. Social Services maintains over 70 sensitive IT systems that requires it to secure them in accordance with the Security Standard.

- Social Services' Division of Compliance (Compliance) continues to not fulfil its responsibilities in its Agency Monitoring Plan. During fiscal year 2024, Social Services disbursed approximately $660 million in federal funds to 342 subrecipients from 30 federal grant programs. The Agency Monitoring Plan is Social Services agreed-upon approach for overseeing the agency's subrecipient monitoring activities. We identified five instances where Compliance did not comply with the Agency Monitoring Plan, of which, including four (80%) that we included in prior reports. These findings are the result of Compliance not periodically evaluating its initial planned corrective actions to determine whether they adequately address the audit findings and not collaborating with division subrecipient monitoring coordinators.

- Social Services continues to report inaccurate information in its performance and special report submissions to the federal government for the Low-Income Home Energy Assistance (LIHEAP) and TANF federal grant programs because of inaccuracies by its third-party service provider. While Social Services has evaluated exceptions and requested modifications from its third-party service provider, the third-party service provider has yet to fulfil Social Services' requests after several months.

While the agency is taking incremental steps to implement planned corrective actions, Social Services is a large and complex agency and cross-division collaboration is necessary to effectively resolve the audit findings. Social Services has experienced significant turnover in several key positions over the last several years and has not formally designated who is responsible for monitoring the overall progress on audit findings, facilitating cross-division collaboration to resolve audit findings, and reporting progress to Social Services' Executive Team. Therefore, Social Services' Executive Team should determine who should be responsible for monitoring the agency's overall progress in addressing audit findings and ensure they have sufficient authority within the organization to enforce accountability, if necessary.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Information Security Program and IT Governance
Type: Internal Control and Compliance
Severity: Material Weakness
First Reported: Fiscal Year 2022

Social Services continues to have 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 information technology (IT) projects and prioritize information security and IT resources to ensure its information security program effectively protects sensitive Commonwealth data in accordance with the Security Standard.

We communicated the control 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 its sensitivity and description of security controls. The Security Standard requires the agency head to maintain an information security program that is sufficient to protect the agency's IT systems and to ensure the agency documents and effectively communicates the information security program. Not prioritizing IT resources to properly manage its information security program can result in a data breach or unauthorized access to confidential and mission-critical data, leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external.

The control weaknesses described in the communication marked FOIAE are the result of Social Services not assessing information security requirements prior to project implementation, in addition to Social Services not prioritizing information security within the IT environment. Social Services has hindered its ability to consistently and timely remediate findings from management recommendations issued during 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.

During fiscal year 2024, Social Services created a cybersecurity team under the Technology Services Division (TSD) to liaison between TSD and the Division of Information Security and Risk Management (ISRM) to help bring the information security program in compliance with the Security Standard. However, due to the magnitude of the project, TSD, the cybersecurity team, ISRM, and the executive team have not yet completed efforts to remediate this finding.

TSD, ISRM, and Social Services' Cybersecurity and Executive teams should continue to work together to bring the IT security program in compliance with the Security Standard. TSD and ISRM should continue to evaluate 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. Additionally, Social Services should evaluate the organizational placement of the Information Security Officer (ISO) to ensure effective implementation of the information security program and controls. 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 Reported: Fiscal Year 2018

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 2024, Social Services disbursed approximately $660 million to 342 subrecipients from 30 federal grant programs. During the audit, we noted the following deviations from the Agency Monitoring Plan:

- Compliance continues to not review programmatic division annual subrecipient monitoring plans to ensure they implement a risk-based approach. 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.

- Compliance does not hold monthly meetings with Subrecipient Monitoring Coordinators, as required by the Agency Monitoring Plan, where divisions can share information concerning risks and federal and/or grant-specific requirements, approaches to assessing risk, and changes that could affect subrecipients and the monitoring processes.

- Compliance has not reviewed each division's monitoring activities nor provided quarterly reports of variances and noncompliance from the Agency Monitoring Plan to Social Services' executive team. As a result, Compliance did not identify that the Division of Benefit Programs (Benefit Programs) did not complete risk assessments for 50 of its 324 (15%) locality subrecipients, properly document considerations for localities with elevated risks, nor perform adequate risk assessments for their non-locality subrecipients.

Since the prior audit, Compliance has communicated the Agency Monitoring Plan to the Subrecipient Monitoring Coordinators. Additionally, Compliance has worked with Social Services' Executive Team to secure funding for a grants management system and additional subrecipient monitor positions. However, Compliance has yet to establish a timeline for when it intends for the system to be fully functional and has not explored alternate options to comply with its Agency Monitoring Plan. Further, Compliance has not collaborated with Subrecipient Monitoring Coordinators to determine how the agency collectively plans to accomplish the goals and objectives set forth within the Agency Monitoring Plan. Collaboration between Compliance and Subrecipient Monitoring Coordinators is imperative to ensuring that Social Services complies with the pass-through entity requirements in 2 CFR § 200.332.

Title 2 CFR § 200.303(a) requires pass-through entities to establish, document, 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, Compliance cannot assure that the agency's subrecipient monitoring efforts are adequate to comply with the regulations at 2 CFR § 200.332. Additionally, Compliance places Social Services at risk of disallowed expenditures and/or suspension or termination of its federal awards by not monitoring the agency's subrecipient monitoring activities. 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 controls over compliance.

Compliance should work collaboratively with Social Services' Executive Team and the subrecipient monitoring coordinators to fulfil the agency's responsibilities in the Agency Monitoring Plan. Further, Compliance should explore alternative solutions to track and monitor each division's subrecipient monitoring activities and report the results to the Executive Team until it develops and implements its grants management system. Evaluating alternative solutions will help Social Services mitigate the risk of incurring federal sanctions because of non-compliance.

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

Benefit Programs does not have adequate internal controls in place to ensure accurate reporting in the ACF-199 and ACF-209 performance reports. The 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 the ACF-199 and ACF-209 reports and relies solely on their internal controls during the data extraction and data reporting process. 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 the extent of its corrective actions, Benefit Programs has not fully implemented all of its corrective actions and continues to rely on ACF's error correction controls, performed after report submission, to obtain assurance over the accuracy of the data included in its submissions.

We audited 60 cases and identified 19 instances (32%) where the third-party service provider did not report key line-item information accurately based on the data Social Services maintains in its case management system or other supporting data and Benefit Programs did not detect or correct these errors before the third-party service provider submitted the data to ACF. Specifically, we noted that Benefit Programs did not accurately report on the following key line items:

- Benefit Programs did not accurately report on the "Work Participation Status" key line item for 13 out of 60 (22%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Receives Subsidized Child Care" key line item for four out of 31 (13%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Hours of Participation" key line item for four out of 60 (7%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Work Eligibility Individual Indicator" key line item for two out of 60 (3%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Number of Months Countable Toward Federal Time Clock" key line item for two out of 56 (4%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Type of Family for Work Participation" key line item for two out of 60 (3%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Parent with Minor Child" key line item for one out of 56 (2%) cases tested during the audit.

- Benefit Programs did not accurately report on the "Unsubsidized Employment" key line item for one out of 60 (2%) cases tested during the audit.

Additionally, because of the lack of internal control over the ACF-199 and ACF-209 federal reports, Benefit Programs did not identify that the ACF revised the reporting specifications in November 2023 for certain key line items. Although ACF provided administering agencies with nearly a year to implement the new reporting specifications, Benefit Programs has not yet initiated discussions with its service provider to bring its current reporting model in line with the new reporting specifications. Therefore, there is risk that Social Services will continue to report inaccurate information to ACF going forward without working with its service provider to implement the new reporting specifications.

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. Additionally, 2 CFR § 303(a) requires that Social Services establish, document, and maintain effective internal control over the federal award that provides reasonable assurance that the recipient or subrecipient is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award. 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. Further, ACF can impose a penalty if it finds Social Services did not meet statutory required work participation rates. 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 comply with the provisions at 45 CFR § 265.7(b).

Benefit Programs should implement internal controls over the TANF federal performance reporting process and include a documented secondary review process of the service providers' data for which it should complete prior to the report submission. Additionally, Benefit Programs should develop

a process to track changes to the reporting specifications and communicate the changes to the service provider in advance of the applicable implementation date.

Continue Improving IT Risk Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2018

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

- accurately verify and validate data and system sensitivity ratings;
- create risk assessments for 90 percent of its sensitive systems;
- create system security plans for the 55 current systems identified as sensitive;
- review risk assessments for 100 percent of its existing documentation; and
- implement corrective actions identified in risk assessments.

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

ISRM and TSD defined and documented a new risk assessment policy and procedure in April 2024. Social Services also established a new risk assessment process that engages system administrators and system owners to complete a risk assessment worksheet to submit to ISRM for evaluation. ISRM meets with system administrators, system owners, and the Agency Head, to review the resulting risk assessment report and establish a risk mitigation plan. However, Social Services has not yet matured the new risk assessment process due to recently formalizing the process. Social Services established the Cybersecurity Team as part of TSD in fiscal year 2024; therefore, the Cybersecurity Team and ISRM have not yet assessed and integrated the various risk management processes. Additionally, the new risk assessment procedure does not define and document the requirements and processes Social Services must follow to implement the corrective action responsibilities.

ISRM should work with TSD, the Cybersecurity Team, and business units to ensure Social Services establishes and maintains an up-to-date sensitive systems list. The Information Security Officer, in conjunction with system and data owners, should classify agency IT systems and data based on sensitivity. Following its new risk assessment procedure and process, ISRM and the Cybersecurity Team

should prioritize completing risk assessments and system security plans for its sensitive systems and review those documents annually to validate that the information reflects the current environment. Additionally, TSD 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 Reported: 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 state law. Social Services' case management system stores several types of federal benefit program records with varying retention requirements supporting ten programs and services, such as the Medical Assistance (Medicaid), Supplemental Nutrition Assistance (SNAP), Child Care and Development Fund (CCDF), LIHEAP, and TANF 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 2024.

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. Social Services determined that due to the risk and complexity of the project, as well as changes to federal requirements since its first analysis, the retention requirements for all ten programs and services supported by its case management system were not feasible as a single release. Therefore, Social Services planned a phased delivery approach including multiple releases. In November 2023, Social Services defined and documented a purge and retention design document to implement Release 1 of the record purge and retention project for its case management system. Social Services subsequently implemented Release 1 of the record purge and retention project in February 2024. However, Social Services has not completed the process to implement 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 an agency does not lose information 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. Section § 42.1-86.1 requires 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.

Further, 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.

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 critical information according to recovery times. Finally, retaining records longer than necessary causes the Commonwealth to spend additional resources to maintain, back-up, and protect information that no longer serves a business purpose.

The magnitude and complexity of effectively implementing a retention and purge process for an integrated eligibility system delayed completion of the record purge and retention project. Additionally, following Release 1 implementation, Social Services identified an additional required element of the purge and retention project. For these reasons, Social Services plans to update the purge and retention design document and implement Release 2 in February 2025. Further, Social Services plans to complete the purge and retention project with the final release, Release 3, by September 2025. Social Services should complete the record purge and retention project for its case management system and, thereafter, implement consistent records retention and destruction processes across business divisions to ensure compliance with laws and regulations.

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

Social Services continues to not configure a sensitive web application in accordance with the Security Standard. During fiscal year 2024, Social Services remediated two of the five previously identified weaknesses; however, these two weaknesses existed during the fiscal year under review. Additionally, Social Services has not remediated three 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. Social Services prioritizing other projects also contributed to the weaknesses persisting.

TSD, ISRM, and business owners should work together to remediate the remaining weaknesses to secure the web application and meet the minimum requirements in its internal policies and the

Security Standard. Addressing these weaknesses will help to ensure the confidentiality, integrity, and availability of sensitive and mission-critical data and achieve compliance with both internal policies and the Security Standard.

Continue Improving IT Change and Configuration Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: 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 description of security mechanisms.

The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Social Services' information systems and data. Social Services' 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, Social Services migrated to a new change management system of record in October 2023, which also contributed to the delay in remediating the remaining issues due to Social Services prioritizing the migration project. Not prioritizing and 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 Reported: 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 the control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard 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.

In May 2024, Social Services established a Cybersecurity Team to track and manage technologies but has not yet completed their processes. 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 controls and recommendations discussed in the communication marked FOIAE in accordance with the Security Standard. By dedicating the necessary resources to evaluate and implement these controls and recommendations, Social Services will help to ensure that it adequately secures its IT environment and systems.

Conduct Information Technology Security Audits
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

Social Services is making progress in conducting a comprehensive IT security audit on each sensitive system at least once every three years. While Social Services conducted an IT security audit over an additional 22 percent of its sensitive systems, 14 of the 79 sensitive systems (18%) due for an IT Security Audit remain unaudited. Social Services indicates it is on track to complete the remaining IT security audits by the end of calendar year 2025.

The Security Standard 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 Commonwealth's IT Security Audit Standard, SEC502 (IT Audit Standard). 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. Without conducting full IT security audits 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.

During fiscal year 2024, Social Services' Audit Services Manager collaborated with the business divisions, TSD, and ISRM to schedule and conduct audits. However, Social Services did not perform the remaining IT security audits due to the large number of sensitive systems requiring an audit. Lack of a documented procedure and process for conducting IT security audits also contributed to the lapse in IT security audits conducted over the last three years.

Social Services should define and document a formal procedure and process for conducting IT security audits over each sensitive system at least once every three years that tests the effectiveness of the IT security controls and their compliance with Security Standard requirements. Social Services should then complete all outstanding IT security audits to ensure it meets 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 Reported: Fiscal Year 2018

Social Services continues to implement internal controls to monitor the timely removal of system access. The Security Standard requires the organization to disable information system access within 24 hours of employment termination.

In response to the prior audit recommendations, ISRM developed an overarching policy governing system access that addresses the timely removal of system access and Social Services' Division of Human Resources developed a policy to ensure supervisors follow the appropriate steps to offboard separated employees. Additionally, ISRM and the Division of Human Resources worked collaboratively to develop a process to identify individuals whose separation did not follow the offboarding policy and manually removed their access from Social Services' access management system. However, because of the extent of its corrective actions, Social Services was not able to implement all of its planned corrective actions by the end of fiscal year 2024.

Social Services administers numerous public assistance programs that collect personally identifiable information and other protected information from beneficiaries. Social Services could place 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 Reported: Fiscal Year 2022

Social Services' Division of Finance (Finance) continues to implement written documentation to justify and authorize conflicting access to its financial accounting and reporting system. Since the prior year's audit, Finance has developed internal controls to document and authorize conflicting access in its financial accounting and reporting system, including a conflicting responsibility report to monitor user accounts with separation of duty conflicts and an updated access request form to provide only temporary access for users with separation of duty conflicts. However, Finance did not fully implement these internal controls as of the end of fiscal year 2024 due to the extent of its corrective actions.

The Security Standard requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks. Additionally, 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 separation of duties. There is an increased risk that users can perform unauthorized transactions in Social Services' financial accounting and reporting system when improper separation of duties exists. Therefore, Finance should continue to implement the corrective action efforts necessary to justify and authorize conflicting access to its financial accounting and reporting system.

Evaluate Separation of Duty Conflicts within the Case Management System

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

Benefit Programs, which is the owner of Social Services' case management system, has not performed nor documented a conflicting access review to identify the combination of roles that could pose a separation of duties conflict or to 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, SNAP, CCDF, LIHEAP, and TANF federal grant programs. Social Services authorized over $17 billion in public assistance payments to beneficiaries from these federal programs through its case management system during fiscal year 2024.

The Security Standard requires the agency to separate duties of individuals as necessary, document separation of duties of individuals, and define information system access authorizations to support the separation of duties. Further, Social Services' Information Security Policy states that the system owner is responsible for identifying and documenting separation of duties of individuals and defining system access authorizations to support separation of duties. Without performing and documenting a conflicting access review, Social Services does not know which combination of roles may pose a separation of duties conflict and is unable to implement compensating controls. In effect, this increases the possibility of a system breach or other malicious attack on Social Services' data and places Social Services' reputation at risk.

Benefit Programs has not yet begun their corrective action efforts and ISRM has not included this finding in its Plan of Actions and Milestones (POAM) report, which is its internal corrective action plan that it shares with Social Services' Executive Team. As a result, Social Services' Executive Team was not aware that Social Services continues to be non-compliant with the Security Standard and its Information Security Policy. According to Social Services' Organizational Structure Report, ISRM provides guidance to system owners about security requirements and is ultimately responsible for protecting Social Services' information systems by addressing security compliance and risk.

Benefit Programs should conduct a conflicting access review for the case management system and collaborate with ISRM to ensure it performs and documents this review in accordance with Social Services' Information Security Policy. Additionally, ISRM should monitor this finding's progress through its POAM report and provide periodic updates to Social Services' Executive Team.

Perform Annual Review of Case Management System Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

Benefit Programs, which is the owner of Social Services' case management system, continues to not perform the required annual access review. Social Services uses the case management system to determine applicant eligibility and authorize benefit payments for the Medicaid, SNAP, CCDF, LIHEAP, and TANF federal grant programs. Social Services authorized over $17 billion in public assistance payments to beneficiaries from these federal programs through its case management system during fiscal year 2024.

The Security Standard requires the agency to review accounts for compliance with account management on an annual basis. Additionally, ISRM's Procedures Manual for State and Local Security Officers requires system owners and security officers to review user access privileges annually. System owners and security officers must complete this review within 364 days from the completion date of the last security review. Benefit Programs last completed a security review over the case management system in June 2022.

Benefit Programs is responsible for obtaining the case management system's access listing from ISRM, coordinating the annual review with the security officers, and working with ISRM to modify user access privileges as necessary. However, Benefit Programs did not perform the required annual access review for the case management system because it did not initiate the process with ISRM, and ISRM did not include this finding in its POAM report, which is its internal corrective action plan that it shares with Social Services' Executive Team. As a result, Social Services' Executive Team was not aware that Social Services continues to be non-compliant with the Security Standard and its Procedures Manual for State and Local Security Officers.

According to Social Services' Organizational Structure Report, ISRM provides guidance to System Owners about security requirements and is ultimately responsible for protecting Social Services' information systems by addressing security compliance and risk. Social Services increases the risk of improper or unnecessary access to sensitive systems by not reviewing access to the case management system annually, which could potentially result in a system breach or other malicious attack on Social Services' data and adversely affect its reputation.

Benefit Programs should perform the required annual security review for the case management system and collaborate with ISRM to ensure it completes this review in accordance with the Procedures Manual for State and Local Officers. Additionally, ISRM should monitor this finding's progress through its POAM report and provide periodic updates to Social Services' Executive Team.

Develop and Provide Role-Based Security Awareness Training to System Administrators and Data Custodians

Type: Internal Control and Compliance
Severity: Significant Deficiency

ISRM does not provide applicable role-based training to system administrators or data custodians that have security roles and responsibilities with elevated privileges. Additionally, ISRM does not document a procedure that outlines the steps it follows to administer the role-based training. 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.

Social Services' Awareness and Training Policy requires that Social Services' Information Security Officer or designee provide role-based security and privacy training to personnel with the roles and responsibilities of system administrator and data custodian. Social Services' Security Awareness and Training Policy and the Security Standard also require that Social Services administer role-based training to personnel before authorizing access to the system, information, or performing assigned duties; and annually thereafter, as well as when required by system changes.

Without providing role-based training to all personnel with security-related roles, including personnel with the roles and responsibilities of system administrator and data custodian, Social Services increases the risk of human error and negligence. Additionally, lack of adequate role-based training increases the risk that users will be unaware or lack pertinent skills and knowledge to perform their security-related functions, resulting in an increased security risk.

ISRM did not provide role-based training to personnel with designated information security roles due to competing priorities. Additionally, although the Awareness and Training Policy requires role-based training, Social Services does not define and document their process to provide role-based training to personnel with security-related functions, such as the specific training that each role should take, the deadline for role-based training completion, and the enforcement measure resulting from not completing the role-based training timely.

ISRM should develop procedures that detail the process to provide role-based training to personnel with designated security roles. ISRM should also develop and administer role-based training for systems administrators and data custodians. Improving the security awareness training program will help protect Social Services from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Ensure Subaward Agreements Meet Federal Regulations
Type: Internal Control and Compliance
Severity: Significant Deficiency

Social Services does not include all information required by federal regulations in its subaward renewal agreements. We tested 20 subaward renewal agreements and noted that all of them did not contain one or more of the elements required by 2 CFR § 200.332(a)(1). Specifically, we noted the following instances of non-compliance in these subaward renewal agreements:

- Social Services did not include the correct Federal Award Identification Number (FAIN) in 15 of the 20 (75%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(iii).

- Social Services did not include the federal award date in eight of the 20 (40%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(iv).

- Social Services did not update the federal award date in 12 of the 20 (60%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(iv).

- Social Services did not include the FAIN in five of the 20 (25%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(iii).

- Social Services did not include the amount of federal funds obligated in the subaward in four of the 20 (20%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(vii).

- Social Services did not include the subrecipient's unique entity identifier in four of the 20 (20%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(ii).

- Social Services did not include the contact information for the awarding official of the pass-through entity in four of the 20 (20%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(xi).

- Social Services did not identify whether the federal award was for research and development in four of the 20 (20%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(xiii).

- Social Services did not include the federal award project description in two of the 20 (10%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(x).

- Social Services did not accurately report the name of the federal awarding agency in two of the 20 (10%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(xi).

- Social Services did not include the Assistance Listing Number in one of the 20 (5%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(xii).

- Social Services did not identify the indirect cost rate for the federal award in one of the 20 (5%) subaward renewal agreements, as required by 2 CFR § 200.332(a)(1)(xiv).

During fiscal year 2024, Social Services disbursed approximately $46 million in federal funds from the TANF federal grant program through 238 subawards. While Social Services communicates federal award information to subgrantees, it does not consistently communicate all of the federal grant award information required in its subaward renewal agreements. The Contract and Procurement team within Social Services' Division of General Services works collaboratively with grants administrators when preparing subaward agreements. However, the Contract and Procurement team has experienced turnover over the last several years and has lost institutional knowledge in some of its key positions as it pertains to federal grant requirements. Additionally, the Contract and Procurement team does not consistently retain all incorporated attachments in the subaward agreement.

Compliance is responsible for ensuring that the agency adheres to federal regulations in 2 CFR § 200.332 through its Agency Monitoring Plan; however, Compliance was not aware of these instances of non-compliance because it was not involved in the preparation of the subaward agreements. According to Social Services' Organizational Structure Report, Compliance is responsible for agency-wide compliance and risk mitigation that helps ensure adherence to state and federal legal and regulatory standards. Because of the lack of agency-wide collaboration, there were inconsistencies in the information included in the subaward agreements.

Without communicating the required federal award information, Social Services increases the risk that subrecipients are unaware of the source of the funding and the applicable requirements, which increases the potential for unallowable costs and non-compliance with federal requirements. Compliance should work collaboratively with the Contract and Procurement team and grants administrators to ensure that subaward agreements include all information required by federal regulations.

Review Non-Locality Subrecipient Single Audit Reports

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

Compliance continues to not review non-locality subrecipient Single Audit reports as set forth within its Agency Monitoring Plan. Non-locality subrecipients are subrecipients who are not local governments and are mainly comprised of non-profit organizations. During fiscal year 2024, Social Services disbursed approximately $107 million in federal funds to 244 non-locality subrecipients. While reviewing the Single Audit reports submitted to the Federal Audit Clearinghouse (Clearinghouse) for the most recent audit period for the 27 non-locality subrecipients that received more than $750,000 in federal funds from Social Services during state fiscal year 2024, we noted the following:

- Six non-locality subrecipients (22%) did not have a Single Audit report available in the Clearinghouse for the most recent audit period. Of the six non-locality subrecipients, three

appeared to have never submitted a Single Audit report to the Clearinghouse. Title 2 CFR § 200.332(f) requires pass-through entities to 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.

- Three non-locality subrecipients (11%) had audit findings that affected at least one of Social Services' federal grant programs. One of the non-locality subrecipient auditors identified $82,253 in known questioned costs as the non-locality subrecipient did not maintain proper documentation to support payroll charges to the TANF federal grant program. Title 2 U.S. 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, including determining if the questioned costs are disallowed and need to be repaid to the federal awarding agency, and proposed corrective actions.

As part of its planned corrective action, Compliance stated that it intends to procure a grants management system with subrecipient monitoring capabilities necessary to comply with federal requirements and has worked with Social Services' Executive Team to secure funding. However, Compliance has yet to establish a timeline for when it intends for the solution to be fully functional. Additionally, Compliance has not evaluated what alternative corrective actions are available to become compliant.

According to Social Services' Organizational Structure Report, Compliance is responsible for agency-wide compliance and risk mitigation that helps ensure adherence to state and federal legal and regulatory standards. Additionally, Social Services' Agency Monitoring Plan assigns the responsibility to Compliance for overseeing the agency's subrecipient monitoring process. Without verifying whether non-locality subrecipients received a Single Audit, Compliance is unable to assure Social Services' Executive Team that it is fulfilling the pass-through entity responsibilities in 2 CFR § 200.332. Not complying with federal regulations could result in federal awarding agencies temporarily withholding payments until it takes corrective action, disallowing costs for all or part of the activity associated with the noncompliance, suspending, or terminating the federal award in part or in its entirety, initiating initial suspension or debarment proceedings, and/or withholding further federal funds for the project or program. Further, Social Services may be unaware of a potential liability to the Commonwealth by not reviewing the non-locality Single Audit reports.

Compliance should consider exploring alternative corrective actions as it continues to develop and implement its grants management system, such as obtaining a list of non-locality subrecipients from its internal accounting system and reviewing the Single Audit reports in the Clearinghouse. Evaluating alternative corrective actions to become compliant with federal regulations will help Social Services mitigate the risks of incurring federal sanctions.

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

Benefit Programs did not confirm that program consultants evaluated each subrecipient's risk of noncompliance in accordance with federal regulations. Benefit Programs oversees the administration of the Medicaid, SNAP, TANF, and LIHEAP federal grant programs. During fiscal year 2024, Social Services disbursed approximately $660 million in federal funds to roughly 342 subrecipients from 30 federal grant programs.

As part of its fiscal year 2024 corrective action efforts, Benefit Programs updated its monitoring plan to include risk assessment and monitoring reviews for both localities and non-localities subrecipients, began performing locality and non-locality risk assessments, and created tracking documents to better manage the subrecipient monitoring process. Additionally, Benefit Programs partnered with program consultants to perform risk assessment procedures.

While auditing Benefit Programs' fiscal year 2024 subrecipient monitoring activities, we noted the following deviations from its subrecipient monitoring plan:

- Program consultants did not complete non-locality programmatic risk assessments for 219 out of 251 (87%) subawards with payments during the fiscal year.

- Program consultants did not include adequate justification for why it would not perform a monitoring review during the monitoring period for 83 out of 274 (30%) locality programmatic risk assessments assessed as high or medium risk.

- Program consultants did not complete 50 out of 324 (15%) locality programmatic risk assessments.

- Program consultants assessed three of the non-locality subrecipients as moderate risk without an adequate justification of why a monitoring review would not be scheduled for these non-locality subrecipients.

- Program consultants improperly assessed two of the non-locality subrecipients as low risk even though they had never submitted a Single Audit report to the Clearinghouse.

- Program consultants did not include a locality programmatic risk assessment that was identified as requiring a targeted monitoring review in their schedule for the fiscal year.

Title 2 CFR § 200.332(b) requires pass-through entities to evaluate each subrecipient's risk of noncompliance with federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring. Without performing the proper risk

assessment procedures, Benefit Programs cannot demonstrate that it monitored the activities of the subrecipients as necessary to ensure that the pass-through entities used the subawards for authorized purposes in compliance with federal statutes, regulations, and the terms and conditions of the subaward.

Benefit Programs was not able to adequately oversee the implementation of its risk assessment processes due to turnover in its subrecipient monitoring coordinator position. Additionally, Social Services' Compliance Division was not aware of this non-compliance because it was not performing its monitoring responsibilities in accordance with its Agency Monitoring Plan. Benefit Programs should continue to evaluate its resource levels to ensure that it has adequate resources to effectively oversee the execution of its subrecipient monitoring plan. Additionally, Benefit Programs should dedicate the necessary resources to confirm that program consultants complete risk assessment procedures for all of its subrecipients in accordance with its subrecipient monitoring plan.

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

Benefit Programs did not confirm that program consultants performed all required subrecipient monitoring activities in accordance with its subrecipient monitoring plan. During fiscal year 2024, Social Services disbursed approximately $660 million in federal funds to roughly 342 subrecipients from 30 federal grant programs. As part of its fiscal year 2024 corrective action efforts, Benefit Programs updated its monitoring plan to include risk assessment and monitoring reviews for both localities and non-localities subrecipients, began performing locality and non-locality risk assessments, and created tracking documents to better manage the subrecipient monitoring process. Further, Benefit Programs partnered with program consultants to execute its subrecipient monitoring activities. While auditing Benefit Programs' fiscal year 2024 monitoring activities, we noted the following deviations from its subrecipient monitoring plan:

- Benefit Programs did not confirm program consultants notified the locality timely about the subrecipient monitoring review process. As a result, Benefit Programs did not identify that program consultants did not initiate timely communications for five out of 19 (26%) scheduled locality monitoring reviews.

- Benefit Programs did not confirm that program consultants fully documented corrective actions taken by its subrecipients in accordance with its subrecipient monitoring plan. As a result, Benefit Programs was not able to provide fully documented corrective action plans for four out of 19 (21%) scheduled locality monitoring reviews.

- Benefit Programs did not confirm that program consultants uploaded all fiscal year 2024 monitoring review records to its data repository in accordance with its subrecipient monitoring plan. As a result, Benefit Programs was not able to provide complete documentation for three out of 19 (16%) scheduled locality monitoring reviews.

- Benefit Programs did not confirm that program consultants included the appropriate sampling units, as outlined in its subrecipient monitoring plan. As a result, Benefit Programs did not identify that three out of 19 (16%) locality monitoring reviews had less sampling units than required by its subrecipient monitoring plan.

- Benefit Programs did not confirm that program consultants performed all scheduled monitoring reviews. As a result, Benefit Programs did not identify that program consultants did not perform a scheduled monitoring review for one out of 19 (5%) of its locality subrecipients. Based on Benefit Programs' subrecipient monitoring risk assessments, this locality review was necessary due to the presence of risk factors which created a higher risk of non-compliance.

- Benefit Programs has not fully implemented its non-locality risk assessment and monitoring review processes which caused program consultants to perform only one monitoring review over approximately 251 non-locality subawards with payments during the fiscal year.

Title 2 CFR § 200.332(e) requires the pass-through entity to monitor the activities of the subrecipient as necessary to ensure that the subrecipient uses the subaward for authorized purposes in compliance with federal statutes, regulations, and the terms and conditions of the subaward. Without confirming that program consultants conducted monitoring activities in accordance with the monitoring plan, Benefit Programs cannot provide assurance that it complied with federal regulations and potentially places Social Services at risk of disallowed expenditures and/or suspension or termination of its federal awards.

Benefit Programs was not able to adequately oversee the execution of monitoring activities because of turnover in its subrecipient monitoring coordinator position. Additionally, Social Services' Compliance Division was not aware of this non-compliance because it was not performing its monitoring responsibilities in accordance with its Agency Monitoring Plan. Benefit Programs should continue to evaluate its resource levels to ensure that it has adequate resources to effectively oversee the execution of its subrecipient monitoring plan. Additionally, Benefit Programs should dedicate the necessary resources to confirm that program consultants are performing monitoring procedures in accordance with its subrecipient monitoring plan.

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

Benefit Programs has not documented its processes for preparing and verifying the information reported in the LIHEAP federal grant program's Annual Household Report. The federal government requires Social Services to annually submit this data and uses this information to provide reports to Congress for assessing the uses of funds for the assistance of households in need.

Benefit Programs uses a third-party service provider to produce data reports from its case management system that program staff use to populate the LIHEAP Annual Household Report and Benefit Programs relies on the third-party service provider's internal controls during the data extraction process. Benefit Programs could not substantiate the information reported for four out of seven (57%) of the line items in Section I - Number of assisted households of the most recent LIHEAP Annual Household Report. Specifically, we noted the following inconsistencies:

- Benefit Programs reported 2,571 households assisted on the Emergency Furnace Repair and Replacement line, which is 12 percent higher than the information in the case management system.

- Benefit Programs reported 118,347 households assisted on the Any Type of LIHEAP Assistance line, which is 21 percent lower than the information in the case management system.

- Benefit Programs reported 117,274 households assisted on the Bill Payment Assistance line, which is 20 percent higher than the information in the case management system.

- Benefit Programs could not provide support to substantiate the Weatherization line.

Title 2 CFR § 200.303(a) requires the non-federal entity to establish, document, and maintain effective internal control over the federal award that provides reasonable assurance that the recipient is managing the federal award in compliance with federal statutes, regulations, and its terms and conditions. Further, 45 CFR § 96.82(a) requires each grantee, whether a State or an insular area, that receives an annual allotment of at least $200,000 to submit this data for the 12-month period preceding the federal fiscal year in which the grantee requests the funds. The grantee must report the data separately for LIHEAP heating, cooling, crisis, and weatherization assistance. If Social Services does not submit this report properly, ACF may not grant them their LIHEAP grant allotment as per 45 CFR § 96.82(c).

Benefit Programs has not dedicated the necessary resources to document its processes for preparing the LIHEAP Annual Household Report. Documented policies and procedures will help Social Services maintain continuity with its processes to comply with laws and regulations. Without documented policies and procedures, there is a risk that Social Services could report inaccurate information to the federal government that could lead to Social Services incurring fines and/or penalties. Additionally, reporting potentially inaccurate information prevents the federal government from adequately monitoring Social Services' overall performance for the LIHEAP federal grant program. Therefore, Benefit Programs should dedicate the necessary resources to document its processes for preparing the LIHEAP Annual Household Report, including the processes used to verify the data provided by its third-party service provider.

Implement Internal Controls over TANF Federal Special Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

Benefit Programs has not documented its process for preparing the ACF's Annual Report on State MOE Programs (ACF-204) for the TANF federal grant program. ACF requires Social Services submit this data annually and uses the 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. Title 2 CFR § 200.303(a) requires the non-federal entity to establish, document, and maintain effective internal control over the federal award that provides reasonable assurance that the recipient is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

During fiscal year 2024, Benefit Programs performed an analysis of ACF-204 reporting errors identified during the prior audit to determine causality and has taken actions to resolve those errors. Additionally, Benefit Programs created a systems modification request to correct errors that it identified as occurring due to inaccurate programming in the data modification phase of the federal report creation. However, Benefit Programs has not yet documented its processes for preparing the ACF-204 report through a written policy and procedure.

Documented policies and procedures will help Social Services maintain continuity with its processes to comply with laws and regulations. Without documented policies and procedures, there is a risk that Social Services could report inaccurate information to the federal government that could lead to Social Services incurring fines and/or penalties. Benefit Programs should dedicate the necessary resources to document its processes for preparing the ACF-204 report to ensure reasonably accurate reporting of TANF MOE Programs to ACF in accordance with the ACF-204 reporting instructions.

Strengthen Internal Controls over FFATA Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Finance is not maintaining 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 funds. During fiscal year 2024, Social Services disbursed approximately $660 million in federal funds from roughly 5,300 subawards.

While auditing FFATA reporting for the TANF federal grant program, we noted that Finance did not file any FFATA reports for its subrecipients. Social Services awarded over $72 million in nearly 300 new TANF subawards during fiscal year 2024. Title 2 CFR Part 170 Appendix A requires the non-federal entity to report each obligating action that equals or exceeds $30,000 to the FFATA Subaward Reporting System (FSRS) by the end of the month following the obligating action. This also applies to any subaward modifications that increase the amount to equal or exceed $30,000. Finally, 2 CFR § 200.303(a) states

that the non-federal entity must establish, document, and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award.

Finance uses a decentralized approach to fulfil its FFATA reporting responsibilities since it does not determine which subrecipients will receive federal funding. Since there is an elevated risk that Finance will not report all subaward information to FSRS, it has obtained a report of subrecipients from its financial reporting system and identified those who spent $30,000 or more in TANF funds during fiscal year 2024. However, Finance management did not compare this report to its FSRS submissions to verify that the agency submitted the submissions accurately and timely. As a result, Finance management did not recognize that it did not comply with the FFATA reporting requirements.

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. Finance management should provide sufficient oversight to confirm that the agency is submitting FFATA reporting submissions timely. Specifically, Finance management should periodically compare the report of subrecipients from its financial reporting system to FSRS to ensure it is reporting all subawards to FSRS and escalate any concerns that hinder its ability to comply with federal regulations.

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

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

Social Services continues to not obtain, review, and document System and Organization Controls (SOC) reports, specifically SOC 1, Type 2 reports, to gain assurance over its third-party service providers' internal controls relevant to financial reporting. SOC 1, Type 2 reports address the service organization's internal controls and the effect those internal controls may have on the user entity's financial statements. Social Services uses service organizations to perform functions that are significant to its financial operations such as administering the electronic benefit transfer (EBT) process for several of its public assistance programs. For instance, during fiscal year 2024, one of Social Services' third-party service providers issued more than $2 billion in financial assistance to beneficiaries on EBT cards.

Topic 10305 of the CAPP Manual requires agencies to have adequate interaction with service providers to appropriately understand the service provider's internal control environment and maintain oversight over service providers to gain assurance over outsourced operations. Additionally, 2 CFR § 200.303(a) requires non-federal entities to establish, document, 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' tasks contract administrators with responsibility for obtaining, reviewing, and documenting SOC 1, Type 2 reports. However, contract administrators are often not familiar with the CAPP Manual requirements, and Social Services has not made them aware of the expectations for obtaining, reviewing, and documenting SOC 1, Type 2 reports through a documented policy and procedure. As a result, contract administrators have not been obtaining, reviewing, and documenting SOC 1, Type 2 reports.

Without adopting a policy and procedure over SOC 1, Type 2 reports and communicating those expectations to contract administrators, 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 1, Type 2 reports. In effect, Social Services is increasing the risk that it will not detect a weakness in a service provider's environment by not obtaining the necessary SOC 1, Type 2 reports timely or properly documenting its review of the reports.

Social Services should designate a resource within the agency, who is knowledgeable of the CAPP Manual and SOC 1, Type 2 report requirements, with responsibility for developing an office-wide policy and procedure that contract administrators can use for obtaining, reviewing, and documenting SOC 1, Type 2 reports. At a minimum, Social Services' policy and procedure should include the timeframes for obtaining SOC 1, Type 2 reports from service providers, documentation requirements for user entity complementary controls, the steps needed to address internal control deficiencies and/or exceptions found in reviews, and the staff responsible for any corrective actions necessary to mitigate the risk to the Commonwealth until the service provider corrects the deficiency. Thereafter, Social Services should communicate the policy and procedure to all individuals responsible for overseeing service provider operations to ensure compliance with federal and state regulations. Finally, Social Services should retain this information as part of its annual Agency Risk Management and Internal Control Standard certification.

Reconcile the Commonwealth's Retirement Benefits System

Type: Internal Control
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Social Services' Division of Human Resources (Human Resources) continues to implement corrective actions necessary to reconcile retirement contributions in the Commonwealth's retirement benefits system. In response to prior audit recommendations, Human Resources has updated its policies and procedures to align with the CAPP Manual and the Payroll Services Bureau's Scope of Services Manual. The policies and procedures include processes for reconciling the Commonwealth's human resource and payroll management and retirement benefits systems and resolving any identified discrepancies between the two systems; confirming that new hires appear in the correct retirement plan; reviewing any separations or retirements in the Commonwealth's retirement benefits system; and reviewing and confirming transactions between the Commonwealth's human resource and payroll management and retirement benefits systems monthly. However, Human Resources was not able to

implement the processes outlined in its policies and procedures as of the end of fiscal year 2024 due to the extent of its corrective actions.

CAPP Manual Topic 50470, Human Capital Management Benefits Reconciliation, 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. Additionally, CAPP Manual Topic 50470 requires a prompt review of the retirement benefits system cancelled records report. 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. Human Resources anticipates that its corrective actions will be complete by December 2024. Human Resources should continue to implement its corrective action efforts necessary to reconcile retirement contributions in the Commonwealth's retirement benefits system.

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

Type: Internal Control and Compliance
Severity: Deficiency
First Reported: Fiscal Year 2023

Social Services did not comply with certain federal eligibility requirements for the TANF federal grant program, resulting in known questioned costs of $6,968. The TANF federal grant program provided over $89 million in assistance to approximately 26,000 needy families during fiscal year 2024. During the audit, we reperformed the eligibility determinations for all needy families that received assistance during the fiscal year and identified 24 instances (<1%) where the facts in the recipient's case record did not support the eligibility determination. Specifically:

- For 14 payments, Social Services did not properly evaluate whether individuals were already counted as eligible for TANF benefits under an existing case which allowed these individuals to receive multiple benefit payments in excess of its Standards of Assistance and maximum program benefit amounts. Title 42 United States Code (USC) § 604(a)(1) mandates that a state may use the grant in any manner that is reasonably calculated to accomplish the purpose of TANF where Social Services' reasonable calculation is defined by its Standard of Assistance and maximum program benefit amounts within its TANF Program Manual.

- For five payments, Social Services did not properly assign to the state the rights that the family member may have for child support in which recipients were underpaid in their benefit amount. Title 42 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 one payment, Social Services did not properly evaluate the income eligibility of the case. 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 one payment, Social Services did not properly evaluate the extended absence of a child or adult to the case. Title 42 USC § 608(a)(10) mandates that a state shall not use any part of the grant to provide assistance to a minor child who has been absent from the home for a period of 45 consecutive days.

- For two payments, Social Services did not properly reduce or terminate assistance for individuals not complying with the Commonwealth's work requirements for the TANF program. 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.

- For one payment, Social Services did not properly evaluate the qualified alien status of the case as required by 8 USC § 1611.

Social Services relies on its case management system to properly determine eligibility, correctly calculate benefit payments, and achieve the federal requirements of the TANF federal grant program. Of the exceptions noted above, five of the 24 (21%) were the result of local Social Services 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 USC. The remaining 19 exceptions (79%) resulted from local Social Services eligibility workers not including sufficient documentation to justify the rationale for their eligibility determinations. Social Services did not identify these exceptions because it did not have a mechanism to identify risky transactions in its case management system that deviate from its normal practices and require further follow-up. Non-compliance with these provisions increases Social Services' risk of incurring disallowed costs and having to repay grant funds to the federal government.

Social Services should continue to provide additional training to local Social Services eligibility workers on how to properly determine and document eligibility determinations in its case management system. Additionally, Social Services should consider implementing a data-driven approach to monitor and analyze data from its case management system to identify risky transactions that deviate from its normal practices. By providing additional training and implementing additional risk-based data analytics, Social Services will be able to ensure that the facts in the applicant's or recipient's case record supports each decision in its case management system regarding eligibility and complies with federal requirements.

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

Type: Internal Control and Compliance
Severity: Deficiency

Social Services did not comply with certain federal eligibility requirements for the LIHEAP federal grant program, resulting in known questioned costs of $6,569. Social Services provided over $114 million in assistance to approximately 215,000 needy families during fiscal year 2024 through the LIHEAP federal grant program. During the audit, we reperformed the eligibility determinations for all needy families that received assistance during the fiscal year and identified 12 instances (<1%) where individuals applied for benefits more than once and received benefit payments in excess of Social Services' maximum benefit amounts.

Social Services relies on its case management system to ensure it determines eligibility properly, calculates benefit payments correctly, and complies with the federal and state laws and regulations. However, Social Services' case management system does not prevent eligibility workers from authorizing individuals on multiple cases but instead provides a warning message for which they could choose to ignore. Additionally, Social Services does not have a mechanism to detect when an individual has received benefits from multiple cases and/or received benefit payments in excess of its maximum benefit amount.

Title 42 USC § 8624(b)(10) mandates that the State shall provide fiscal control to assure the proper disbursal of and accounting for Federal funds, including procedures for monitoring the assistance provided. Further, Social Services' Energy Assistance Program Manual, which it developed to comply with 42 USC § 8624(b)(10), stipulates that the eligibility worker will determine whether each adult household member is associated with an existing case number when they apply or reapply for benefits. Non-compliance with these provisions increases Social Services' risk of incurring disallowed costs and having to repay grant funds to the federal government.

Social Services should provide additional training to eligibility workers to properly identify individuals who have already applied for and received LIHEAP benefits. Additionally, Social Services should review the case management system's current warning messages to determine how it can strengthen internal controls so that eligibility workers will not be able to approve cases which could result in this type of error. Finally, Social Services should consider implementing a detective control, such as reviewing payment reports, to identify potential disallowed payments resulting from an individual appearing on multiple case records.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Health and Human Resources

James Williams
Commissioner, Virginia Department of Social Services

We have audited the financial records, operations, and federal compliance of the **Virginia Department of Social Services** (Social Services) for the year ended June 30, 2024. 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 Social Services' 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, 2024. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, Social Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts; reviewed the adequacy of Social Services' 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

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

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

- 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 the following federal grant programs:
  - Low-Income Home Energy Assistance
  - Medicaid Cluster
  - Pandemic EBT Food Benefits
  - Temporary Assistance for Needy Families
- Financial reporting
- Human resources
- Information system security (including access controls)

We performed audit tests to determine whether Social Services' 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 Social Services' 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 on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. We consider the deficiencies titled "Improve Information Security Program and IT Governance," "Perform Responsibilities Outlined in the Agency Monitoring Plan," and "Implement Internal Controls over TANF Federal Performance Reporting," 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 20 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 explicitly identified two findings in the section titled "Internal Control and Compliance Findings and Recommendations" as deficiencies.

Conclusions

We found that Social Services properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Social Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations." As stated in the deficiency titled "Implement Internal Controls over TANF Performance Reporting," which is described in the section titled "Internal Control and Compliance Findings and Recommendations," Social Services did not materially comply with one of the federal reporting requirements for the TANF federal grant program. As a result, we issued a qualified opinion over the reporting compliance requirement for the TANF federal grant program, as described in 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 is included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2024. Outside of this instance of material non-compliance, Social Services complied, in

all material respects, with all other compliance requirements that could have a direct and material effect on the TANF federal grant program for the year ended June 30, 2024.

Social Services has taken adequate corrective action with respect to audit findings and recommendations identified as complete in the Findings Summary 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, 2024. The Single Audit Report will be available at www.apa.virginia.gov in February 2025.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 14, 2025. Government Auditing Standards require the auditor to perform limited procedures on Social Services' response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Social Services' response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

MAS/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Comply with TANF Requirement to Participate in the Income Eligibility and Verification System	Complete	2018
Communicate Responsibilities to Subrecipient Monitoring Coordinators	Complete	2020
Monitor Internal Procedures to Ensure Compliance with the Conflict of Interests Act	Complete	2021
Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities	Complete	2022
Strengthen Internal Controls over Financial Reporting of Non-Reimbursement Grants	Complete	2023
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
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
Develop and Provide Role-Based Security Awareness Training to System Administrators and Data Custodians	Ongoing	2024
Ensure Subaward Agreements Meet Federal Regulations	Ongoing	2024
Review Non-Locality Subrecipient Single Audit Reports	Ongoing	2018
Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations	Ongoing	2021
Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan	Ongoing	2022
Implement Internal Controls over LIHEAP Federal Special Reporting	Ongoing	2024

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Implement Internal Controls over TANF Federal Special Reporting	Ongoing	2023
Strengthen Internal Controls over FFATA Reporting	Ongoing	2022
Obtain, Review, and Document System and Organization Control Reports of Third-Party Service Providers	Ongoing	2021
Reconcile the Commonwealth's Retirement Benefits System	Ongoing	2022
Monitor Case Management System Records to Ensure Compliance with TANF Eligibility Requirements	Ongoing	2023
Monitor Case Management System Records to Ensure Compliance with LIHEAP Eligibility Requirements	Ongoing	2024
Perform Analysis to Identify Service Provider Agencies That Perform Significant Fiscal Processes	Ongoing**	2022
Obtain Reasonable Assurance over Contractor Compliance with Program Regulations	Ongoing**	2023

* A status of **Complete** indicates management has taken adequate corrective action. **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

**These audit findings originated from the fiscal year 2022 audit of the Social Services Block Grant federal grant program and the fiscal year 2023 audit of the Low-Income Household Water Assistance federal grant program. These federal grant programs are out of scope for the Commonwealth's 2024 Single Audit, and as such, we limited our audit procedures to confirm the accuracy of the corrective action statuses in the Commonwealth's Summary Schedule of Prior Audit Findings. Per inquiry with Social Services' management, we determined that corrective action was ongoing for both of these audit findings as of June 30, 2024.

COMMONWEALTH of VIRGINIA

DEPARTMENT OF SOCIAL SERVICES

Office of the Commissioner

James Hunter Williams
Commissioner

January 14, 2025

Auditor of Public Accounts
Virginia Department of Social Services
5600 Cox Road
Glen Allen, Virginia 23060

Dear Ms. Henshaw,

The Virginia Department of Social Services concurs with the audit findings included in the 2024 review conducted by the Auditor of Public Accounts.

Should you require additional information, please do not hesitate to contact John Vosper via email at john.vosper@dss.virginia.gov or by telephone at 703-244-8693.

Sincerely,

Kevin Erskine
Chief Deputy Commissioner / Chief Operating Officer